sui generis

RITÉ DES URES LA GESTION DENTS EN

La cybersécurité des infrastructures critiques et la gestion de cyberincidents en droit suisse

Pauline Meyer

Notes sur la version numérique de ce livre :

— La version numérique (Open Access) est disponible sur le site de la maison d'édition (www.suigeneris-verlag.ch), sur Google Books et directement via le Digital Object Identifier (DOI). Le DOI de ce livre est indiqué dans les mentions légales.
— Tous les articles juridiques ainsi que tous les arrêts de tribunaux et les décisions de l'autorité librement accessibles sont liés dans la version numérique.
— Les auteurs utilisent souvent des liens vers d'autres sources dans leurs manuscrits. Ceux-ci ne sont pas imprimés dans les livres mais sont inclus sous forme d'hyperliens dans la version digitale.
— Les liens permanents sont utilisés pour créer des liens. Il s'agit de liens vers une version archivée des pages web au moment de l'établissement du lien. Les liens sont persistants, c'est-à-dire qu'ils fonctionnent toujours même si la page d'origine n'est plus accessible et leur contenu ne change pas si la page d'origine change.

Pauline Meyer

La cybersécurité des infrastructures critiques et la gestion de cyberincidents en droit suisse

sui generis, Zurich 2025

À mamoune

Remerciements

L'on m'avait dit que la rédaction d'une thèse consistait en une expérience solitaire. Outre mon plaisir bien connu de mon entourage à travailler dans ma bulle, tel n'a pas (et heureusement !) été le cas. J'ai au contraire eu le plaisir de côtoyer de nombreuses personnes durant ces années de recherche et de rédaction, avec lesquelles j'ai eu la chance de collaborer, d'échanger et aux côtés desquelles j'ai pu évoluer.

Je tiens tout d'abord à remercier toute l'équipe du projet « L'éthique et le droit pour promouvoir la confiance dans la cybersécurité ». Merci à David-Olivier Jaquet-Chiffelle qui, même s'il n'a finalement pas été mon co-directeur de thèse, a été aussi présent et disponible que s'il l'avait été, avec une bienveillance constante, une patience et une attention aux détails dans toutes les explications qu'il m'a fournies sur les aspects techniques de mes recherches. Merci également à Markus Christen, Melanie Knieps, Sara Pangrazzi ainsi qu'aux collègues du NCSC de m'avoir accueillie à Zurich, respectivement à Berne durant une partie de mes recherches, et de m'avoir permis de participer à quelques projets supplémentaires et plus vastes. Finalement, merci à Delphine Sarrasin et à Christophe Hauert pour les différents échanges, le soutien et les collaborations de ces quelques années.

La route aurait également été bien plus solitaire en l'absence de mes collègues, qui ont été tout particulièrement présentes, que ce soit pour discuter de nos sujets de recherches, de notre quotidien ou encore de nos luttes respectives. Merci aux collègues du Centre de droit pénal (CDP) qui m'ont accueillie comme si j'en faisais totalement partie, avec qui de nombreux rires, des projets communs et des moments extérieurs au travail m'ont permis d'avancer dans mes recherches, de prendre confiance en moi et d'évoluer le plus sereinement possible dans mon environnement de travail. Un merci tout particulier à Enzo Bastian, de m'avoir soutenue comme tu l'as fait, de m'avoir poussée et rassurée quand je doutais, pour les relectures si méticuleuses (entre coquilles et utilisation du féminin comme genre universel, la tâche était difficile) et pour la bienveillance dont tu as toujours fait preuve lors de nos échanges. Un grand merci également à Laura Ces pour la colocation de bureau durant mes trois années de contrat, toutes ces soirées à travailler, notre beau voyage ainsi que cette chouette complicité.

J'ai également la chance de pouvoir compter sur un entourage particulièrement aimant et soutenant qui m'a permis de mener à bien cette recherche. Merci à Livio, Vanja, Ryan, Hub, Léo, Maxime, Aleks, Nouki, Alex, Margaux, Léa, Val, Cloclo et toutes les autres personnes qui m'ont écoutée radoter des heures durant sur la cybersécurité des infrastructures critiques alors que personne

ne comprenait ce qu'était une infrastructure critique. Merci d'avoir épongé mon stress la veille de conférences importantes, d'avoir écouté mes plaintes au sujet de mes notes de bas de pages contrariantes et surtout d'avoir été auprès de moi avec tout l'amour et l'affection qu'on se donne pour s'aider à évoluer.

Dans cet entourage proche, je ne peux naturellement pas manquer de remercier deux des personnes les plus importantes, Chachon et Mamoune. Chachon, merci d'être toujours là pour moi, dans les bons moments comme dans les plus durs, de me faire confiance et de toujours avoir une oreille attentive et sans jugement sur ce que je partage. Mamoune, je ne sais même pas par où commencer. Merci pour ton soutien inconditionnel durant tout mon parcours, pour ton éducation pleine de douceur, d'amour et d'encouragement, pour toujours croire en moi, pour ton aide quotidienne et pour, à chaque réussite (et peu importe laquelle), partager ma joie et ma fierté. C'est en partie pourquoi je tiens tout particulièrement à ce que cette thèse te soit dédiée. Je vous suis à toutes deux éternellement reconnaissante.

Il me reste à remercier tout chaleureusement deux personnes qui ont endossé un rôle tout à fait central dans mes années de travail à l'Université de Lausanne et en particulier pour la réussite de ce doctorat. Tout d'abord un immense merci à Camille Perrier Depeursinge, car bien que je ne fusse pas votre doctorante, vous m'avez prise sous votre aile et m'avez impliquée dans différents projets tout à fait passionnants, me permettant d'une part d'approfondir mes connaissances dans d'autres domaines me tenant à cœur, et, d'autre part, de travailler avec vous qui êtes une personne et professeure pour qui j'ai beaucoup de respect et d'admiration. J'en profite aussi pour vous remercier de m'avoir donné l'une de mes premières opportunités académiques en m'accompagnant dans ma toute première publication il y a trois ans.

Finalement, je tiens à remercier infiniment Sylvain Métille. Malgré les remerciements déjà échangés, je souhaitais inclure dans cette thèse une mention écrite pour vous exprimer ma gratitude pour la confiance que vous m'avez témoignée et pour les nombreuses opportunités que vous m'avez offertes. Vous m'avez permis d'être assistante-étudiante, puis m'avez donné ma chance avec cette thèse de doctorat et le projet qui l'entoure. Merci d'avoir eu confiance en ma manière de travailler, d'avoir en même temps toujours été disponible pour discuter (entre rires et conversations constructives), et de continuer à m'offrir des opportunités externes passionnantes. Vous avez été un réel mentor pour moi et le produit fini ainsi que la mention assortie relèvent de notre collaboration, ce dont je vous suis extrêmement reconnaissante.

Lausanne, 1er septembre 2024
Pauline Meyer

Sommaire

Remerciements V
Sommaire VII
Table des matières IX
Table des abréviations et des locutions latines XXVII
Table des réglementations citées XXXV
Bibliographie LI
Avant-propos XCI

Introduction générale 1

Première Partie : les fondements 11

Chapitre 1 : les notions principales 13

Chapitre 2 : le contexte stratégique 73

Chapitre 3 : les compétences principales en cybersécurité 87

Deuxième partie : un état des lieux du cadre réglementaire suisse 149

Chapitre 4 : le cadre réglementaire pour la cybersécurité des infrastructures critiques 151

Chapitre 5 : le cadre légal pour l'activité des prestataires de gestion de cyberincidents 247

Chapitre 6 : la protection des informations au centre de la gestion de cyberincidents 321

Chapitre 7 : une conclusion intermédiaire sur les lacunes observées en droit suisse 400

Troisième Partie : les pistes réglementaires 413

Chapitre 8 : la nécessité de développer la réglementation 415

Chapitre 9 : la réglementation de la cybersécurité des infrastructures critiques 423

Chapitre 10 : les solutions ciblant les prestataires de gestion de cyberincidents **492**

Conclusion générale **543**

Table des matières

Remerciements V
Sommaire VII
Table des matières IX
Table des abréviations et des locutions latines XXVII
Table des réglementations citées XXXV
Bibliographie LI
Avant-propos XCI

Introduction générale 1

Première Partie : les fondements 11

Chapitre 1 : les notions principales 13
Préambule au chapitre 1 13
I. La cybersécurité et son contexte 13
A. La notion de cybersécurité 13
1. Le contexte de la protection contre les cybermenaces 13
a. Les trois domaines de la protection contre les cybermenaces 13
b. Le domaine de la cybersécurité 15
c. Le domaine de la poursuite pénale de la cybercriminalité 16
d. Le domaine de la cyberdéfense 17
2. La cybersécurité comme état 17
a. Des définitions 17
b. Les délimitations 21
B. Les autres notions clés 23
1. La cybermenace et le cyberrisque 23
2. Le cyberincident 25
3. La cyberattaque 27
4. La vulnérabilité 28
5. La cyberrésilience 29
6. Les groupes cibles 30
a. Les autorités 30
b. Les infrastructures critiques 31
c. Les autres groupes cibles 36
C. La gestion de cyberincidents 37

1. Les notions ... 37
2. Les mesures de gestion de cyberincidents ... 40
a. Un aperçu des étapes de la gestion de cyberincidents ... 40
b. La planification et la préparation ... 41
c. La détection ... 43
d. La réaction et les mesures post-cyberincident ... 44
e. Des mesures complémentaires ... 46
(i) Le traitement de renseignements sur les cybermenaces 46
(ii) La cyberassurance ... 47
(iii) Les évaluations, labels et certifications ... 49
D. Une conclusion ... 51
II. Un bref aperçu des principaux enjeux ... 52
A. Les enjeux globaux ... 52
1. La protection des informations ... 52
2. L'augmentation, la professionnalisation et la complexification des attaques ... 53
3. La coopération ... 55
a. Au niveau national ... 55
b. Au niveau international ... 57
4. La subsidiarité de l'intervention étatique ... 58
B. Les enjeux concrets ... 59
1. Les coûts ... 59
2. La chaîne d'approvisionnement ... 61
3. Mieux vaut prévenir que guérir ... 62
4. Une question de confiance ... 63
5. La cybersécurité et l'éthique ... 64
6. Les évolutions technologiques : vecteurs de progrès comme de risques ... 66
a. Quelques évolutions technologiques ... 66
b. Concrètement ... 66
(i) L'intelligence artificielle ... 66
(ii) L'Internet des objets ... 67
(iii) L'informatique en nuage ... 68
c. Des sources de progrès et de risques ... 69
C. Une synthèse ... 71
III. Une conclusion au chapitre 1 ... 72

Chapitre 2 : le contexte stratégique ... 73
Préambule au chapitre 2 ... 73
I. La transformation numérique et les stratégies s'y rapportant ... 74

A. La Stratégie Suisse numérique 74
B. La Cyberstratégie nationale 75
C. Les autres stratégies de la Suisse numérique 78
D. En résumé 79
II. D'autres stratégies pour la protection contre les cybermenaces 80
A. La Stratégie pour la protection des infrastructures critiques 80
B. La Stratégie de lutte contre la criminalité 81
C. Le cadre stratégique pour la cyberdéfense 81
D. La Stratégie de politique extérieure numérique 83
E. La politique de gestion de risques de la Confédération 83
F. En résumé 84
III. Une conclusion au chapitre 2 85

Chapitre 3 : les compétences principales en cybersécurité 87
Préambule au chapitre 3 87
I. Les actrices principales de la Confédération 88
A. Pour la cybersécurité 88
1. L'évolution en cours 88
2. La situation jusqu'à fin décembre 2023 88
a. Le Centre national pour la cybersécurité et son organisation 88
(i) Le Centre national pour la cybersécurité 88
(ii) La personne déléguée à la cybersécurité 89
(iii) L'ancienne MELANI 89
(iv) GovCERT 90
(v) Les autres services du NCSC 92
b. Les départements, la chancellerie et les unités administratives 93
c. D'autres autorités impliquées 93
3. La situation depuis janvier 2024 95
a. La création de l'Office fédéral de la cybersécurité 95
b. L'organisation au sein du Conseil fédéral 97
4. Un résumé des changements pour la cybersécurité 97
B. La poursuite pénale de la cybercriminalité 99
1. Le département fédéral compétent 99
2. Les autorités de poursuite pénale 99
3. D'autres entités compétentes 100
C. La cyberdéfense 102
1. Le département fédéral compétent 102
2. Le service du renseignement 103

3. L'armée et le commandement Cyber ... 104
4. Les autres entités compétentes ... 105
D. Les autorités compétentes issues d'autres domaines ... 106
1. Le SEPOS ... 106
2. Le secteur TNI ... 107
3. La Préposée fédérale à la protection des données et à la transparence ... 108
4. D'autres autorités ... 108
E. Une synthèse ... 110
II. Les actrices privées ... 112
A. Une contextualisation de la gestion de cyberincidents ... 112
B. Les organisations compétentes dans la gestion technique des cyberincidents ... 113
1. Une multitude de structures et de pratiques ... 113
2. Le Security Operation Center ... 114
3. Le Computer Security Incident Response Team ... 115
4. Les Cyber Fusion Centers, Red Teams et autres structures 117
5. Le rôle de la responsable de la sécurité des systèmes d'information ... 117
C. Les compétences des prestataires de gestion de cyberincidents 118
1. Des remarques introductives ... 118
2. La planification et la préparation ... 121
3. De la prévention à la détection de cyberincidents ... 122
4. La réaction ... 123
a. La réception comme déclencheur ... 123
b. L'analyse ... 125
(i) Des généralités ... 125
(ii) L'analyse de cyberincidents ... 125
c. La circonscription, l'éradication et la restauration ... 128
(i) La circonscription des cyberincidents ... 128
(ii) L'éradication ... 130
(iii) La restauration ... 131
d. La question de l'attribution ... 132
e. Les activités post-incident ... 133
5. Tout au long du processus ... 135
a. Un point de contact ... 135
(i) Les communications hors cyberincident ... 135
(ii) Les échanges dans le cadre de la gestion de cyberincidents ... 135
b. La documentation ... 138

6. Des compétences accessoires ... 139
a. La gestion des vulnérabilités ... 139
b. La gestion de la qualité de la sécurité ... 140
c. Les compétences de renseignement ... 141
D. Des communautés et les organisations en développement ... 142
1. Les communautés ... 142
(i) De manière générale ... 142
(ii) Dans la pratique de gestion de cyberincidents ... 144
2. Une nouvelle entité : l'Institut national de test pour la cybersécurité ... 146
E. Une synthèse ... 146
III. Une conclusion au chapitre 3 ... 147

Deuxième partie : un état des lieux du cadre réglementaire suisse 149

Chapitre 4 : le cadre réglementaire pour la cybersécurité des infrastructures critiques ... 151
Préambule au chapitre 4 ... 151
I. La cybersécurité comme domaine transversal et dispersé ... 152
A. La nécessité de légiférer au fil du temps ... 152
B. La prise en compte de standards internationaux ... 153
1. Les références aux standards internationaux ... 153
2. Les cadres du NIST ... 155
3. Les normes ISO ... 157
4. D'autres documents fréquemment utilisés ... 158
C. Les lois applicables aux secteurs et sous-secteurs critiques ... 160
1. Une introduction aux réglementations sectorielles ... 160
2. Le secteur critique des autorités ... 161
a. Le secteur ... 161
b. La Loi sur la sécurité de l'information et son ordonnance ... 162
c. Un exemple d'autre loi pertinente ... 164
d. D'autres instruments pour les autorités de la Confédération ... 165
e. Les normes cantonales ... 167
f. Les obligations d'annonce ... 171
g. En conclusion ... 171
3. Le secteur critique de l'énergie ... 173
a. Le secteur ... 173
b. Les lois générales ... 173

(i) La Loi fédérale sur l'énergie ... **173**
(ii) La Loi sur la sécurité de l'information ... **174**
c. La révision de la Loi fédérale sur l'approvisionnement en électricité ... **174**
d. La Loi fédérale sur l'énergie nucléaire et ordonnances relatives ... **176**
e. Quelques autres exemples de bases légales ... **178**
f. Les normes minimales ... **180**
g. En conclusion ... **181**
4. Le secteur critique de l'élimination ... **183**
a. Le secteur ... **183**
b. La protection de la population et de l'environnement ... **183**
c. Les obligations d'annonce ... **184**
d. Les normes minimales non contraignantes ... **184**
e. En conclusion ... **185**
5. Le secteur critique des finances ... **185**
a. Le secteur ... **185**
b. L'Autorité fédérale de surveillance des marchés financiers ... **186**
c. Les obligations d'annonce ... **187**
d. En conclusion ... **188**
6. Le secteur critique de la santé ... **190**
a. Le secteur ... **190**
b. L'Ordonnance sur les dispositifs médicaux ... **190**
c. La Loi fédérale sur le dossier électronique du patient ... **191**
d. Les obligations d'annonce ... **192**
e. Les recommandations dans le secteur de la santé ... **193**
f. En conclusion ... **194**
7. Le secteur critique de l'information et de la communication ... **195**
a. Le secteur ... **195**
b. Les services informatiques ... **196**
(i) Les organisations concernées ... **196**
(ii) Le cas particulier des pirates éthiques ... **197**
(iii) Les limites du cadre légal ... **200**
c. Les télécommunications ... **203**
d. Les obligations d'annonce ... **205**
e. En conclusion ... **206**
8. Les autres secteurs critiques ... **207**
a. Le secteur critique de l'alimentation ... **207**

b. Le secteur critique de la sécurité publique 209
c. Le secteur critique des transports 210
D. Des réglementations sectorielles aux réglementations transversales 212
1. Une explication 212
2. Les obligations d'annonce 213
a. La Loi sur la sécurité de l'information 213
b. L'obligation d'annoncer les violations de la sécurité des données 214
3. Les autres obligations de protection des données personnelles 216
4. La norme de l'Office fédéral de l'approvisionnement économique 219
E. Une synthèse 220
II. Un survol des autres domaines de la protection contre les cybermenaces 222
A. Une remarque introductive 222
B. La cybercriminalité 222
1. La criminalisation comme point de départ 222
a. Les infractions dans le cyberespace 222
b. Les infractions informatiques typiques principales 224
c. Les infractions informatiques atypiques principales 227
d. Le droit pénal accessoire 232
2. Les mesures de lutte contre la cybercriminalité 233
a. Une histoire de compétences 233
(i) Au niveau suisse 233
(ii) Au niveau international 235
b. Tout est question de coopération 235
(i) La coopération en Suisse 235
(ii) La coopération internationale 236
c. L'exploitabilité des moyens de preuve informatiques 238
3. D'autres mesures de lutte contre la cybercriminalité 240
a. L'Ordonnance sur les domaines Internet 240
b. Des actes cantonaux et intercantonaux 241
C. La cyberdéfense 241
1. La cyberdéfense dans la protection des infrastructures critiques 241
a. La base légale pour le Service de renseignement de la Confédération 241
b. Les bases légales légitimant l'intervention de l'armée 242

2. La spécificité du domaine de la cyberdéfense ... 243
D. Une synthèse ... 243
III. Une conclusion au chapitre 4 ... 245

Chapitre 5 : le cadre légal pour l'activité des prestataires de gestion de cyberincidents ... 247
Préambule au chapitre 5 ... 247
I. Les prestataires de gestion de cyberincidents ... 249
A. La double casquette des prestataires de gestion de cyberincidents ... 249
B. La prestataire de gestion de cyberincidents comme infrastructure critique ... 250
1. Les bases légales principales ... 250
2. Les spécificités pour les fabricantes ... 251
C. Les prestataires de gestion de cyberincidents et les organisations privées ... 252
1. Une diversité de possibilité ... 252
2. La réglementation entre cocontractantes privées ... 254
a. Les contrats envisageables ... 254
(i) Les facteurs d'influence ... 254
(ii) Le contrat individuel de travail ... 255
(iii) Les autres contrats pour la prestataire externe ... 256
(iv) Une réalité pratique ... 259
b. Les conséquences ... 260
(i) Les impacts de la qualification du contrat ... 260
(ii) Un exemple de responsabilité contractuelle ... 261
(iii) Quelques autres aspects de la responsabilité contractuelle ... 264
D. Entre prestataire privée et cliente critique ... 265
1. Les fournisseuses internes aux infrastructures critiques ... 265
2. Les prestataires externes de gestion de cyberincidents ... 267
a. Le cas particulier de la cliente étatique ... 267
(i) Le cadre légal ... 267
(ii) Les conditions générales et clauses types ... 269
b. L'exemple de l'approvisionnement en électricité ... 271
3. Une conclusion sur l'influence sectorielle ... 271
E. Les responsabilités indépendantes du contrat ... 272
1. Une remarque introductive ... 272
2. La responsabilité civile pour acte illicite ... 273
a. La responsabilité civile ... 273

b. La responsabilité de l'employeuse ... 274
c. La responsabilité du fait des produits ... 275
d. La responsabilité pour violation du droit d'auteure ... 276
3. La responsabilité pour violation d'obligations de sécurité ... 276
4. La responsabilité pour violation d'obligations de signaler ... 277
F. Une conclusion ... 278
II. L'Office fédéral de la cybersécurité ... 279
A. Un contexte en mouvement ... 279
1. Le développement des fondements légaux ... 279
2. L'Office fédéral de la cybersécurité et son service technique 280
a. Les compétences générales pour la cybersécurité ... 280
b. Le service technique de l'office fédéral ... 284
c. Les compétences liées à la sécurité de l'information ... 285
B. L'office fédéral et la cybersécurité des infrastructures critiques ... 285
1. Ses compétences préventives et de gestion de la qualité de la sécurité ... 285
2. Ses compétences réactives ... 286
a. Une remarque introductive ... 286
b. Les recherches passives ... 287
(i) Après le signalement d'un cyberincident ou d'une cyberattaque ... 287
(ii) Les mesures concrètes ... 288
c. Une surveillance active ? ... 291
3. L'office fédéral comme point de contact ... 292
a. Les flux de données généraux ... 292
b. Le partage d'informations avec les infrastructures critiques ... 293
c. La collaboration avec les autorités de poursuite pénale 296
d. Les échanges avec le Service de renseignement de la Confédération ... 298
e. Les échanges avec d'autres autorités ... 300
f. La collaboration avec d'autres prestataires analogues ... 301
4. La gestion de vulnérabilités ... 303
5. L'activité du secteur privé comme limite ... 304
C. Quelques généralités ayant trait à la responsabilité ... 305
D. Une conclusion ... 307
III. Un bref détour par le service spécialisé pour la sécurité de l'information ... 308
A. La création du nouveau service ... 308

B. Le lien étroit entre le service et l'Office fédéral de la cybersécurité ... 309
C. Une conclusion sur l'impact du nouveau service ... 312
IV. Un survol de quelques chefs communs de responsabilité ... 312
A. La responsabilité pénale ... 312
B. Pour des infractions au Code pénal ... 313
C. Pour des infractions à d'autres lois ... 317
D. Une conclusion ... 318
V. Une conclusion au chapitre 5 ... 318

Chapitre 6 : la protection des informations au centre de la gestion de cyberincidents ... 321
Préambule au chapitre 6 ... 321
I. Les informations et leur protection ... 322
A. Les informations ... 322
B. Les garde-fous ... 325
C. En résumé ... 326
II. La sécurité de l'information dans la LSI ... 326
A. Les mesures garantissant la sécurité de l'information ... 326
B. La classification d'informations ... 327
C. D'autres mesures ... 330
D. Une synthèse ... 331
III. La protection des données personnelles ... 331
A. Une remarque introductive ... 331
B. La distinction entre un organe fédéral et une responsable du traitement privée ... 332
C. Une responsable du traitement ou une sous-traitante ... 334
1. Les responsables du traitement et les sous-traitantes ... 334
2. L'Office fédéral de la cybersécurité ... 335
3. Les autres prestataires de gestion de cyberincidents ... 339
a. Les prestataires internes ou externes ... 339
b. La sous-traitance ... 341
D. La sécurité des données et des obligations s'en rapprochant ... 343
1. La sécurité des données ... 343
a. Les mesures de sécurité en général ... 343
b. L'impact de la sécurité des données lors d'un cyberincident ... 344
2. La protection des données dès la conception et par défaut ... 345
E. La coopération par la communication de données personnelles ... 346

1. Des généralités sur la communication de données personnelles ... 346
2. Les flux de communication sur le plan national pour l'OFCS 347
a. Les communications effectuées par l'office fédéral ... 347
b. Les données personnelles communiquées à l'OFCS ... 349
3. La communication de prestataires de gestion de cyberincidents d'autorités ... 350
4. La communication de données personnelles par les privées en Suisse ... 350
5. Les communications de données concernant des personnes morales ... 351
6. La communication de données personnelles à l'étranger ... 352
a. Les cas de figure et les normes à respecter ... 352
b. La communication avec une décision d'adéquation du Conseil fédéral ... 354
c. La communication sans décision d'adéquation du Conseil fédéral ... 355
d. La publication de données personnelles sur un site web 358
e. La question de l'importation de données personnelles ... 359
F. La surveillance ... 359
1. Les cas de figure ... 359
2. La surveillance des collaboratrices ... 360
G. Un survol d'autres dispositions pertinentes dans la gestion de cyberincidents ... 362
1. Le principe de proportionnalité ... 362
a. Des généralités ... 362
b. La minimisation de données ... 362
c. La conservation et la destruction de données ... 363
2. Le devoir d'information ... 364
3. Le respect des autres principes et obligations de protection des données ... 366
H. Les traitements illicites et les sanctions en cas de violations ... 367
1. La responsabilité civile des prestataires de gestion de cyberincidents ... 367
2. La responsabilité administrative pour l'OFCS ... 368
3. La responsabilité commune administrative ... 369
4. La responsabilité pénale fondée sur la LPD ... 371
a. Une limitation des violations analysées ... 371
b. La violation des devoirs de diligence ... 372
c. La violation du devoir de discrétion ... 372

I. Une synthèse ... 373
IV. La protection des secrets ... 374
A. L'intérêt de la question en pratique ... 374
B. Des exemples de secrets pertinents ... 375
1. Le secret de fonction ... 375
2. Le secret de fabrication et secret commercial ou d'affaires 377
3. Le secret professionnel ... 379
4. Le secret des télécommunications ... 381
5. D'autres secrets spécifiques ... 383
6. Les secrets contractuels ... 383
C. Des exemples de violations d'une obligation de garder le secret ... 384
1. La violation du secret de fonction ... 384
2. La violation du secret de fabrication et d'affaires ... 385
3. D'autres violations ... 389
D. Une synthèse ... 391
V. En pratique ... 392
A. De la théorie à la pratique ... 392
B. Les outils contractuels ... 393
1. Le périmètre ... 393
2. Les accords de confidentialité ... 395
3. L'utilisation du Traffic Light Protocol ... 395
C. Une synthèse ... 397
VI. Une conclusion au chapitre 6 ... 398

Chapitre 7 : une conclusion intermédiaire sur les lacunes observées en droit suisse ... 400
Préambule au chapitre 7 ... 400
I. Le cadre légal existant ... 401
A. Les trois domaines de la protection contre les cybermenaces 401
1. La cybersécurité des infrastructures critiques ... 401
2. La cybercriminalité et la cyberdéfense ... 404
B. La gestion de cyberincidents ... 404
C. Les autres domaines juridiques ... 405
D. En résumé ... 406
II. Les questions et les lacunes légales ... 406
A. Les lacunes et les questions traitées ... 406
1. La cybersécurité des infrastructures critiques ... 406
2. L'activité des prestataires de gestion de cyberincidents ... 408
B. Les lacunes et les questions laissées ouvertes ... 408

1. Quelques exemples de questions juridiques ... 408
2. Les autres lacunes et questionnements ... 409
C. En résumé ... 410
III. Une conclusion au chapitre 7 ... 411

Troisième Partie : les pistes réglementaires ... 413

Chapitre 8 : la nécessité de développer la réglementation ... 415
Préambule au chapitre 8 ... 415
I. Les contours ... 416
A. L'origine du besoin de réglementer ... 416
B. Un rappel des enjeux pour développer la réglementation ... 417
C. La limite des propositions ... 418
D. En résumé ... 418
II. Des hypothèses légales ... 419
A. Les angles d'approche ... 419
B. La responsabilisation des infrastructures critiques comme point de départ ... 420
C. La réglementation des prestataires de soutien ... 421
D. En résumé ... 422
III. Une conclusion au chapitre 8 ... 422

Chapitre 9 : la réglementation de la cybersécurité des infrastructures critiques ... 423
Préambule au chapitre 9 ... 423
I. La réglementation ponctuelle ... 424
A. L'alternative de la Cyberstratégie nationale ... 424
B. Un résumé de la réglementation existante ... 424
1. Les bases légales ... 424
2. Les réglementations non contraignantes ... 425
C. L'évolution à venir ... 425
1. La nécessité de se pencher sur toutes les infrastructures critiques ... 425
2. Les changements en cours ... 426
D. La mise en œuvre ... 427
1. La nécessité pour les secteurs de définir les champs d'application ... 427
2. Les exigences minimales ... 428
3. Le contrôle de la conformité aux réglementations ... 429
E. Une conclusion ... 431

1. En résumé ... 431
2. Les avantages ... 431
3. Les problèmes ... 432
II. La création d'une législation centralisée ... 433
A. La ratio legis ... 433
B. La compétence législative fédérale ... 434
1. Le principe de subsidiarité ... 434
2. Le respect de l'autonomie cantonale ... 435
a. Le principe de subsidiarité dans la Constitution ... 435
b. Les normes attributives de compétence actuellement utilisées ... 435
c. La sécurité comme fondement constitutionnel supplémentaire ... 437
(i) La notion de sécurité et la portée de l'art. 57 Cst. ... 437
(ii) La sécurité et la subsidiarité ... 440
3. Le respect d'une autonomie sectorielle ? ... 442
C. La forme de la législation centrale ... 443
1. La nécessité de disposer d'une loi fédérale ... 443
2. Le choix de la loi fédérale ... 445
a. La loi sur la sécurité de l'information ... 445
b. Une nouvelle loi ? ... 447
3. La possibilité de compléter la loi ... 448
a. L'ordonnance du Conseil fédéral ... 448
b. Une ordonnance de l'Office fédéral de la cybersécurité ? 449
c. D'autres actes d'exécution ... 451
D. Le contenu de la législation ... 453
1. Une question de densité normative ... 453
2. Le but, les définitions et le champ d'application ... 454
3. Les exigences minimales de cybersécurité ... 459
a. Le point de départ ... 459
b. La planification et la préparation ... 461
(i) L'approche fondée sur les risques et la planification ... 461
(ii) Les responsabilités ... 463
(iii) La sécurité de l'information et la sécurité informatique ... 466
(iv) Les autres mesures de la LSI ... 472
c. La détection ... 473
d. La réaction et les mesures post-incidents ... 474
e. Tout au long du processus : les communications et la documentation ... 477

f. Le renvoi à l'état de la technique ... 478
g. L'utilisation d'une annexe ? ... 479
4. Le contrôle de l'application de la législation ... 479
a. Les différents moyens de contrôler l'application de la législation ... 479
b. La certification ... 480
c. Les mesures d'exécution par l'Office fédéral de la cybersécurité ... 484
d. Les sanctions ... 485
E. Une conclusion sur la portée de cette solution ... 486
1. En résumé ... 486
2. Les conséquences positives ... 487
3. Les défis dans une perspective critique ... 488
III. Une conclusion au chapitre 9 ... 489

Chapitre 10: les solutions ciblant les prestataires de gestion de cyberincidents ... 492
Préambule au chapitre 10 ... 492
I. La réglementation des prestataires de gestion de cyberincidents ... 494
A. La raison à l'origine d'une réglementation de ces prestations 494
1. La double casquette des prestataires de gestion de cyberincidents ... 494
2. Des fournisseuses de services informatiques ... 494
3. Les différentes structures ... 495
4. La prise en compte des différents services et des différentes prestations ... 496
B. La compétence constitutionnelle de la Confédération à légiférer ... 497
C. Le choix des normes ... 498
1. La loi ... 498
2. Les actes d'exécution ... 499
D. Le contenu de la réglementation ... 500
1. Les conditions matérielles et personnelles de l'exercice ... 500
2. La réglementation de l'exercice de l'activité ... 501
a. L'obligation de cybersécurité dans les prestations ... 501
(i) L'obligation générale de cybersécurité ... 501
(ii) Quelques exemples de concrétisation de l'obligation ... 504
(iii) Le respect du principe de proportionnalité ... 506
b. L'obligation de transparence ... 506

c. L'examen d'autres obligations ... 507
(i) Une obligation de collaboration accrue ? ... 507
(ii) L'obligation de souscrire à une assurance responsabilité civile ? ... 509
(iii) L'exemple particulier des pirates éthiques ... 510
E. Les mécanismes de contrôle ... 512
1. Les instruments pour l'ensemble des infrastructures critiques ... 512
2. Les obligations d'annonce ou l'autorisation ... 512
F. Une conclusion ... 514
1. Laisser le temps au temps ... 514
2. En résumé, une réglementation minimaliste ... 515
3. Une portée plus large ... 516
a. Les technologies impactées ... 516
b. L'intelligence artificielle ... 516
c. L'internet des objets ... 517
d. L'informatique en nuage ... 517
e. La chaîne d'approvisionnement ... 519
II. La réglementation de l'activité de l'OFCS ... 519
A. La nécessité d'une réglementation exclusive ... 519
B. Le principe de la légalité ... 520
1. Un rappel de la situation actuelle ... 520
2. L'OFCS, son équipe technique et le principe de la légalité ... 521
C. Le droit européen comme point de comparaison ... 522
1. Les autorités de la Directive SRI2 et leurs compétences principales ... 522
2. La difficulté de comparer les deux systèmes ... 525
D. Les changements nécessaires ... 526
1. Les compétences de soutien ... 526
a. Les compétences générales, préventives et détectives ... 526
b. Les compétences réactives ... 527
c. Le rôle de l'office dans les échanges d'informations ... 530
2. La limite entre soutien et surveillance : les compétences « réglementaires » ... 532
3. Les compétences de surveillance ... 533
4. Les autres compétences prévues par le droit européen ... 536
E. En conclusion : des perspectives d'avenir ... 536
III. Une conclusion au chapitre 10 ... 538

Conclusion générale ... 543

Table des abréviations et des locutions latines

AES	Association des entreprises électriques suisses
AF	Assemblée fédérale
AIEA	Agence internationale d'énergie atomique
ANSSI	Agence nationale [française] de la sécurité des systèmes d'information
al.	alinéa(s)
a[loi]	ancienne [loi]
AR	*Kanton Appenzell Ausserrhoden* (= canton d'Appenzell Rhodes-Extérieures)
armasuisse	Office fédéral de l'armement
art.	article(s)
ATF	Recueil officiel des arrêts du Tribunal fédéral suisse
AVS	assurance-vieillesse et survivants
BAC	Base d'aide au commandement
BCR	*Binding Corporate Rules* (= règles d'entreprise contraignantes)
BE	canton de Berne
bGS	*Systematische Sammlung Appenzell Auserrhoden*
BGS	*Systematische Sammlung Kanton Zug*
BLV	Base législative vaudoise
BNS	Banque nationale suisse
BR	*Bündner Rechtsbuch*
BS	*Kanton Basel-Stadt* (= canton de Bâle-Ville)
BSI	*Bundesamt für Sicherheit in der Informationstechnik* (= Office fédéral [allemand] pour la sécurité de l'information)
BSK	*Basler Kommentar* (= Commentaire bâlois)
c.	considérant(s)
CA	Conférence des achats de la Confédération
CCDJP	Conférence des directrices et directeurs des départements cantonaux de justice et police
CCMP	Centre de compétence des marchés publics de la Confédération
CCT	clauses contractuelles types
CDS	Conférence des directrices et directeurs cantonaux de la santé
CEPD	Comité européen de la protection des données

CENAL	Centrale nationale d'alarme
CERT	*Computer Emergency Response Team(s)* (= équipe(s) d'intervention informatique d'urgence)
CERT/CC	*CERT Coordination Center* (= centre de coordination de l'équipe d'intervention d'urgence en matière de sécurité informatique)
CF	Conseil fédéral
cf.	*confer*
CFF	Chemins de fer fédéraux
Cff	Contrôle fédéral des finances
CG	conditions générales
ch.	chiffre(s)
ChF	Chancellerie fédérale
CHF	Francs suisses
CIO	*Chief Information Officer* (= directrice des systèmes d'information)
CISO	*Chief Information Security Officer* (= directrice de la sécurité des systèmes d'information)
CJ/GE	Cour de justice du canton de Genève
CJUE	Cour de justice de l'Union européenne
CNAI	Réseau suisse de compétences en intelligence artificielle
COBIT	*Control Objectives for Information and related Technology* (= Objectifs de Contrôle de l'Information et des Technologies associées)
CR	Commentaire romand
CSIRT	*Computer Security Incident Response Team(s)* (= équipe(s) d'intervention en cas d'incident lié à la sécurité informatique)
CSN	Cyberstratégie nationale
CTI	*cyber threat intelligence (= renseignement sur la cybermenace)*
CYD Campus	*Cyber-Defence Campus* d'armasuisse
Délséc	Délégation du CF pour la sécurité
DETEC	Département fédéral de l'environnement, des transports, de l'énergie et de la communication
DDoS	*distributed denial of service* (= déni de service distribué)
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DEFR	Département fédéral de l'économie, de la formation et de la recherche
DFAE	Département fédéral des affaires étrangères
DFF	Département fédéral des finances
DFJP	Département fédéral de justice et police

DGNSI	Direction générale du numérique et des systèmes d'information de l'État de Vaud
DLP	*data loss prevention* (= prévention de perte de données)
DoS	*denial of service* (= déni de service)
DSID	Déléguée à la sécurité informatique
DSI	Direction de la sécurité informatique de l'État de Vaud
DSIO	Déléguée à la sécurité informatique des unités administratives
éd.	éditeur/éditrice
éds	éditeurs/éditrices
EEE	Espace économique européen
EGC	*Europan Government CERT group* (= groupe des CERT des gouvernements européens)
ElCom	Commission fédérale de l'électricité
ENISA	*European Union Agency for Cybersecurity* (= Agence européenne chargée de la sécurité des réseaux et de l'information)
EPFZ	École polytechnique fédérale de Zurich
et al.	*et alii* (= et autres)
etc.	*et caetera* (= et tout le reste)
ETSI	Institut européen des normes de télécommunication
EUCC	*European Common Criteria-based cybersecurity certification scheme* (= système européen de certification de la cybersécurité fondé sur des critères communs)
fedpol	Office fédéral de la police
FF	Feuille fédérale
FINMA	Autorité fédérale de surveillance des marchés financiers
FIRST	*Forum of Incident Response and Security Teams* (= Forum des équipes de sécurité et de réponse aux incidents)
FMH	*Foederatio Medicorum Helveticorum*
FR	canton de Fribourg
FS-CSC	*Swiss Financial Sector Cyber Security Centre* (= Centre de cybersécurité pour le secteur financier suisse)
GE	canton de Genève
GovCERT	*Swiss Government Computer Emergency Response Team* (= équipe d'intervention en cas d'urgence informatique)
GR	*Kanton Graubünden* (= canton des Grisons)
GS	Groupe sécurité
GS	*Systematische Sammlung Kanton Appenzell Innerrhoden*
ICS-CERT	*US Industrial Control Systems Cyber Emergency Response Team* (= équipe d'intervention informatique pour les systèmes de contrôle industriels américains)

IDE	numéro(s) unique(s) d'identification des entreprises
IdO	Internet des objets
IDPS	*intrusion detection and prevention system(s)* (= système(s) de détection et de prévention d'intrusion)
IDS	*intrusion detection system* (= système de détection d'intrusion)
IEC	*International Electrotechnical Commission* (= Commission internationale électrotechnique)
IFSN	Inspection fédérale de la sécurité nucléaire
IIdO	Internet industriel des objets
Inventaire PIC	Méthode d'élaboration de l'Inventaire des infrastructures critiques
IOA	*indicators of attacks* (= indicateurs d'attaques)
IOC	*indicators of compromise* (= indicateurs de compromission)
IP	*Internet Protocol* (= protocole Internet)
IPI	Institut Fédéral de la Propriété Intellectuelle
ISAC	*Information Sharing and Analysis Centre(s)* (= centre(s) de partage et d'analyse d'informations)
ISACA	*Information Systems Audit and Control Association* (= Association pour l'audit et le contrôle des systèmes d'information)
ISO	*International Organization for Standardization* (= Organisation internationale de normalisation)
IT	*Information Technology* (= technologie de l'information)
JO	Journal officiel de l'Union européenne
litt.	*littera* (= lettre(s))
LS	*Loseblattsammlung*
LU	*Kanton Luzern* (= canton de Lucerne)
MELANI	Centrale d'enregistrement et d'analyse pour la sûreté de l'information
METAS	Institut fédéral de métrologie
MilCERT	*Military Computer Emergency Response Team* (= CERT militaire)
MPC	Ministère public de la Confédération
N	numéro(s)
NCSC	Centre national pour la cybersécurité
NDA	*non-disclosure agreement* (= accord de confidentialité)
NE	canton de Neuchâtel
NEDIK	*Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung* (= Réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique)
NIST	*National Institute of Standards and Technology* (= Institut national [américain] des normes et de la technologie)

NTC	Institut national de test pour la cybersécurité
OCDE	Organisation de coopération et de développement économiques
OEWG	Groupe de travail ouvert
OFAC	Office fédéral de l'aviation civile
OFAE	Office fédéral pour l'approvisionnement économique du pays
OFCOM	Office fédéral de la communication
OFCS	Office fédéral de la cybersécurité
OFDF	Office fédéral des douanes et de la sécurité des frontières
OFEN	Office fédéral de l'énergie
OFIT	Office fédéral de l'informatique et de la télécommunication
OFJ	Office fédéral de la justice
OFPP	Office fédéral de la protection de la population
OFSP	Office fédéral de la santé publique
OFT	Office fédéral des transports
OGD	*Open Government Data* (= données publiques en libre accès)
OIC	*Operation Information Center (= centre d'information sur les opérations)*
ONG	Organisation non gouvernementale
OSINT	*Open Source Intelligence* (= renseignements de sources ouvertes)
OT	*Operational Technology* (= technologie opérationnelle)
p.	page(s)
PACD	Plan d'action Cyberdéfense
par.	paragraphe(s)
PFPDT	Préposée fédérale à la protection des données et à la transparence
PIC	Protection des infrastructures critiques
PICSEL	Plateforme d'Information de la Criminalité Sérielle en Ligne
PME	Petite(s) ou moyenne(s) entreprise(s)
pp.	pages
PPP	Partenariat(s) public(s)-privé(s)
PSC	Prévention suisse de la Criminalité
PSIRT	*Product Security Incident Response Team(s)* (= équipe(s) d'intervention en cas d'incident relatif à la sécurité des produits)
RB	*Erlass-Sammlung Kanton Thurgau*
RC3	*Cyber Competence Center* (= Centre régional de compétences cyber)
REE	numéro(s) d'enregistrement non significatif
RSB	Recueil systématique du canton de Berne
RSDA	Revue suisse de droit des affaires et du marché financier

RSF	Recueil systématique de l'État de Fribourg
rsGE	Recueil systématique de la législation genevoise
RSN	Recueil systématique de la législation neuchâteloise
RSSI	Responsable de la sécurité des systèmes d'information
rev.	révision
s.	suivant(e)
SaS	Service d'accréditation suisse
SCADA	*Supervisory Control and Data Acquisition* (= système de contrôle et d'acquisition de données)
SCOCI	Service national de coordination de la lutte contre la criminalité sur Internet
SCI	systèmes de contrôle industriels
Service SCPT	Service de surveillance de la correspondance par poste et télécommunication
SECO	Secrétariat d'État à l'économie
SEPOS	Secrétariat d'État à la politique de sécurité
SG	*Systematische Gesetzsammlung*
SG-DDPS	Secrétariat général du DDPS
SG-DFF	Secrétariat général du DFF
SGSI	système de gestion de la sécurité de l'information
SH	*Kanton Schaffhausen* (= canton de Schaffhouse)
SHR	*Schauffauser Rechtsbuch*
SIPD	sûreté de l'information et de protection des données
SITel	service de l'informatique et des télécommunications
SIEM	*security information and event management* (= système de gestion de l'information et des événements en matière de sécurité)
SITeL	Service fribourgeois de l'informatique et des télécommunications
SLA	*service level agreement* (= accord de niveau de service)
SMSI	système de management de la sécurité de l'information (= SGSI)
SNPC	Stratégie nationale de protection de la Suisse contre les cyberrisques
SNV	*Schweizerische Normen-Vereinigung* (= Association Suisse de Normalisation)
SOC	*Security Operation Center(s)* (= centre(s) des opérations de sécurité)
SPHN	*Swiss Personalized Health Network*
SRC	Service de renseignement de la Confédération
SRL	*Systematische Rechtssamlung Luzern*
ss	suivant(e)s

SSIGE	Société Suisse de l'Industrie du Gaz et des Eaux
Stratégie PIC	Stratégie nationale de protection des infrastructures critiques
Swissmedic	Institut suisse des produits thérapeutiques
SZ	*Kanton Schwyz* (= canton de Schwytz)
TAF	Tribunal administratif fédéral
TF	Tribunal fédéral
TG	*Kanton Thurgau* (= canton de Thurgovie)
TIC	Technologies de l'information et de la communication
TLP	*Traffic Light Protocol*
TNI	Transformation numérique et gouvernance de l'informatique
TTP	*tactics, techniques, and procedures* (= tactiques, techniques et procédures)
UE	Union européenne
UIT	Union internationale des télécommunications
UNIDIR	*United Nations Institute for Disarmament Research* (= Institut des Nations Unies pour la recherche sur le désarmement)
UNIL	Université de Lausanne
UPIC	Unité de pilotage informatique de la Confédération
USA	*United States of America* (= États-Unis d'Amérique)
USIC	Unité de stratégie informatique de la Confédération
VBS	*Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport* (= DDPS)
VD	canton de Vaud
vol.	volume
VPN	*Virtual Private Network(s)* (= réseau(x) privé(s) virtuel(s))
WEF	*World Economic Forum* (= Forum économique mondial)
ZG	*Kanton Zug* (= canton de Zoug)
ZH	*Kanton Zürich* (= canton de Zurich)

Table des réglementations citées

Lois fédérales

CC	Code civil suisse du 10 décembre 1907 (RS 210)
CO	Loi fédérale du 30 mars 1911 complétant le Code civil suisse (Livre cinquième : Droit des obligations ; RS 220)
CP	Code pénal suisse du 21 décembre 1937 (RS 311.0)
CPC	Code de procédure civile du 19 décembre 2008 (RS 272)
CPM	Code pénal militaire du 13 juin 1927 (RS 321.0)
CPP	Code de procédure pénale suisse du 5 octobre 2007 (Code de procédure pénale ; RS 312.0)
Cst.	Constitution fédérale de la Confédération suisse du 18 avril 1999 (RS 101)
DPA	Loi fédérale du 22 mars 2974 sur le droit pénal administratif (RS 313.0)
EIMP	Loi fédérale du 29 mars 1981 sur l'entraide internationale en matière pénale (Loi sur l'entraide pénale internationale ; RS 351.1)
LAAM	Loi fédérale du 3 février 1995 sur l'armée et l'administration militaire (Loi sur l'armée ; RS 510.10)
LAMal	Loi fédérale du 18 mars 1994 sur l'assurance-maladie (RS 832.10)
LAP	Loi fédérale du 17 juin 2016 sur l'approvisionnement économique du pays (Loi sur l'approvisionnement du pays ; RS 531)
LApEl	Loi fédérale du 23 mars 2007 sur l'approvisionnement en électricité (RS 734.7)
LAr	Loi fédérale du 26 juin 1998 sur l'archivage (RS 152.1)
LB	Loi fédérale du 8 novembre 1934 sur les banques et les caisses d'épargnes (Loi sur les banques ; RS 952.0)
LBI	Loi fédérale du 25 juin 1954 sur les brevets d'invention (Loi sur les brevets ; RS 232.14)
LBN	Loi fédérale du 3 octobre 2003 sur la Banque nationale suisse (Loi sur la Banque nationale ; RS 951.11)
LCA	Loi fédérale du 2 avril 1908 sur le contrat d'assurance (Loi sur le contrat d'assurance ; RS 221.229.1)
LCart	Loi fédérale du 6 octobre 1995 sur les cartels et autres restrictions à la concurrence (Loi sur les cartels ; RS 251)

LCB	Loi fédérale du 13 décembre 1996 sur le contrôle des biens utilisables à des fins civiles et militaires, des biens militaires spécifiques et des biens stratégiques (Loi sur le contrôle des biens ; RS 946.202)
LCD	Loi fédérale du 19 décembre 1986 contre la concurrence déloyale (RS 241)
LCdF	Loi fédérale du 20 décembre 1957 sur les chemins de fer (RS 742.101)
LDA	Loi fédérale du 9 octobre 1992 sur le droit d'auteur et les droits voisins (Loi sur le droit d'auteur ; RS 231.1)
LDAI	Loi fédérale du 20 juin 2014 sur les denrées alimentaires et les objets usuels (Loi sur les denrées alimentaires ; RS 817.0)
LDEP	Loi fédérale du 19 juin 2015 sur le dossier électronique du patient (RS 816.1)
LDét	Loi fédérale du 8 octobre 1999 sur les mesures d'accompagnement applicables aux travailleurs détachés et aux contrôles des salaires minimaux prévus par les contrats-types de travail (Loi sur les travailleurs détachés ; RS 823.20)
LDIP	Loi fédérale du 18 décembre 1987 sur le droit international privé (RS 291)
LEFin	Loi fédérale du 15 juin 2018 sur les établissements financiers (RS 954.1)
LEHE	Loi fédérale du 30 septembre 2011 sur l'encouragement des hautes écoles et de la coordination dans le domaine suisse des hautes écoles (RS 414.20)
LEne	Loi fédérale du 30 septembre 2016 sur l'énergie (RS 730.0)
LEp	Loi fédérale du 28 septembre 2012 sur la lutte contre les maladies transmissibles de l'homme (Loi sur les épidémies ; RS 818.101)
LENu	Loi fédérale du 21 mars 2003 sur l'énergie nucléaire (RS 732.1)
LFINMA	Loi fédérale du 22 juin 2007 sur l'Autorité fédérale de surveillance des marchés financiers (RS 956.1)
LHID	Loi fédérale du 14 décembre 1990 sur l'harmonisation des impôts directs des cantons et des communes (RS 642.14)
LIE	Loi fédérale du 24 juin 1902 concernant les installations électriques à faible et à fort courant (Loi sur les installations électriques ; RS 734.0)
LIFD	Loi fédérale du 14 décembre 1990 sur l'impôt fédéral direct (RS 642.11)

LIMF	Loi fédérale du 19 juin 2015 sur les infrastructures des marchés financiers et le comportement sur le marché en matière de négociation de valeurs mobilières et de dérivés (Loi sur l'infrastructure des marchés financiers ; RS 958.1)
LMETA	Loi fédérale du 17 mars 2023 sur l'utilisation de moyens électroniques pour l'exécution des tâches des autorités (RS 172.019)
LMP	Loi fédérale du 21 juin 2019 sur les marchés publics (RS 172.056.1)
LMSI	Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (RS 120)
LNMPV	Loi fédérale du 23 septembre 1953 sur la navigation maritime sous pavillon suisse (RS 747.30)
LOGA	Loi fédérale du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (RS 172.010)
Loi sur les EPF	Loi fédérale du 4 octobre 1991 sur les écoles polytechniques fédérales (RS 414.110)
LPD	Loi fédérale du 25 septembre 2020 sur la protection des données (RS 235.1)
LPE	Loi fédérale du 7 octobre 1983 sur la protection de l'environnement (RS 814.01)
LPers	Loi fédérale du 24 mars 2000 sur le personnel de la Confédération (RS 172.220.1)
LPGA	Loi fédérale du 6 octobre 2000 sur la partie générale du droit des assurances sociales (RS 830.1)
LPMA	Loi fédérale du 18 décembre 1998 sur la procréation médicalement assistée (RS 810.11)
LPO	Loi fédérale du 17 décembre 2010 sur la poste (RS 783.0)
LPPCi	Loi fédérale du 20 décembre 2019 sur la protection de la population et sur la protection civile (RS 520.1)
LPTh	Loi fédérale du 15 décembre 2000 sur les médicaments et les dispositifs médicaux (Loi sur les produits thérapeutiques ; RS 812.21)
LRCF	Loi du 14 mars 1958 sur la responsabilité de la Confédération, des membres de ses autorités et de ses fonctionnaires (Loi sur la responsabilité ; RS 170.32)
LRens	Loi fédérale du 25 septembre 2015 sur le renseignement (RS 121)
LRFP	Loi fédérale du 18 juin 1993 sur la responsabilité du fait des produits (RS 221.112.944)
LSA	Loi fédérale du 17 décembre 2004 sur la surveillance des entreprises d'assurance (Loi sur la surveillance des assurances ; RS 961.01)

LSCPT	Loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication (RS 780.1)
LSE	Loi fédérale 6 octobre 1989 sur le service de l'emploi et la location de services (RS 823.11)
LSI	Loi fédérale du 18 décembre 2020 sur la sécurité de l'information au sein de la Confédération (Loi sur la sécurité de l'information ; RS 128)
LSIP	Loi fédérale du 13 juin 2008 sur les systèmes d'information de la police de la Confédération (RS 361)
LSPro	Loi fédérale du 12 juin 2009 sur la sécurité des produits (RS 930.11)
LTC	Loi fédérale du 30 avril 1997 sur les télécommunications (RS 784.10)
LTrans	Loi fédérale du 17 décembre 2004 sur le principe de la transparence dans l'administration (RS 152.3)
LTV	Loi fédérale du 20 mars 2009 sur le transport de voyageurs (RS 745.1)
LTVA	Loi fédérale du 12 juin 2009 régissant la taxe sur la valeur ajoutée (Loi sur la TVA ; RS 641.20)
PA	Loi fédérale du 20 décembre 1968 sur la procédure administrative (RS 172.021)
SCSE	Loi fédérale du 18 mars 2016 sur les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques (Loi sur la signature électronique ; RS 943.03)

Ordonnances fédérales

OAEP	Ordonnance du CF du 10 mai 2017 sur l'approvisionnement économique du pays (RS 531.11)
OAG	Ordonnance du CF du 25 octobre 2017 sur la sécurité des appareils à gaz (Ordonnance sur les appareils à gaz ; RS 930.116)
OApEl	Ordonnance du CF du 14 mars 2008 sur l'approvisionnement en électricité (RS 734.71)
OAsc	Ordonnance du CF du 25 novembre 2015 sur la sécurité des ascenseurs (Ordonnance sur les ascenseurs ; RS 930.112)
OCB	Ordonnance du CF du 3 juin 2016 sur le contrôle des biens utilisables à des fins civiles et militaires, des biens militaires spécifiques et des biens stratégiques (Ordonnance sur le contrôle des biens ; RS 946.202.1)

OCMil Ordonnance du CF du 30 janvier 2019 sur la cyberdéfense militaire (RS 510.921)

OCPD Ordonnance du CF du 31 août 2022 sur les certifications en matière de protection des données (RS 235.13)

OCSPN Ordonnance du CF du 9 juin 2006 sur les contrôles de sécurité relatifs aux personnes dans le domaine des installations nucléaires (RS 732.143.3)

ODAIOUs Ordonnance du CF du 16 décembre 2016 sur les denrées alimentaires et les objets usuels (RS 817.02)

OdelO Ordonnance du CF du 25 mai 2011 sur les principes et les délais d'ordre relatifs aux procédures d'autorisation (Ordonnance sur les délais d'ordre ; RS 172.010.14)

ODEP Ordonnance du CF du 22 mars 2017 sur le dossier électronique du patient (RS 816.11)

ODEP-DFI Ordonnance du DFI du 22 mars 2017 sur le dossier électronique du patient (RS 816.111)

ODI Ordonnance du CF du 5 novembre 2014 sur les domaines Internet (ODI ; RS 784.104.2)

ODim Ordonnance du CF du 1er juillet 2020 sur les dispositifs médicaux (RS 812.213)

ODP Ordonnance du CF du 24 mai 1978 sur les droits politiques (RS 161.11)

OEIT Ordonnance du CF du 17 décembre 2014 sur les enquêtes de sécurité en cas d'incident dans le domaine des transports (RS 742.161)

OENu Ordonnance du CF du 10 décembre 2004 sur l'énergie nucléaire (RS 732.11)

OHyRiENu-DETEC — Ordonnance du DETEC du 16 avril 2008 sur les hypothèses de risque et sur les mesures de sûreté pour les installations et les matières nucléaires (RS 732.112.1)

OIBT Ordonnance du CF du 7 novembre 2001 sur les installations électriques à basse tension (Ordonnance sur les installations à basse tension ; RS 734.27)

OIT Ordonnance du CF du 25 novembre 2015 sur les installations de télécommunication (RS 784.101.2)

OLT 1 Ordonnance 1 du CF du 10 mai 2000 relative à la loi sur le travail (RS 822.111)

OLT 3 Ordonnance 3 du CF du 18 août 1993 relative à la loi sur le travail (RS 822.113)

OMach Ordonnance du CF du 2 avril 2008 sur la sécurité des machines (Ordonnance sur les machines ; RS 819.14)
OMoD Ordonnance du CF du 22 juin 2005 sur les mouvements de déchets (RS 814.610)
OOIT Ordonnance du 26 mai 2016 de l'OFCOM sur les installations de télécommunication (RS 784.101.21)
OPAM Ordonnance du CF du 27 février 1991 sur la protection contre les accidents majeurs (Ordonnance sur les accidents majeurs ; RS 814.012)
OPCo Ordonnance du CF du 27 août 2014 sur les produits de construction (RS 933.01)
OPDo Ordonnance du CF du 31 août 2022 sur la Loi fédérale sur la protection des données (RS 235.11)
OPers Ordonnance du CF du 3 juillet 2001 sur le personnel de la Confédération (RS 172.220.111.3)
OProP Ordonnance du CF du 11 novembre 2020 sur la protection de la population (RS 520.12)
ORaP Ordonnance du CF du 26 avril 2017 sur la radioprotection (RS 814.501)
ORAT Ordonnance sur les ressources d'adressage dans le domaine des télécommunications (RS 784.104)
Ordonnance sur courant faible — Ordonnance du CF du 30 mars 1994 sur les installations électriques à courant faible (RS 734.1)
Ordonnance sur courant fort — Ordonnance du CF du 30 mars 1994 sur les installations électriques à courant fort (RS 734.1)
Ordonnance RIPOL — Ordonnance du CF du 26 octobre 2016 sur le système de recherches informatisées de police (RS 361.0)
Org-DDPS Ordonnance du CF du 7 mars 2003 sur l'organisation du Département fédéral de la défense, de la protection de la population et des sports (RS 172.214.1)
Org DEFR Ordonnance du CF du 14 juin 1999 sur l'organisation du Département fédéral de l'économie, de la formation et de la recherche (RS 172.216.1)
Org DFF Ordonnance du CF du 17 février 2010 sur l'organisation du Département fédéral des finances (RS 172.215.1)
Org-OMP Ordonnance du CF du 24 octobre 2012 sur l'organisation des marchés publics de l'administration fédérale (Org-OMP ; RS 172.056.15)
OSCPT Ordonnance du CF du 15 novembre 2017 sur la surveillance de la communication par poste et télécommunication (RS 780.11)

OSI	Ordonnance du CF du 8 novembre 2023 sur la sécurité de l'information dans l'administration fédérale et l'armée (Ordonnance sur la sécurité de l'information ; RS 128.1)
OSITC	Ordonnance du CF du 4 juin 2021 concernant les prescriptions de sécurité pour les installations de transport par conduites (Ordonnance sur la sécurité des installations de transport par conduite ; RS 746.12)
OSJo	Ordonnance du DFI sur la sécurité des jouets (Ordonnance sur les jouets ; RS 817.023.11)
OST	Ordonnance du CF du 9 mars 2007 sur les services de télécommunication (RS 784.101.1)
OTNI	Ordonnance du CF du 25 novembre 2020 sur la coordination de la transformation numérique et la gouvernance de l'informatique dans l'administration fédérale (RS 172.010.58)
OTUIC	Ordonnance sur le traitement des données personnelles et des données des personnes morales lors de l'utilisation de l'infrastructure électronique de la Confédération (RS 172.010.442)
OUMR	Ordonnance du CF du 26 avril 2017 sur l'utilisation des matières radioactives (RS 814.554)
OVotE	Ordonnance de la ChF du 25 mai 2022 sur le vote électronique (RS 161.116)

Bases légales abrogées

aLPD	Ancienne loi fédérale du 19 juin 1992 sur la protection des données (RO 1993 1945)
aOLPD	Ancienne ordonnance du CF du 14 juin 1993 relative à la Loi fédérale sur la protection des données (OLPD ; RO 1993 1962)
aOPCy	Ancienne ordonnance du CF du 27 mai 2020 sur la protection contre les cyberrisques dans l'administration fédérale (Ordonnance sur les cyberrisques ; RO 2020 2107)
aOPri	Ancienne ordonnance du CF du 4 juillet 2007 sur la protection des informations (RO 2007 3401)
aOIAF	Ancienne ordonnance du CF du 9 décembre 2011 sur l'information et la télécommunication dans l'administration fédérale (RO 2016 1783)

Conventions intercantonales et Conventions entre cantons et Confédération

CES — Concordat du 18 octobre 1996 sur les entreprises de sécurité

CL — Convention de Lugano du 30 octobre 2007 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (RS 0.275.12)

Convention TIP — Convention du 2 septembre 2020 entre la Confédération et les cantons sur l'harmonisation et la mise à disposition commune de la technique et de l'informatique policières en Suisse (RS 367.1)

Lois cantonales

Behördenportalgesetz-BS — *Basel-Stadt Gesetz über ein zentrales elektronisches Behördenportal* (SG 153.300)

eGovG-AR — *Appenzell A.Rh. Gesetz über eGovernement und Informatik* (bGS 142.3)

IDG-ZH — *Zürcher Gesetz über die Information und den Datenschutz* (LS 170.4)

LAeL-GE — Loi genevoise du 23 septembre 2016 sur l'administration en ligne (rsGE B 4 23)

LArch-VD — Loi vaudoise du 14 juin 2011 sur l'archivage (BLV 432.11)

LCyb-FR — Loi fribourgeoise du 18 décembre 2020 sur la cyberadministration (RSF 184.1)

LGSU-NE — Loi neuchâteloise sur le guichet sécurisé unique du 28 septembre 2004 (RSN 150.40)

LPol-VD — Loi vaudoise du 17 novembre 1975 sur la police cantonale (BLV 133.11)

LPrD-FR — Loi fribourgeoise du 25 novembre 1994 sur la protection des données (RSF 17.1)

LPrD-VD — Loi vaudoise du 11 septembre 2007 sur la protection des données personnelles (BLV 172.65)

LPrDS-VD — Loi vaudoise sur la protection des données personnelles dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal (BLV 172.68)

LUL-VD — Loi vaudoise du 6 juin 2004 sur l'Université de Lausanne (BLV 414.11)

Ordonnances et règlements cantonaux

E-GovV-SH *Schaffhausen Vereinbarung vom 9. und 16. November 2010 über die E-Government- und Informatikstrategie sowie den gemeinsamen Informatikbetrieb* (SHR 172.601)

Geschäftsordnung Information und Datenschutz-BS — Basel-Stadt Geschäftsordnung des Regierungsrates vom 27. September 2011 über die Information und den Datenschutz (SG 153.280)

IKTV-GR *Graubünden Verordnung vom 19. November 2019 über die Informations- und Kommunikationstechnik in der kantonalen Verwaltung* (BR 170.500)

InfoBeschluss-AI — Appenzell I.Rh. Standeskommissionsbeschluss vom 18. Dezember 2012 über die Informatiknutzung (GS 172.315)

Informatiksicherheitsverordnung-LU — Luzerner Verordnung vom 22. November 2016 über die Informatiksicherheit und über die Nutzung von Informatikmitteln (SRL Nr. 26b)

ISV-BS *Basel-Stadt Verordnung vom 13. Dezember 2016 über die Informationssicherheit* (ISV-BS ; SG 153.320)

ISV-SH *Schaffhausen Verordnung vom 2. Dezember 2014 betreffend Informatiksicherheit* (*Informatiksicherheitsverordnung* ; SHR 174.102)

IKTV-SZ *Schwyz Verordnung vom 1. September 2015 über die Informations- und Kommunikations-Technologie* (SRSZ 143.113)

ITV-TG *Thurgau Informatikverordnung* (RB 172.31)

ITV-ZG *Zug Informatikverordnung* (BGS 153.53)

IVSV-ZH *Zürcher Verordnung über die Informationsverwaltung und -sicherheit* (LS 170.8)

OTIC-BE Ordonnance bernoise sur les technologies de l'information et de la communication de l'administration cantonale (RSB 152.042)

OD SIPD-BE Ordonnance bernoise de Direction du 3 janvier 2011 concernant la sûreté de l'information et la protection des données (RSB 152.040.2)

ORCDo-FR Ordonnance fribourgeoise du 24 juin 2019 concernant la mise en œuvre du Référentiel cantonal de données de personnes, organisations et nomenclatures (projet pilote ; RSF 184.16)

RIC-VD Règlement vaudois du 21 janvier 2009 relatif à l'informatique cantonale (BLV 172.62.1)

ROGSIC-GE Règlement genevois du 26 juin 2013 sur l'organisation et la gouvernance des systèmes d'information et de communication (rsGE B 4 23.03)

RSD-FR	Règlement fribourgeois du 29 juin 1999 sur la sécurité des données personnelles (RSF 17.15)

Bases légales en cours d'élaboration

nLMP	Loi fédérale sur les marchés publics, modification du 29 septembre 2023 (FF 2023 2296)
LSI2	Loi fédérale sur la sécurité de l'information au sein de la Confédération, modification du 29 septembre 2023 (FF 2023 2296)
LSIC-BE	Projet de loi bernoise sur la sécurité de l'information et la cybersécurité (ACE N 873)
P-OCyS	Projet d'Ordonnance sur la cybersécurité

Réglementations étrangères et internationales

BSIG-D	*Deutsches Gesetz vom 14.08.2009 über das Bundesamt für Sicherheit in der Informationstechnik*
CAAS	Convention d'application de l'Accord de Schengen du 16 juin 1985 entre les Gouvernements des États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes (Convention d'application du 19 juin 1990 de l'Accord de Schengen)
CAI	Convention du Conseil de l'Europe sur la conception, le développement et l'utilisation des systèmes d'intelligence artificielle qui se fonde sur les normes du Conseil de l'Europe en matière de droits de l'homme, de démocratie et d'État de droit et est propice à l'innovation, conformément aux décisions pertinentes du Comité des Ministres [En cours], 15 mars 2024
CCC	Convention du 23 novembre 2001 sur la cybercriminalité (Convention de Budapest ; RS 0.311.43)
CEDH	Convention du 4 novembre 1950 de sauvegarde des droits de l'homme et des libertés fondamentales (RS 0.101)
CEEJ	Convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959 (RS 0.351.1)
CEExtr	Convention européenne d'extradition du 13 décembre 1957 (RS 0.353.1)
Convention 108+	Convention modernisée pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 18 mai 2018 (CM/Inf(2018)15-final)

Convention de Palerme	Convention des Nations Unies du 15 novembre 2000 contre la criminalité transnationale organisée (RS 0.311.54)
Directive SRI	Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant les mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194, 19.7.2016, p. 1)
Directive SRI2	Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1149 (JO L 333, 27.12.2022, p. 80)
DSA	Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (Règlement sur les services numériques, *Digital Services Act*) (JO L 277, 27.10.2022, p. 1)
AI-Act	Règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (Législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union (*Artificial Intelligence Act*) (JO L 2024/1689, 12.7.2024)
CRA	Règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020 (Loi sur la cyberrésilience, *Cyber Resilience Act*) (COM/2022/454 final)
RAC-UE	Règlement d'exécution (UE) 2015/1018 de la Commission du 29 juin 2015 établissant une liste classant les événements dans l'aviation civile devant être obligatoirement notifiés conformément au règlement (UE) nº376/2014 du Parlement européen et du Conseil (JO L 163, 30.6.2015, p. 1)
RDM	Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux (JO L 117, 5.5.2017, p. 1)
RGPD	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données) (JO L 119, 4.5.2016, p. 1)

Règlement sur la cybersécurité – Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) 526/2013 (JO L 151, 7.6.2019, p. 15)

Directives et autres normes fédérales

ASSOCIATION DES ENTREPRISES ÉLECTRIQUES SUISSES

- *Directives pour la sécurité des données des systèmes de mesure intelligents pour la certification et l'exploitation de systèmes de mesure intelligents,* Recommandation de la branche pour le marché suisse de l'électricité, 24 octobre 2018 (citée : AES, *Directives pour la sécurité des données des systèmes de mesure intelligents pour la certification et l'exploitation de systèmes de mesure intelligents,* 2018)
- *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung,* juillet 2018 (citée : AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung,* 2018)

AUTORITÉ FÉDÉRALE DE SURVEILLANCE DES MARCHÉS FINANCIERS

- *Circulaire 2008/7 « Outsourcing – banques, Externalisation d'activités dans le secteur bancaire »,* 20 novembre 2008 (citée : FINMA, *Circulaire 2008/7,* 2008)
- *Circulaire 2018/3 « Outsourcing – Externalisations dans le secteur des banques, des entreprises d'assurance et de certains établissements financiers au sens de la LEFin »,* 21 septembre 2017 (citée : FINMA, *Circulaire 2018/3,* 2017)
- *Communication FINMA sur la surveillance 05/2020 – Obligation de signaler les cyberattaques selon l'art. 29 al. 2 LFINMA,* 7 mai 2020 (citée : FINMA, *Communication FINMA sur la surveillance 05/2020 – Obligation de signaler les cyberattaques selon l'art. 29 al. 2 LFINMA,* 2020)
- *Circulaire 2023/1, Risques et résilience opérationnels – Banques,* 7 décembre 2022 (citée : FINMA, *Circulaire 2023/1,* 2022)

CENTRE NATIONAL POUR LA CYBERSÉCURITÉ/GOVCERT, *Cybersécurité dans le secteur de la santé : recommandations,* 24 mai 2022 (citée : NCSC/GovCERT, *Cybersécurité dans le secteur de la santé : recommandations,* 2022)

CENTRE NATIONAL POUR LA CYBERSÉCURITÉ, *Si001 – Protection informatique de base dans l'administration fédérale,* version 5.0, 1er mars 2022 (citée : NCSC, *Si001,* 2022)

CONFÉRENCE DES DIRECTRICES ET DIRECTEURS CANTONAUX DE LA SANTÉ, *Recommandations de la CDS sur la planification hospitalière d'après la révision de la LAMal sur le financement hospitalier du 21.12.2007, la révision de l'OAMal sur les critères de planification du 23.6.2021 et la jurisprudence du 1.1.2012 au 31.12.2021, Version révisée des recommandations adoptée par le Comité directeur de la CDS le 14.5.2009 et le 25.5.2018, approuvée par l'Assemblée plénière de la CDS du 20.5.2022,* 20 mai 2022 (citée : CDS, *Recommandations de la CDS sur la planification hospitalière,* 2022)

CONSEIL FÉDÉRAL, *Directives sur l'organisation de la conduite de la politique de sécurité du Conseil fédéral,* 25 janvier 2023 (FF 2023 241)

H+, *Sécurité de l'information et protection des données, Exigences concernant la sécurité informatique de systèmes* tiers, version 1.2, janvier 2020 (citée : H+, *Sécurité de l'information et protection des données, Exigences concernant la sécurité informatique de systèmes* tiers, 2020)

OFFICE FÉDÉRAL DE LA COMMUNICATION, *Lignes directrices relatives à la sécurité et la disponibilité des infrastructures et des services de télécommunication,* 4e édition, février 2023 (citée : OFCOM, *Lignes directrices relatives à la sécurité et la disponibilité des infrastructures et des services de télécommunication,* 2023)

OFFICE FÉDÉRAL DES TRANSPORTS, *Directive Cybersécurité chemins de fer, Dir. CySec-Rail,* 22 septembre 2023 (citée : OFT, *Dir. CySec-Rail*).

OFFICE FÉDÉRAL POUR L'APPROVISIONNEMENT ÉCONOMIQUE DU PAYS/ASSOCIATION SUISSE DES EXPLOITANTS D'INSTALLATIONS DE TRAITEMENT DES DÉCHETS, *Norme minimale pour la sécurité des technologies de l'information et de la communication (TIC) dans le domaine de l'élimination des déchets,* novembre 2022 (citée : OFAE/ASED, *Norme minimale pour la sécurité des TIC dans le domaine de l'élimination des déchets,* 2022)

OFFICE FÉDÉRAL POUR L'APPROVISIONNEMENT ÉCONOMIQUE DU PAYS
- *Norme minimale pour améliorer la résilience informatique,* mai 2023 (citée : OFAE, *Norme minimale pour améliorer la résilience informatique,* 2023)
- *Norme minimale pour sécuriser la technologie de l'information et de la communication dans la filière alimentaire,* 2019 (citée : OFAE, *Norme minimale pour sécuriser la technologie de l'information et de la communication dans la filière alimentaire,* 2019)

OFFICE FÉDÉRAL POUR L'APPROVISIONNEMENT ÉCONOMIQUE DU PAYS / RÉSEAUX THERMIQUES SUISSES RETS/SOCIÉTÉ SUISSE DE L'INDUSTRIE DU GAZ ET DES EAUX, *Norme minimale pour garantir la sécurité des technologies de l'information et de la communication (TIC) requises pour l'approvisionnement du chauffage et du froid à distance,* février 2023 (citée : OFAE/RETS/SSIGE, *Norme minimale pour garantir la sécurité des technologies de l'information et de la communication (TIC) requises pour l'approvisionnement du chauffage et du froid à distance,* 2023)

OFFICE FÉDÉRAL POUR L'APPROVISIONNEMENT ÉCONOMIQUE DU PAYS / UNION DES TRANSPORTS PUBLICS, *Manuel sur la cybersécurité destiné aux entreprises de transports publics,* 7 mai 2021 (citée : OFAE/UTP, *Manuel sur la cybersécurité destiné aux entreprises de transports publics,* 2021)

OFFICE FÉDÉRAL POUR L'APPROVISIONNEMENT ÉCONOMIQUE DU PAYS / VERBAND SCHWEIZER ABWASSER, *Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie in Abwasserbetrieben,* mars 2021 (citée : BWL/VSA, *Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie in Abwasserbetrieben,* 2021)

SOCIÉTÉ SUISSE DE L'INDUSTRIE DU GAZ ET DES EAUX

- *Recommandation – Norme minimale pour garantir la sécurité des technologies de l'information et de la communication (TIC) requises dans l'approvisionnement en gaz,* édition décembre 2020 (citée : SSIGE, *Norme minimale pour garantir la sécurité des technologies de l'information et de la communication (TIC) requises dans l'approvisionnement en gaz,* 2020)
- *Norme minimale pour garantir la sécurité des technologies de l'information et de la communication (TIC) requises pour l'approvisionnement en eau,* mars 2019 (citée : SSIGE, *Norme minimale pour garantir les TIC requises pour l'approvisionnement en eau,* 2019)
- *Norme minimale pour garantir la sécurité des technologies de l'information et de la communication (TIC) requises pour l'approvisionnement en gaz,* décembre 2020 (citée : SSIGE, *Norme minimale pour garantir la sécurité des technologies de l'information et de la communication (TIC) requises pour l'approvisionnement en gaz,* 2020)

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE, *Directives sur les exigences minimales qu'un système de gestion de la protection des données doit remplir (Directives sur la certification de l'organisation et de la procédure),* 19 mars 2014 (citée : PFPDT, *Directives sur la certification de l'organisation et de la procédure,* 2014)

Normes, standards et cadres internationalement reconnues

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK

- BSI-Standard 100-4, *Notfallmanagement,* version 1.0, 2008 (citée : BSI-Standard 100-4)
- BSI-Standard 200-1, *Managementsysteme für Informationssicherheit (ISMS),* version 1.0, 2017 (citée : BSI-Standard 200-1)
- BSI-Standard 200-2, *IT-Grundschutz Methodik,* version 2.0, 2017 (citée : BSI-Standard 200-2)
- BSI-Standard 200-3, *Risikomanagement,* version 1.0, 2017 (citée : BSI-Standard 200-3)

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION

- COBIT 2019 Framewok for Information Securiy, USA 2019 (citée : ISACA, COBIT 2019)
- COBIT 5 Framework for Information Security, USA 2012 (citée : COBIT 5)

ISO/IEC 27000 : 2018, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire*

ISO/IEC 27001 : 2013, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences*

ISO/IEC DIS 27002 : 2021, *Information security, cybersecurity and privacy protection – Information security controls*

ISO/IEC 27005 : 2018, *Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information*

ISO/IEC 27009 : 2020, *Sécurité de l'information, cybersécurité et protection des données personnelles – Application de l'ISO/IEC 27001 à un secteur spécifique – Exigences*

ISO/IEC 27019 : 2017, *Technologies de l'information – Techniques de sécurité – Mesures de sécurité de l'information pour l'industrie des opérateurs de l'énergie*

ISO/IEC 27032 : 2023, *Cybersécurité – Lignes directrices relatives à la sécurité sur l'internet,* deuxième édition

ISO/IEC 27035-1 : 2016, *Technologies de l'information – Techniques de sécurité – Gestion des incidents de sécurité de l'information – Partie 1 : Principes de la gestion des incidents*

ISO/IEC 27035-2 : 2016, *Technologies de l'information – Techniques de sécurité – Gestion des incidents de sécurité de l'information – Partie 2 : Lignes directrices pour planifier et préparer une réponse aux incidents*

ISO/IEC 27035-3 : 2020, *Technologies de l'information – Gestion des incidents de sécurité de l'information – Partie 3 : Lignes directrices relatives aux opérations de réponse aux incidents TIC*

ISO/IEC 27039 : 2015, *Technologies de l'information – Techniques de sécurité – Sélection, déploiement et opérations des systèmes de détection et prévention d'intrusion*

ISO/IEC 27799 : 2016, *Health informatics – Information security management in health*

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, *Recommandation du Conseil sur la sécurité numérique des activités critiques,* 2023 (citée : OCDE, *Recommandation du Conseil sur la sécurité numérique des activités critiques,* 2023)

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Security and Privacy Controls for Information Systems and Organsizations,* Special Publication 800-53, révision 5, septembre 2020 (citée : NIST, 800-53, rev. 5).

UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

- Recommendation ITU-T X.1051, *Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations,* avril 2016 (citée : ITU-T X.1051)
- Recommandation X.1205, avril 2008 (citée : UIT, X.1205)

Bibliographie[1]

Articles et monographies

ALBERINI Alain / ALBERINI Adrien, *Le droit suisse des noms de domaine,* Quid Iuris ?, Genève/Zurich/Bâle 2019.

ALBERTS Chris et al., *Defining Incident Management Processes for CSIRTs : A Work in Progress,* octobre 2024.

ANCELLE Juliette / FERDJANI Karim, *Les contrats informatiques – États des lieux et questions choisies,* in : Richa Alexandre/Canapa Damiano (éds), *Droit et économique numérique,* Berne 2021.

ANDERSON Atenas / GALETTI Benedetta S., *La conservation des données personnelles : comment déterminer sa durée ?,* sic! 2021, p. 103 ss.

ARPAGIAN Nicolas, *La cybersécurité,* Paris 2022.

ASGHAR Muhammad Rizwan / HU Qinwen / ZEADALLY Sherali, *Cybersecurity in industrial control systems : Issues, technologies, and challenges,* Computer Networks 165, 2019.

AUBERT Gabriel, art. 319 CO, in : Martenet Vincent / Dubey Jacques (éds), *Commentaire Romand, Constitution fédérale, Préambule – art. 80 Cst.*, Bâle 2021.

AUBERT Jean-François
- art. 57 Cst., in : Aubert Jean-François / Mahon Pascal (éds), *Petit commentaire de la Constitution fédérale de la Confédération suisse du 18 avril 1999,* Zurich/Bâle/Genève 2003.
- *Le principe de subsidiarité dans la Constitution fédérale de 1999,* in : Bolle Pierre-Henri (éd.), *Mélanges en l'honneur de Henri-Robert Schüpbach,* Bâle/Genève/Munich 2000, p. 3 ss.

AUBERT Jean-François / MAHON Pascal (éds), *Petit commentaire de la Constitution fédérale de la Confédération suisse du 18 avril 1999,* Zurich/Bâle/Genève 2003.

AUER Andreas / FLÜCKIGER Alexandre / HOTTELIER Michel (éds), *Les droits de l'homme et la constitution : études en l'honneur du Professeur Giorgio Malinverni,* Genève 2007.

1 Sauf indication contraire, les ouvrages et la documentation de cette bibliographie sont citées dans les notes avec l'indication du seul nom des auteures.

BAERISWYL Bruno / PÄRLI Kurt (éds), Datenschutzgesetz (DSG), *Stämpflis Handkommentar SHK,* Berne 2015.

BANDLE Anne Laure / RENOLD Marc-André, *Droit de l'art et des biens culturels,* Bâle 2022.

BARBEY Alexandre, *Les lois dites technologiquement neutres face à la sécurité juridique,* in : Guillaume Florence (éd.), *La technologie, l'humain et le droit,* Berne 2023, p. 1 ss.

BARRELET Denis / EGLOFF Willi (éds), *Le nouveau droit d'auteur, Commentaire de la loi fédérale sur le droit d'auteur et les droits voisins,* 4e édition, Berne 2021.

BAUER Johannes M. / VAN EETEN Michel J.G., *Cybersecurity : Stakeholder incentives, externalities and policy options,* Telecommunications Policy 33 (2009), p. 706 ss.

BÉGUIN Nicolas, art. 8 LPD, in : Benhamou Yaniv/Cottier Bertil (éds), *Loi fédérale sur la protection des données, Petit commentaire,* Bâle 2023.

BÉGUIN Nicolas / VIGNIEU Benjamin, art. 24 LPD, in : Benhamou Yaniv / Cottier Bertil (éds), *Loi fédérale sur la protection des données, Petit commentaire,* Bâle 2023.

BELLANGER François, art. 5*a*, 42 et 43a Cst., in : Martenet Vincent / Dubey Jacques (éds), *Commentaire Romand, Constitution fédérale, Préambule – art. 80 Cst.,* Bâle 2021.

BELSER Eva M. / NOUREDDINE Hussein, *Die Datenschutzgesetzgebung des Bundes,* in : Epiney Astrid / Belser Eva M. / Waldmann Bernhard (éds), *Datenschutzrecht – Grundlagen und öffentliches Recht,* Berne 2011, p. 412 ss.

BENHAMOU Yaniv, *Blocage de sites web en droit suisse : des injonctions civiles et administratives de blocage au séquestre pénal,* in : De Werra Jacques (éd.), *Droit d'auteur 4.0,* Genève 2018.

BENHAMOU Yaniv / BERNARD Frédéric / DURAND Cédric, *Souveraineté numérique, Étude pluridisciplinaire pour la Suisse,* Genève 31 janvier 2023.

BENHAMOU Yaniv / COTTIER Bertil (éds), *Loi fédérale sur la protection des données, Petit commentaire,* Bâle 2023.

BENHAMOU Yaniv / WANG Louise, *Cyberattaque et ransomware : risques juridiques à payer et assurabilité des rançons,* RSDA 2023, p. 80 ss.

BENSOUSSAN Alain / BENSOUSSAN Jérémy, *IA, Robots et Droit,* Bruxelles 2019.

BERGER Stephan / BÜRGER Olga / RÖGLINGER Maximilian, *Attacks on the Industrial Internet of Things – Development of a multi-layer Taxonomy,* mars 2020.

BERTHIER Thierry, *Hacktivisme : vers une complexification des cyberattaques,* Revue Défense Nationale 2015/9 (N 784,) p. 45 ss.

BHATTACHARJEE Sravani, *Practical Industrial Internet of Things Security – A Practionner's Guide to Securing Connected Industries,* juillet 2018.

BIAGGINI Giovanni, art. 5*a,* 42 et 43 BV, in : Waldmann Bernhard / Besler Eva M. / Epiney Astrid (éds), *Basler Kommentar, Bundesverfassung,* Bâle 2015.

BIERI Adrian / POWELL Julian, *Meldung von Verletzungen der Datensicherheit – Rechtslage nach dem totalrevidierten Datenschutzgesetz,* AJP/PJA 6/2021, p. 780 ss.

BLECHTA Gabor P., art. 3 DSG, in : Maurer-Lambrou Urs / Blechta Gabor P. (éds), *Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz,* 3e édition, Bâle 2014.

BLECHTA Gabor P. / DAL MOLIN Luca / WESIAK-SCHMIDT Kirsten, art. 5 DSG, in : Blechta Gabor P. / Vasella David (éds), *Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz,* 4e édition, Bâle 2024.

BLECHTA Gabor P. / VASELLA David (éds), *Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz,* 4e édition, Bâle 2024.

BLEICKER Olivier, art. 57 Cst., in : Martenet Vincent / Dubey Jacques (éds), *Commentaire Romand, Constitution fédérale, Préambule – art. 80 Cst.,* Bâle 2021.

BOETON ENGEL Veronica, art. 285 CP, in : Macaluso Alain et al. (éds), *Commentaire romand, Code pénal II, Art. 111-392 CP,* Bâle 2017.

BOLLE Pierre-Henri (éd.), *Mélanges en l'honneur de Henri-Robert Schüpbach,* Bâle/Genève/Munich 2000.

BONDALLAZ Stéphane, *La protection des personnes et de leurs données dans les télécommunications,* Zurich/Bâle/Genève 2007.

BOILLAT Joséphine / WERLY Stéphane, art. 30, 31 et 32 LPD, in : Meier Philippe / Métille Sylvain (éds), *Commentaire Romand, Loi fédérale sur la protection des données,* Bâle 2023.

BOYES Hugh, *Cybersecurity and Cyber-Resilient Supply Chains, Technology Innovation Management Review*, avril 2015, p. 28 ss.

BRINER Robert G., *Software-Wartungsverträge,* in : Jörg Florian S. / Arter Olivier (éds), *Internet-Recht und IT-Verträge,* Berne 2005, p. 129 ss.

BRODEUR Jean-Paul, *Le risque et la menace,* Toronto 2006.

BÜHLMANN Lukas / REINLE Michael, art. 6 DSG, in : Blechta Gabor P. / Vasella David (éds), *Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz,* 4e édition, Bâle 2024.

BÜHLER Robert / RAMPINI Corrado, art. 9 DSG, in : Blechta Gabor P. / Vasella David (éds), *Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz,* 4e édition, Bâle 2024.

BURTON Cédric, art. 32 GDPR, in : Kuner Christopher / Bygrave Lee A. / Docksey (éds), *The EU General Data Protection Regulation (GDPR) – A Commentary,* Oxford 2020.

CANAPA Damiano, art. 95 Cst., in : Martenet Vincent / Dubey Jacques (éds), *Commentaire Romand, Constitution fédérale, Art. 81 Cst. – dispositions finales,* Bâle 2021.

CARON Pierre, *La protection du patrimoine informationnel,* in : Harbulot Christian (éd.), *Manuel d'intelligence économique,* France 2012, p. 293 ss.

CARTIER Julien, *La poursuite des cybercriminels au quotidien,* in : Perrier Depeursinge et al. (éds), *Lutter contre la cybercriminalité en Suisse,* Berne 2024, à paraître.

CHAIX François, art. 363 et 364 CO, in : Thévenoz Luc / Werro Franz (éds), *Commentaire romand, Code des obligations I, Art. 1-529 CO,* Bâle 2021.

CHAPPUIS Benoît / ALBERINI Adrien, *Secret professionnel de l'avocat et solutions cloud,* Revue de l'avocat 2017/8, p. 337 ss.

CHAPPUIS Benoît, art. 321 CP, in : Macaluso Alain et al. (éds), *Commentaire romand, Code pénal II, Art. 111-392 CP,* Bâle 2017.

CHATTON Gregor T., art. 6 Cst., in : Martenet Vincent / Dubey Jacques (éds), *Commentaire Romand, Constitution fédérale, Préambule – art. 80 Cst.,* Bâle 2021.

CHRISTEN Markus / GORDIJN Bert / LOI Michele (éds), *The Ethics of Cybersecurity,* 2021.

CHRISTEN Markus / KNIEPS Melanie, *CERTs & Ethics : Guidelines, Four steps for a value-driven cybersecurity culture,* Zurich 2024.

CHRISTEN Markus / LOI Michele, *Ethical Frameworks for Cybersecurity,* in : Christen Markus / Gordijn Bert / Loi Michele (éds), *The Ethics of Cybersecurity,* 2021, p. 73 ss.

CORBOZ Bernard
– *Les infractions en droit suisse,* Volume I, Berne 2010 (cité : CORBOZ, volume I).
– *Les infractions en droit suisse,* Volume II, Berne 2010 (cité : CORBOZ, volume II).

COSSALI SAUVAIN Monique, art. 36 LPD, in : Benhamou Yaniv/Cottier Bertil (éds), *Loi fédérale sur la protection des données, Petit commentaire,* Bâle 2023.

DALLÈVES Laure / BAGNOUD Raphaël (éds.), *Internet 2005,* Lausanne 2005.

DAL MOLIN Luca, art. 16, 17 DSG, in : Blechta Gabor P. / Vasella David (éds), *Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz,* 4e édition, Bâle 2024.

DARMS Martin, *Gefährdung Schweizer Spitäler gegenüber Cyberangriffen,* Zurich/Bâle/Genève 2016.

DE TERWANGNE Cécile, art. 5, in : Kuner Christopher / Bygrave Lee A. / Docksey (éds), *The EU General Data Protection Regulation (GDPR) – A Commentary,* Oxford 2020.

DE WERRA Jacques (éd.), *Droit d'auteur 4.0,* Genève 2018.

DE WERRA Jacques, *Entreprises et Big Data : peut-on forcer les entreprises à partager leurs données non-personnelles (par des licences obligatoires ou des licences « FRAND ») ?,* RSDA 2020, p. 365 ss.

DE WERRA Jacques / BENHAMOU Yaniv, *Cyberassurance : instrument utile pour la cybersécurité des entreprises?,* Jusletter 24 août 2020.

DIGGELMANN Oliver / ALTWICKER Tilmann, art. 57 BV, in : Waldmann Bernhard / Belser Eva M. / Epiney Astrid (éds), *Basler Kommentar, Schweizerische Bundesverfassung (BV),* Bâle 2015.

DIGGELMANN Oliver / HERTIG RANDALL Maya/SCHINDLER Benjamin (éds), *Droit constitutionnel suisse,* Zurich/Bâle/Genève 2020.

DIOGENES Yuri / OZKAYA Erdal, *Cybersecurity – Attack and Defense Strategies – Infrastructure security with Red Team and Blue Team tactics,* Birmingham 2018.

DONZALLAZ Yves, *Traité de droit médical,* Volume I, Berne 2021.

DRECHSLER Christian, art. 2 DSG, in : Blechta Gabor P. / Vasella David (éds), *Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz,* 4e édition, Bâle 2024.

DSOUZA Zahra, *Are Cyber Security Incident Response Teams (CSIRT) Redundant or Can They Be Relevant to International Cyber Security ?,* Federal Communications Law Journal, vol. 69, janvier 2018, pp. 201-226.

DUBEY Jacques, art. 5, 164 Cst., in : Martenet Vincent/Dubey Jacques (éds), *Commentaire Romand, Constitution fédérale, Préambule – art. 80 Cst.,* Bâle 2021.

DUBEY Jacques / ZUFFEREY Jean-Baptiste, *Droit administratif général,* Bâle 2014.

DUPUIS Michel et al., *Petit commentaire – Code pénal,* Bâle 2017.

DURBHA Surya / JOGLEKAR Jyoti, *Internet of Things,* New Delhi 2021.

EGLI Urs, *Agile Softwareprojekte : Rechtliche Qualifikation und vertragliche Umsetzung,* Jusletter 31 août 2015.

EGLOFF Willi / HEINZMANN Michel, art. 62 LDA, in : Barrelet Denis / Egloff Willi (éds), *Le nouveau droit d'auteur, Commentaire de la loi fédérale sur le droit d'auteur et les droits voisins,* 4e édition, Berne 2021.

EHRENSPERGER Jennifer
- art. 19 DSG, in : Maurer-Lambrou Urs / Blechta Gabor P. (éds), *Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz,* 3e édition, Bâle 2014.
- art. 36 DSG, in : Blechta Gabor P. / Vasella David (éds), *Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz,* 4e édition, Bâle 2024.

EPINEY Astrid
- Allgemeine Grundsätze, in : Epiney Astrid / Belser Eva M. / Waldmann Bernhard (éds), *Datenschutzrecht – Grundlagen und öffentliches Recht,* Berne 2011, p. 510 ss.
- art. 36 et 41 LPD, in : Meier Philippe / Métille Sylvain (éds), *Commentaire Romand, Loi fédérale sur la protection des données,* Bâle 2023.

EPINEY Astrid / BELSER Eva M. / WALDMANN Bernhard (éds), *Datenschutzrecht – Grundlagen und öffentliches Recht,* Berne 2011.

EPINEY Astrid / FASNACHT Tobias, *Besondere Grundsätze,* in : Epiney Astrid / Belser Eva M. / Waldmann Bernhard (éds), *Datenschutzrecht – Grundlagen und öffentliches Recht,* Berne 2011, p. 559 ss.

EPINEY Astrid / POSSE Samah, art. 33 LPD, in : Meier Philippe / Métille Sylvain (éds), *Commentaire Romand, Loi fédérale sur la protection des données,* Bâle 2023.

ÉRARD Frédéric, *Le secret médical – Étude des obligations de confidentialité des soignants en droit suisse,* thèse Lausanne, Zurich 2021.

ETTLINGER Claudius, *Die Informationspflicht gemäss neuem Datenschutzgesetz,* Jusletter IT 16 décembre 2021.

FANTI Sébastien / STAEGER Alexandre, art. 7, 8 LPD, in : Meier Philippe / Métille Sylvain (éds), *Commentaire romand, Loi sur la protection des données,* Bâle 2023.

FAVRE Anne-Christine / MARTENET Vincent / POLTIER Étienne (éds), *La responsabilité de l'État,* Genève/Zurich/Bâle 2012.

FÉLIX Romain, *Location de services versus autres contrats de prestations : critères de distinction,* in : Wyler Rémy (éd.), *Panorama III en droit du travail, Recueil d'études réalisées par des praticiens,* Berne 2017, p. 779 ss.

FISCHER Philipp, art. 13, 16, 17 LPD, in : Meier Philip/Métille Sylvain (éds), *Commentaire romand, Loi sur la protection des données,* Bâle 2023.

FISCHER Philipp / RICHA Alexandre, art. 273 CP, in : Macaluso Alain et al. (éds), *Commentaire romand, Code pénal II, Art. 111-392 CP,* Bâle 2017.

FISCHER Philipp / RICHA Alexandre / RAEDLER David, art. 162 CP, in : Macaluso Alain et al. (éds), *Commentaire romand, Code pénal II, Art. 111-392 CP,* Bâle 2017.

FLÜCKIGER Christian, art. 19, 20 LPD, in : Meier Philip / Métille Sylvain (éds), *Commentaire romand, Loi sur la protection des données,* Bâle 2023.

FLÜCKIGER Alexandre, *(Re)faire la loi – Traité de légistique à l'ère du droit souple,* Genève 2019.

FRANCEY Julien, art. 6, 18 LPD, in : Benhamou Yaniv / Cottier Bertil (éds), *Loi fédérale sur la protection des données, Petit commentaire,* Bâle 2023.

FRATTOLILLO Andrea, *Le droit constitutionnel des médias à l'ère numérique, De la définition des médias à la compétence de la Confédération, en passant par la liberté du journalisme,* Berne 2024.

FRICK Markus R., art. 6 UWG, in : Hilty Reto M. / Arpgaus Reto (éds), *Basler Kommentar, Bundesgesetz gegen den unlauteren Wettbewerb (UWG),* Bâle 2013.

FUCHS Philippe / KUNZ Christian, art. 20 DSG, in : Blechta Gabor P. / Vasella David (éds), *Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz,* 4e édition, Bâle 2024.

GAUCH Peter, *Le contrat d'entreprise,* adaptation française par Carron Benoît, Zurich 1999.

GENECAND Téo, art. 16, 32, 41 et 62 LPD, in : Benhamou Yaniv / Cottier Bertil (éds), *Loi fédérale sur la protection des données, Petit commentaire,* Bâle 2023.

GEISER Thomas, *Schnittstellen zwischen IT-Recht und Arbeitsrecht,* in : Jörg Florian S. / Arter Olivier (éds), *Internet-Recht und IT-Verträge,* Berne 2005, p. 163 ss.

GHERNAOUTI Solange
- *Cybercriminalité, Comprendre. Prévenir. Réagir,* 2023 (citée : GHERNAOUTI, *Cybercriminalité,* 2023).
- *Cyberpower – Crime, Conflict and Security in Cyberspace,* Lausanne 2013 (citée : GHERNAOUTI, *Cyberpower,* 2013).
- *Cybersécurité – sécurité informatique et réseaux,* 5e édition, 2011 (citée : GHERNAOUTI, *Cybersécurité,* 2011).
- *La cybersécurité des infrastructures électriques,* revue spécialisée et informations des associations Electrosuisse, AES, 2019, volume 110 (12), p. 46 ss (citée : GHERNAOUTI, *La cybersécurité des infrastructures électriques,* 2019).

GÖBEL Oliver, *Incident Response Capabilities,* digma 2008, cahier 4, p. 166 ss.

GRAF Martin / THELER Cornelia / VON WYSS Moritz (éds), *Parlamentsrecht und Parlamentspraxis der Schweizerischen Bundesversammlung, Kommentar zum Parlamentsgesetz (ParlG) vom 13. Dezember 2002,* Bâle 2014.

GUILLOD Olivier / STEFFEN Gabrielle, art. 19/20 CO, in : Thévenoz Luc / Werro Franz (éds), *Commentaire romand, Code des obligations I, Art. 1-529 CO,* Bâle 2021.

GUISAN Alexandre / HIRSCH Célian, *La surveillance secrète de l'employé,* RSJ 115/2019, p. 707 ss.

GUROVITS KOHLI András A., *IT-Outsourcing Verträge in der Vertragspraxis,* in : Jörg Florian S. / Arter Olivier (éds), *Internet-Recht und IT-Verträge,* Berne 2005, p. 261 ss.

HÄMERLI Bernhard M., *Sicherheitsmassnahmen und Vorbeugung,* digma décembre 2020, cahier 4, p. 190 ss.

HARBULOT Christian (éd.), *Manuel d'intelligence économique,* France 2012.

HENZELIN Marc / MASSROURI Maryam, art. 160 CP, in : Macaluso Alain et al. (éds), *Commentaire romand, Code pénal II, Art. 111-392 CP,* Bâle 2017.

HIRSCH Célian, *Le devoir d'informer lors d'une violation de la sécurité des données, Avec un regard particulier sur les données bancaires*, thèse Genève/Zurich 2023.

HILTY Reto M. / ARPGAUS Reto (éds), *Basler Kommentar, Bundesgesetz gegen den unlauteren Wettbewerb (UWG),* Bâle 2013.

HOLLIGER-HAGMANN Eugénie, art. 3 PrSG, in : Fischer Willi / Luterbacher Thierry (éds), *Haftpflichtkommentar, Kommentar zu den schweizerischen Haftpflichtbestimmungen,* Zurich/Saint-Gall 2015.

HOOPER Val / MCKISSACK Jeremy, *The emerging role of the CISO, Business Horizons,* vol. 59, issue 6, Wellington 2016, p. 585 ss.

HURTADO POZO José / GODEL Thierry, *Droit pénal général,* 4e édition, Genève/Zurich 2023.

HUSI-STÄMPFLI Sandra, *Informationssicherheits- und Datenschutzgesetz : Chance auf ein neues Zeitalter,* Jusletter, 25 septembre 2023.

HUSI-STÄMPFLI Sandra / MORAND Anne-Sophie, *Datenschutzrecht,* 2e édition, Zurich/Genève 2024.

HUSMANN Markus, art. 273 StGB, in : Niggli Marcel A. / Wiprächtiger (éds), *Basler Kommentar, Strafrecht II, Art. 137-392 StGB, Jugendstrafgesetz,* Bâle 2019.

IGLEZAKIS Ioannis (éd.), *The Legal Regulation of Cyber Attacks,* Alphen aan den Rijn 2020.

ILG Niclas et al., *A survey of contemporary open-source honeypots, frameworks, and tools*, Journal of Network and Computer Applications, vol. 220, novembre 2023.

JAAG Tobias, *Le système général du droit de la responsabilité de l'État,* in : Favre Anne-Christine / Martenet Vincent / Poltier Étienne (éds), *La responsabilité de l'État,* Genève/Zurich/Bâle 2012, p.23 ss.

JACCARD Michel, *Intelligence artificielle et prestation de services, Réflexions juridiques et pratiques autour des contrats de l'intelligence artificielle,* in : Richa Alexandre / Canapa Damiano (éds), *Aspects juridiques de l'intelligence artificielle,* Berne 2024.

JACCARD Michel / ROBERT Vincent, *Les contrats informatiques,* in : Pichonnaz Pascal / Werro Franz (éds), *La pratique contractuelle : actualité et perspectives, Smposium en droit des contrats,* Genève/Zurich/Bâle 2009, p. 95 ss.

JACCOUD Lisa / FANTI Sébastien / STAEGER Alexandre, art. 20 LPD, in : Benhamou Yaniv / Cottier Bertil (éds), *Loi fédérale sur la protection des données, Petit commentaire,* Bâle 2023.

JACOT-GUILLARMOD Émilie, art. 5 LPD, in : Benhamou Yaniv / Cottier Bertil (éds), *Loi fédérale sur la protection des données, Petit commentaire,* Bâle 2023.

JAQUET-CHIFFELLE David-Olivier, *Continuité de la preuve (numérique) – de la scène de crime au tribunal,* in : Perrier Depeursinge et al. (éds), *Cimes et Châtiments*, Berne 2022, p. 193 ss.

JAQUIER Sébastien, *Cybersécurité, et si nous faisions fausse route,* in : Jaquier Sébastien / Beaudet-Labrecque / Zbinden Renaud (éds), *Criminalité économique et cybercriminalité – Mélanges en l'honneur de la professeure Isabelle Augsburger-Bucheli,* Bâle 2021, p. 217 ss.

JAQUIER Sébastien / BEAUDET-LABRECQUE Olivier / ZBINDEN Renaud (éds), *Criminalité économique et cybercriminalité – Mélanges en l'honneur de la professeure Isabelle Augsburger-Bucheli,* Bâle 2021.

JEANNERET Yvan, art. 142 CP, in : Macaluso Alain et al. (éds), *Commentaire romand, Code pénal II, Art. 111-392 CP,* Bâle 2017.

JOHANSEN Gerard, *Digital Forensics and Incident Response – Third Edition,* Birmingham 2022.

JÖRG Florian S. / ARTER Olivier (éds)
- *Internet-Recht und IT-Verträge,* Berne 2005.
- *Internet-Recht und IT-Verträge,* 2e édition, Berne 2009.

JOTTERAND Alexandre, *Contrats cloud : qualification, gestion des données et sortie de la relation,* in : Métille Sylvain (éd.), *L'informatique en nuage,* Berne 2024, p. 1 ss.

KESSLER COENDET Franz / SCHEFER Andreas, art. 4, 5 KEG, in : Kratz Brigitta et al. (éds), *Kommentar zum Energierecht, Band II: CO2-Gesetz / KEG / ENSIG,* Berne 2016.

KIESER Ueli / PÄRLI Kurt / UTTINGER Ursula (éds), *Datenschutztagung 2017, Baustelle Datenschutz – Observation als Brennpunkt,* Zurich/Saint-Gall 2017.

KILLCRECE Georgia et al.
- *Organizational Models for Computer Security Incident Response Teams (CSIRT),* Carnegie Mellon Software Engineering Institue, décembre 2003 (citées : KILLCRECE et al., *Organisational Models for CSIRT,* 2003).
- *State of the Practice of Computer Security Incident Response Teams (CSIRT),* Carnegie Mellon Software Engineering Institute, octobre 2003 (citées : KILLCRECE et al., *State of Practice of CSIRT,* 2003).

KILOVATY Ido, *Psychological Data Breach Harms,* North Carolina Journal of Law & Technology, vol. 23/1, 10 janvier 2021.

KNIEPS et al., *La cybersécurité : entre autonomie et soutien étatique,* Plaidoyer 4/2023, p. 22 ss.

KÖNIGS Hans-Peter, *ISO/IEC-Standards gegen Cyber-Risiken,* digma septembre 2017, cahier 3, p. 142 ss.

KORFF Douwe, *First do no harm: the potential of harm being caused to fundamental rights and freedoms by state cybersecurity interventions,* in : Wagner Ben / Kettermann Matthias C. / Vieth Kilian (éds), *Research Handbook on Human Rights and Digital Technology – Global Politics, Law and International Relations,* Janvier 2019, p. 129 ss.

KRATZ Brigitta, art. 7, 8 EnG, in : Kratz Brigitta et al. (éds), *Kommentar zum Energierecht, Band III: Totalrevision EnG sowie Teilrevisionen CO2-Gesetz / DBG / StHG / RPG / WRG / KEG / EleG / StromVG / RLG,* Berne 2020.

KRATZ Brigitta et al. (éds)
- *Kommentar zum Energierecht, Band I : WRG / EleG / StromVG / RLG,* Berne 2016.
- *Kommentar zum Energierecht, Band II : CO_2-Gesetz / KEG / ENSIG,* Berne 2016.

– *Kommentar zum Energierecht, Band III : Totalrevision EnG sowie Teilrevisionen CO_2-Gesetz / DBG / StHG / RPG / WRG / KEG / EleG / StromVG / RLG,* Berne 2020.

KUNER Christopher / BYGRAVE Lee A. / DOCKSEY Christopher (éds), *The EU General Data Protection Regulation (GDPR) – A Commentary,* Oxford 2020.

KÜNZLI Jörg, art. 182 BV, in : Waldmann Bernhard / Besler Eva M. / Epiney Astrid (éds), *Basler Kommentar, Bundesverfassung,* Bâle 2015.

LEGRENZI Christophe, *Informatique, numérique et système d'information : définitions, périmètre, enjeux économiques*, Vis & Sciences de l'entreprise 2015/2, N 200, p. 49 ss.

LEMNITZER Jan Martin, *Why cybersecurity insurance should be regulated and compulsory,* Journal of Cyber Policy 6:2, p. 118.

LIVET Ludivine / DOLIVO-BONVIN Marie, art. 260*ter* CP in : Macaluso Alain et al. (éds), *Commentaire romand, Code pénal II, Art. 111-392 CP,* Bâle 2017.

LUBISHTANI Kastriot, art. 60 Cst., in : Martenet Vincent / Dubey Jacques (éds), *Commentaire Romand, Constitution fédérale, Préambule – art. 80 Cst.,* Bâle 2021.

LUDWICZAK GLASSEY Maria, *Accès transfrontière aux preuves électroniques : l'avenir de l'entraide internationale en matière de cybercriminalité,* in : Perrier Depeursinge et al. (éds), *Lutter contre la cybercriminalité en Suisse,* Berne 2024, à paraître.

MACALUSO Alain et al. (éds), *Commentaire romand, Code pénal II, Art. 111-392 CP,* Bâle 2017.

MARCELLA Albert / MENENDEZ Doug, *A Field Manual for Collectint, Examining, and Preserving Evidence of Computer Crimes,* 2e édition, Floride 2008.

MARKWALDER Nora, *Internet et facilitation du passage à l'acte,* in : Perrier Depeursinge et al. (éds), *Lutter contre la cybercriminalité en Suisse,* Berne 2024, à paraître.

MAROONIAN Anaïs / KOLB Robert, art. 54 Cst., in : Martenet Vincent / Dubey Jacques (éds), *Commentaire Romand, Constitution fédérale, Préambule – art. 80 Cst.,* Bâle 2021.

MARTENET Vincent / DUBEY Jacques (éds)
– *Commentaire Romand, Constitution fédérale, Art. 81 Cst. – dispositions finales,* Bâle 2021.

– *Commentaire Romand, Constitution fédérale, Préambule – art. 80 Cst.*, Bâle 2021.

MARTENET Vincent
– art. 3, 27 et 94 Cst., in : Martenet Vincent / Dubey Jacques (éds), *Commentaire Romand, Constitution fédérale, Préambule – art. 80 Cst.*, Bâle 2021.
– *La Constitution et l'économie,* in : Diggelmann Oliver / Hertig Randall Maya / Schindler Benjamin (éds), *Droit constitutionnel suisse,* Zurich/Bâle/Genève 2020, p. 2061 ss.

MATHYS Roland / THOMANN Kenzo, art. 24 DSG, in : Blechta Gabor P. / Vasella David (éds), *Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz,* 4e édition, Bâle 2024.

MAURER-LAMBROU Urs / BLECHTA Gabor P. (éds), *Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz,* 3e édition, Bâle 2014.

MAURER-LAMBROU Urs / KUNZ Simon, art. 2 DSG, in : Maurer-Lambrou / Blechta Gabor P. (éds), *Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz,* 3e édition, Bâle 2014.

MAURER-LAMBROU Urs / SCHÖNBÄCHLER Matthias R., art. 5 DSG, in : Maurer-Lambrou Urs / Blechta Gabor P. (éds), *Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz,* 3e édition, Bâle 2014.

MAURER-LAMBROU Urs / STEINER Adrea, art. 4, 6 DSG, in : Maurer-Lambrou Urs / Blechta Gabor P. (éds), *Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz,* 3e édition, 2014.

MEIER Anne, art. 319 CO, in : Thévenoz Luc / Werro Franz (éds), *Commentaire Romand, Code des Obligations I, Art. 1-529 CO,* Bâle 2021.

MEIER Philippe / MÉTILLE Sylvain (éds), *Commentaire Romand, Loi fédérale sur la protection des données,* Bâle 2023.

MEIER Philippe, *Protection des données – Fondements, principes généraux et droit privé,* Berne 2011.

MEIER Philippe / TSCHUMY Nicolas, art. 5, 6 LPD, in : Meier Philippe / Métille Sylvain (éds), *Commentaire Romand, Loi fédérale sur la protection des données,* Bâle 2023.

MERKER Michael, art. 3 EleG, in : Kratz Brigitta et al. (éds), *Kommentar zum Energierecht, Band I : WRG / EleG / StromVG / RLG,* Berne 2016.

MERKER Michael / CONRADIN-TRIACA Philip, art. 11 KEG, in : Kratz Brigitta et al. (éds), *Kommentar zum Energierecht, Band II : CO_2-Gesetz / KEG / ENSIG,* Berne 2016.

MÉTILLE Sylvain / AESCHLIMANN Joanna, *Infrastructures et données informatiques : quelle protection au regard du code pénal suisse ?,* RPS 132/2014, p. 283 ss.

MÉTILLE Sylvain / DI TRIA Livio, art. 2 LPD, in : Meier Philippe / Métille Sylvain (éds), *Commentaire Romand, Loi fédérale sur la protection des données,* Bâle 2023.

MÉTILLE Sylvain
- art. 9, 62 LPD, in : Meier Philippe / Métille Sylvain (éds), *Commentaire Romand, Loi fédérale sur la protection des données,* Bâle 2023.
- *Internet et droit – Protection de la personnalité et questions pratiques,* Quid Iuris ?, Genève/Zurich/Bâle 2017 (cité : MÉTILLE, *Internet et droit,* 2017).
- *Mesures techniques de surveillance et respect des droits fondamentaux – en particulier dans le cadre de l'instruction pénale et du renseignement,* Bâle 2011 (cité : MÉTILLE, *Mesures techniques de surveillance et respect des droits fondamentaux – en particulier dans le cadre de l'instruction pénale et du renseignement,* 2011).

MÉTILLE Sylvain (éd.), *L'informatique en nuage,* Berne 2024.

MÉTILLE Sylvain / MEYER Pauline
- *Annonce des violations de la sécurité des données : une nouvelle obligation de la nLPD,* SZW/RSDA 1/2021, p. 23 ss.
- art. 24 LPD, in : Meier Philippe / Métille Sylvain (éds), *Commentaire Romand, Loi fédérale sur la protection des données,* Bâle 2023.
- *Plusieurs approches pour lutter contre la cybercriminalité,* in : Perrier Depeursinge et al. (éds), *Lutter contre la cybercriminalité en Suisse,* Berne 2024, à paraître.

MEYER Pauline / DAVIES Ryan, *Portée pratique du caractère approprié des mesures de sécurité des données sous la LPD,* Jusletter 25 septembre 2023.

MEYER Pauline / MÉTILLE Sylvain
- *Computer security incident response teams : are they really regulated ? The Swiss example,* International Cybersecurity Law Review, 1er octobre 2022, p. 40 ss (citées : MEYER/MÉTILLE, *Computer security incident response teams : are they really regulated ? The Swiss example,* 2022).

– *Loi fédérale sur la sécurité de l'information : version 2.0,* Jusletter 5 septembre 2022 (citées : MEYER/MÉTILLE, *Loi fédérale sur la sécurité de l'information : version 2.0,* 2022).

MEYER Pauline / PANGRAZZI Sara / SARRASIN Delphine, *Ransomware Payments : On Regulatory Incentives to Limit Them,* AJP/PJA 10/2023, p. 1146 ss.

MITROPOULOS Sarandis / PATSOS Dimitrios / DOULIGERIS Christos, *On Incident Handling and Response : A state-of-the-art approach,* Computers & Security, volume 25, Juillet 2006, p. 351 ss.

MITROU Lilian, *Technical Definitions,* in : Iglezakis Ioannis (éd.), *The Legal Regulation of Cyber Attacks,* Alphen aan den Rijn 2020, p. 3 ss.

MOECKLI Daniel, *Sicherheitsverfassung,* in : Diggelmann Oliver / Hertig Randall Maya / Schindler Benjamin (éds), *Droit constitutionnel suisse,* Zurich/Bâle/Genève 2020, p. 2259 ss.

MONNIER Gilles
– art. 143, 143*bis,* 144*bis,* 179*novies* CP, in : Macaluso Alain et al. (éds), *Commentaire romand, Code pénal II, Art. 111-392 CP,* Bâle 2017.
– art. 15 CP, in : Moreillon Laurent et al. (éds), *Commentaire Romand, Code pénal I, Art. 1110 CP,* Bâle 2021.

MONTAVON Michael, *Cyberadministration et protection des données – Étude théorique et pratique de la transition numérique en Suisse du point de vue de l'État, des citoyen-n-es et des autorités de contrôle,* Genève/Zurich/Bâle 2021.

MOOR Pierre, art. 182 Cst, in : Martenet Vincent / Dubey Jacques (éds), *Commentaire Romand, Constitution fédérale, Art. 81 Cst. – dispositions finales,* Bâle 2021.

MORAND Pierre-André, *Le contrat de maintenance,* in : Pichonnaz Pascal / Werro Franz (éds), *La pratique contractuelle : actualité et perspectives, Symposium en droit des contrats,* Genève/Zurich/Bâle 2009, p. 127 ss.

MOREILLON Laurent et al. (éds), *Commentaire Romand, Code pénal I, Art. 1-110 CP,* Bâle 2021.

MOURA Vincente Dário / DE VASCONCELOS Casimiro Sofia (éds), *Data Protection in the Internet,* Allemagne 2020.

MÜLLER Christoph, *Contrats de droit suisse – Présentation systématique des contrats les plus importants en pratique,* Neuchâtel 2021.

NEUENSCHWANDER Peter K., *Vom Outtasking zum BPO – was gilt es zu beachten ?,* in : Jörg Florian S. / Arter Oliver (éds), *Internet-Recht und IT-Verträge,* Berne 2009, p. 115 ss.

NICOLET Yves / PEISSARD Jean-Philippe, *Cybercriminalité : difficultés et enjeux de la poursuite pénale,* in : Jaquier Sébastien / Beaudet-Labrecque / Zbinden Renaud (éds), *Criminalité économique et cybercriminalité – Mélanges en l'honneur de la professeure Isabelle Augsburger-Bucheli,* Bâle 2021, p. 161 ss.

NIGGLI Marcel A. / GFELLER Diego R., art. 102 StGB, in : Niggli Marcel A. / Wiprächtiger Hans (éds), *Basler Kommentar, Strafrecht I, Art. 1-136 StGB,* Bâle 2019.

NIGGLI Marcel A. / HAGENSTEIN Nadine, art. 162 StGB, in : Niggli Marcel A. / Wiprächtiger (éds), *Basler Kommentar, Strafrecht II, Art. 137-392 StGB, Jugendstrafgesetz,* Bâle 2019.

NIGGLI Marcel A. / MAEDER Stefan, art. 12 StGB, in : Niggli Marcel A. / Wiprächtiger Hans (éds), *Basler Kommentar, Strafrecht I, Art. 1-136 StGB,* Bâle 2019.

NIGGLI Marcel A. / WIPRÄCHTIGER Hans (éds), *Basler Kommentar, Strafrecht II, Art. 137-392 StGB, Jugendstrafgesetz,* Bâle 2019.

OBERHOLZER Niklaus, art. 320, 321 StGB, in : Niggli Marcel A. / Wiprächtiger Hans (éds), *Basler Kommentar, Strafrecht II, Art. 137-392 StGB, Jugendstrafgesetz,* Bâle 2019.

OBERSON ABELS, *Enquête administrative « Fuite de données », Rapport à l'attention de l'Organe de coordination (SG-DFF),* 28 mars 2024 (cité : OA, *Enquête administrative « Fuite de données »,* 2024).

ODERMATT Luzian, art. 22 ParlG, in : Graf Martin / Theler Cornelia / Von Wyss Moritz (éds), *Parlamentsrecht und Parlamentspraxis der Schweizerischen Bundesversammlung, Kommentar zum Parlamentsgesetz (ParlG) vom 13. Dezember 2002,* Bâle 2014.

OESCH Matthias / RUFF Fränzi, art. 102 BV, in : Waldmann Bernhard / Besler Eva M. / Epiney Astrid (éds), *Basler Kommentar, Bundesverfassung,* Bâle 2015.

PAHUD Joël / PITTET Sébastien, *Les infractions pénales de la loi sur la protection des données,* Jusletter 25 septembre 2023.

PAREIN-REYMOND Aude / PAREIN Loïc / VUILLE Joëlle, art. 221 CP, in : Macaluso Alain et al. (éds), *Commentaire romand, Code pénal II, Art. 111-392 CP,* Bâle 2017.

PÄRLI Kurt, *Observation im Arbeitsverhältnis,* in : Kieser Ueli / Pärli Kurt / Uttinger Ursula (éds), *Datenschutztagung 2017, Baustelle Datenschutz – Observation als Brennpunkt,* Zurich/Saint-Gall 2017.

PERRAY Romain / ARZUAGA Pilar, *Regulating Cybersecurity across the EU and the UK,* janvier 2023.

PERRIER DEPEURSINGE Camille et al. (éds)
– *Cimes et Châtiments,* Berne 2022.
– *Lutter contre la cybercriminalité en Suisse,* Berne 2024, à paraître.

PERRIN Bertrand / ROUBATY Romain, *Accès indu à un système informatique, soustraction et détérioration de données : contribution à la résolution de quelques questions interprétatives,* in : Jaquier Sébastien / Beaudet-Labrecque / Zbinden Renaud (éds), *Criminalité économique et cybercriminalité – Mélanges en l'honneur de la professeure Isabelle Augsburger-Bucheli,* Bâle 2021, p. 203 ss.

PICHONNAZ Pascal
– art. 97 Cst, in : Martenet Vincent / Dubey Jacques (éds), *Commentaire Romand, Constitution fédérale, Art. 81 Cst. – dispositions finales,* Bâle 2021.
– *Les contrats innommés : quelques questions récurrentes,* in : Pichonnaz Pascal / Werro Franz (éds), La pratique contractuelle : actualité et perspectives, Symposium en droit des contrats, Genève/Zurich/Bâle 2009, p. 21 ss.

PICHONNAZ Pascal / WERRO Franz (éds), *La pratique contractuelle : actualité et perspectives, Symposium en droit des contrats,* Genève/Zurich/Bâle 2009.

PIETH Mark / TRECHSEL Stefan (éds.), *Schweizerisches Strafgesetzbuch, Praxiskommentar,* 4e édition, Zurich 2021.

POLTIER Étienne, *La responsabilité de l'État pour acte illicite* : l'exigence de l'illicéité, in : Favre Anne-Christine / Martenet Vincent / Poltier Étienne (éds), *La responsabilité de l'État,* Genève/Zurich/Bâle 2012, p. 45 ss.

RAEDLER David, art. 49 LPD, in : Meier Philippe / Métille Sylvain (éds), *Commentaire Romand, Loi fédérale sur la protection des données,* Bâle 2023.

RAMPINI Corrado / FUCHS Philippe / KUNZ Christian, art. 19 DSG, in : Blechta Gabor P. / Vasella David (éds), *Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz,* 4e édition, Bâle 2024.

RASHID Zahid / NOOR Umara / ALTMANN Jörn, *Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem,* Future Generation Compure Systems, vol. 24, novembre 2021, p. 436 ss.

RIBAUX Olivier / SOUVIGNET Thomas, *Transformations numériques et changements d'échelles. L'exponentielle et ses consequences pour les pratiques pénales,* in: Perrier Depeursinge et al. (éds), *Lutter contre la cybercriminalité en Suisse,* Berne 2024, à paraître.

RICHA Alexandre / CANAPA Damiano (éds)
– *Aspects juridiques de l'intelligence artificielle,* Berne 2024.
– *Droit et économique numérique,* Berne 2021.

ROSENTHAL David, *Controller oder Processor : Die datenschutzerchtliche Gretchenfrage,* Jusletter 17 juin 2019.

RUDIN Beat, art. 3 DSG, in : Baeriswyl Bruno / Pärli Kurt (éds), *Datenschutzgesetz (DSG), Stämpflis Handkommentar,* Berne 2015.

SALAMON Yann, *Cybersécurité cyberdéfense – Enjeux stratégiques,* Paris 2020.

SANGIORGIO Didier / REUTTER Mark A., *Service Level Agreements,* in : Jörg Florian S. / Arter Oliver (éds), *Internet-Recht und IT-Verträge,* Berne 2009, p. 97 ss.

SARRASIN Delphine / PANGRAZZI Sara / MEYER Pauline, *The Legal Risks of Ransomware Payments,* AJP/PJA 9/2023, p. 1077 ss.

SCHUBART Martin, art. 110 CP, in : Moreillon Laurent et al. (éds), *Commentaire Romand, Code pénal I, Art. 1-110 CP,* Bâle 2021.

SHARMA Himanshu / SINGH Harpreet, *Hands-On Red Team Tactics, A practical guide to mastering Red Team operations,* Birmingham 2018.

SKOPIK Florian / SETTANNI Giuseppe / FIEDLER Roman, *A problem shared is a problem halved : A survey on the dimensions of collective cyber defense through security information,* Computers & Security 60 (2016), p. 154 ss.

SOLOVE Daniel J. / HARTZOG Woodrow, *Breached !, Why Data Security Law Fails and How to Improve It,* New York 2022.

SPAS Mark, *Phénomènes cybercriminels, Descriptions et réponses juridiques,* Jusletter 10 novembre 2014.

STAIGER Dominic N., *Swiss Data Protection Law,* in : Moura Vincente Dário / de Vasconcelos Casimiro Sofia (éds), *Data Protection in the Internet,* vol. 38, 2020, p. 397 ss.

STAMM-PFISTER Christa, art. 8 DSG, in : Blechta Gabor P. / Vasella David (éds), *Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz,* 4e édition, Bâle 2024.

STAUB Roger, *IP-Klauseln/Datenschutz in IT-Verträgen,* in : Jörg Florian S./Arter Oliver (éds), *Internet-Recht und IT-Verträge,* Berne 2009, p. 179 ss.

STÖCKLI Andreas / GRÜNINGER Christoph, art. 33 DSG, in : Blechta Gabor P. / Vasella David (éds), *Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz,* 4e édition, Bâle 2024.

STRATENWERTH Günter, art. 47 BankG, in : Watter Rolf et al. (éds), *Basler Kommentar, Bankengesetz,* Bâle 2013.

STRAUB Wolfgang
- *Gewährleistung und Haftung aus IT-Verträgen,* in : Jörg Florian S./Arter Oliver (éds), *Internet-Recht und IT-Verträge,* Berne 2009, p. 237 ss (cité : STRAUB, *Gewährleistung und Haftung aus IT-Verträgen,* 2009).
- *Verantwortung für Informationstechnologie – Gewährleistung, Haftung und Verantwortlichkeitsansprüche,* Zurich/Saint-Gall 2008 (cité : STRAUB, *Verantwortung für Informationstechnologie,* 2008).
- *Verträge für agil geführte Projekte,* Jusletter 21 décembre 2015 (cité : STRAUB, *Verträge für agil geführte Projekte,* 2015).

SUBILIA-BIGLER Nathalie, *La location de services et le placement transfrontalier,* in : Wyler Rémy (éd.), *Panorama II en droit du travail, Recueil d'études réalisées par des praticiens,* Berne 2012, p. 553 ss.

SURY Ursula
- *Digital in Law – Informatikrecht,* 2e édition, Berne 2021 (citée : SURY, *Digital in Law,* 2021).
- *Informatikrecht,* Berne 2013 (citée : SURY, *Informatikrecht,* 2013).

SVANTESSON Dan Jerker B., art. 3 in : Kuner Christopher / Bygrave Lee A. / Docksey (éds), *The EU General Data Protection Regulation (GDPR) – A Commentary,* Oxford 2020.

TEICHMANN Fabian / GERBER Léonard
- *Cybercriminalité en Suisse – Le phishing,* Jusletter IT 27 mai 2021 (cités : TEICHMANN/GERBER, *Le phishing,* 2021).

– *La qualification pénale des attaques DDoS en droit suisse,* Jusletter 27 septembre 2021 (cités : TEICHMANN/GERBER, *La qualification pénale des attaques DDoS en droit suisse,* 2021).
– *Les attaques classiques par ransomware,* Jusletter 7 juin 2021 (cités : TEICHMANN/GERBER, *Les attaques classiques par ransomware,* 2021).
– *Les chevaux de Troie – Un danger pour les tribunaux helvétiques?,* Jusletter IT 16 décembre 2021 (cités : TEICHMANN/GERBER, *Les chevaux de Troie,* 2021).

TERCIER Pierre / BIERI Laurent / CARRON Blaise, *Les contrats spéciaux,* 2e édition, Genève/Zurich/Bâle 2016.

THÉVENOZ Luc, art. 101 CO, in : Thévenoz Luc / Werro Franz (éds), *Commentaire Romand, Code des Obligations I, Art. 1-529 CO,* Bâle 2021.

THÉVENOZ Luc / WERRO Franz (éds), *Commentaire Romand, Code des Obligations I, Art. 1-529 CO,* Bâle 2021.

TIRELLI Ludovic, art. 355*a* CP, in : Macaluso Alain et al. (éds), *Commentaire romand, Code pénal II, Art. 111-392 CP,* Bâle 2017.

TRECHSEL Stefan / JEAN-RICHARD Marc, art. 102 StGB, in : Pieth Mark / Trechsel Stefan (éds), *Schweizerisches Strafgesetzbuch, Praxiskommentar,* 4e édition, Zurich 2021.

TSCHIDER Charlotte A., *Regulating the Internet of Things: Discrimination, Privacy, And Cybersecurity In The Artifical Intelligence Age,* Denver Law Review 96 (2018-2019), p. 87 ss.

VAN DE POEL Ibo, *Core Values and Value Conflicts in Cybersecurity : Beyond Privacy Versus Security,* in : Christen Markus / Gordijn Bert / Loi Michele (éds), *The Ethics of Cybersecurity,* 2021, p. 45 ss.

VAN DER KLEIJ Rick / KLEINHUIS Geert / YOUNG Heather, *Computer Security Incident Response Team Effectiveness : A Needs Assessment,* Frontiers in Psychology, vol. 8, article 2179, 2017, p. 1 ss.

VERNIORY Jean-Marc, Art. 320 CP, in : Macaluso Alain et al. (éds), *Commentaire romand, Code pénal II, Art. 111-392 CP,* Bâle 2017.

VON OW Andreas, *Konzepte gegen Cyberspace-Angriffe,* digma octobre 2015, cahier 3, p. 86 ss.

VOYAME Claudine, *Accords de confidentialité,* L'expert-comptable suisse 4/14, p. 341 ss.

WAGNER Ben / KETTERMANN Matthias C. / VIETH Kilian (éds), *Research Handbook on Human Rights and Digital Technology – Global Politics, Law and International Relations*, Janvier 2019.

WALDMANN Bernhard / BESLER Eva M. / EPINEY Astrid (éds), *Basler Kommentar, Bundesverfassung,* Bâle 2015.

WATTER Rolf et al. (éds), *Basler Kommentar, Bankengesetz,* Bâle 2013.

WATTER Rolf (éd.), *Basler Kommentar, Finanzmarktaufischtgesetz, Finanzmarktinfrastrukturgesetz,* Bâle 2019.

WEBER Claude, *La place de l'homme dans les enjeux de cybersécurité,* Stratégique 2017/4, N 17, p. 83 ss.

WEBER Rolf H. / YILDIZ Okan, *Cybersicherheit und Cyber-Resilienz in den Finanzmärkten,* Zurich 2022.

WEBER Rolf H. / WILLI Annette, *IT-Sicherheit und Recht – Grundlagen eines integrativen Gestaltungskonzepts,* Zurich/Bâle/Genève 2006.

WEISSENBERGER Philippe, art. 143, 143*bis* StGB, in : Niggli Marcel A./Wiprächtiger Hans (éds), *Basler Kommentar, Strafrecht II, Art. 137-392 StGB, Jugendstrafgesetz,* Bâle 2019.

WERLY Stéphane / BARRELET Denis, *Droit de la communication,* 3e édition, Berne 2024.

WERRO Franz, art. 394, in : Thévenoz Luc / Werro Franz (éds), *Commentaire Romand, Code des Obligations I, Art. 1-529 CO,* Bâle 2021.

WERRO Franz / PERRITAZ Vincent, art. 55 CO, in : Thévenoz Luc / Werro Franz (éds), *Commentaire Romand, Code des Obligations I, Art. 1-529 CO,* Bâle 2021.

WEST-BROWN Moira J. et al., *Handbook for Computer Security Incident Response Teams (CSIRT),* Carnegie Mellon Software Engineering Institute, avril 2003.

WIDMER Michael, art. 7 DSG, in : Blechta Gabor P. / Vasella David (éds), *Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz,* 4e édition, Bâle 2024.

WINZELER Christoph, art. 7 FINMAG, in : Watter Rolf (éd.), *Basler Kommentar, Finanzmarktaufischtgesetz, Finanzmarktinfrastrukturgesetz,* Bâle 2019.

WISCHMEYER Thomas, *Informationssicherheit,* Tübingen 2023.

WITZIG Aurélien, art. 321*e* CO, in : Thévenoz Luc / Werro Franz (éds), *Commentaire Romand, Code des Obligations I, Art. 1-529 CO,* Bâle 2021.

WYLER Rémy (éd.)
– *Panorama II en droit du travail, Recueil d'études réalisées par des praticiens,* Berne 2012.
– *Panorama III en droit du travail, Recueil d'études réalisées par des praticiens,* Berne 2017.

WYLER Rémy / HEINZER Boris, *Droit du travail,* 4e édition, Berne 2019.

WYTTENBACH Judith / WYSS Karl-Marc, art. 164 Cst., in : Waldmann Bernhard / Besler Eva M. / Epiney Astrid (éds.), *Basler Kommentar, Bundesverfassung,* Bâle 2015.

YOUNG Derek et al., *A framework for incorporating insurance in critical infrastructure cyber risk strategies,* International Journal of Critical Infrastructure Protection 14 (2016), p. 43 ss.

ZIEGLER Andreas R., art. 101, 102 Cst., in : Martenet Vincent / Dubey Jacques (éds.), *Commentaire Romand, Constitution fédérale, Art. 81 Cst. – dispositions finales,* Bâle 2021.

ZIMMERMANN Robert, *La coopération judiciaire internationale en matière pénale,* Berne 2019.

ZUFFEREY Jean-Baptiste / CONTRATTO Franca, *FINMA, The Swiss Financial Market Supervisory Authority,* Bâle 2009.

ZUFFEREY Jean-Baptiste, *Nouveau droit (fédéral) des marchés publics : faire du neuf avec de l'ancien ? Un peu plus tout de même,* Revue du droit de la construction et des marchés publics, février 2020, p. 5 ss.

Documentations

ADMINISTRATION FÉDÉRALE DES FINANCES
– *Fédéralisme/Subsidiarité « D'où vient la Suisse ? »,* septembre 2004 (citée : AFF, *Fédéralisme/Subsidiarité « D'où vient la Suisse ? »,* 2004).
– *Manuel de gestion des risques de la Confédération,* 14 septembre 2020 (citée : AFF, *Manuel de gestion des risques de la Confédération,* 2020).
– *Manuel de gestion des risques de la Confédération,* 24 septembre 2021 (citée : AFF, *Manuel de gestion des risques de la Confédération,* 2021).
– *Manuel de gestion des risques de la Confédération,* 22 mars 2022 (citée : AFF, *Manuel de gestion des risques de la Confédération,* 2022).

AGENCE EUROPÉENNE POUR LA CYBERSÉCURITÉ
- *Baseline Capabilities of National/Governmental CERT (Part 2 : Policy Recommandations),* 17 décembre 2010 (citée : ENISA, *Baseline Capabilities of National/Governmental CERT, Part 2,* 2010).
- *Cyber Insurance : Recent Advances, Good Practices and Challenges,* novembre 2016 (citée : ENISA, *Cyber Insurance : Recent Advances, Good Practices and Challenges,* 2016).
- *Electronic evidence – A basic guide for First Responders,* mars 2015 (citée : ENISA, *Electronic evidence,* 2015).
- *Good Practice Guide for Incident Management,* décembre 2010 (citée : ENISA, *Good Practice Guide for Incident Management,* 2010).
- *Good practices in the innovation under NCSS – Good practices in innovation on cybersecurity under the national cyber security strategies,* novembre 2019 (citée : ENISA, *Good practices in innovation on cybersecurity under the national cyber security strategies,* 2019).
- *How to set up CSIRT and SOC – Good practice guide,* novembre 2020 (citée : ENISA, *How to set up CSIRT and SOC,* 2020).
- *Information Sharing and Analysis Centres (ISAC), Cooperative models,* février 2018 (citée : ENISA, *ISAC,* 2018).
- *National Capabilities Assessment Framework,* décembre 2020 (citée : ENISA, *National Capabilities Assessment Framework,* 2020).
- *National Cyber Security Strategies – Setting the course for national efforts to strengthen security in cyberspace,* 2012 (citée : ENISA, *National Cyber Security Strategies,* 2012).
- *National/governmental CERT – ENISA's recommendations on baseline capabilities,* décembre 2014 (citée : ENISA, *National/governmental CERT,* 2014).
- *NCSS Good Practice Guide – Designing and Implementing National Cyber Security Strategies,* novembre 2016 (citée : ENISA, *NCSS Good Practice Guide,* 2016).
- *Public Private Partnerships (PPP) – Cooperative models,* novembre 2017 (citée : ENISA, *PPP,* 2017).
- *Recommendations on European Data Protection Certification,* version 1.0, novembre 2017 (citée : ENISA, *Recommendations on European Data Protection Certification,* 2017).
- *Roadmap on the cooperation between CSIRT and LE,* décembre 2019 (citée : ENISA, *Roadmap on the cooperation between CSIRT and LE,* 2019).

ALBERTS Chris et al., *Defining Incident Management Processes for CSIRTs: A Work in Progress,* Software Engineering Institute, 1er octobre 2004.

ASSOCIATION SUISSE DE NORMALISATION, *Normalisation et droit – Le statut juridique des normes,* juillet 2013 (citée : SNV, *Le statut juridique des normes,* 2013).

ARMÉE SUISSE, *Conception générale cyber, Conception du développement des capacités de l'Armée suisse, dans le cyberespace et l'espace électromagnétique (CYBEEM) d'ici au milieu des années 2030,* 2023 (citée : ARMÉE SUISSE, *Conception générale cyber,* 2023).

AUTORITÉ FÉDÉRALE DE SURVEILLANCE DES MARCHÉS FINANCIERS, *Communication FINMA sur la surveillance 03/2024, Enseignements tirés de l'activité de surveillance des cyberrisques, précisions sur la communication FINMA sur la surveillance 05/2020 et sur les cyberexercices fondés sur des scénarios,* 7 juin 2024 (cité : FINMA, *Communication sur la surveillance 03/2024,* 2024).

AUTORITÉ FÉDÉRALE DE SURVEILLANCE DES MARCHÉS FINANCIERS, *Rapport annuel 2022,* mars 2023 (citée : FINMA, *Rapport annuel 2022,* 2023).

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK, *Informationssicherheit mit System, Der IT-Grundschutz des BSI,* 15 juin 2021 (cité : BSI, *Informationssicherheit mit System,* 2021).

CENTER FOR STRATEGIC & INTERNATIONAL STUDIES, *Economic Impact of Cybercrime – No Slowing Down,* février 2018 (cité : CSIS/MCAFEE, *Economic Impact of Cybercrime – No Slowing Down,* 2018).

CENTRE DE COMPÉTENCE DES MARCHÉS PUBLICS DE LA CONFÉDÉRATION

- *Conditions générales pour l'acquisition et la maintenance de logiciels standard,* 5 décembre 2023 (cité : CCMP, *Conditions générales pour l'acquisition et la maintenance de logiciels standard,* 2023).
- *Conditions générales pour les services informatiques,* 5 décembre 2023 (cité : CCMP, *Conditions générales pour les services informatiques,* 2023).
- *Révision des CG au 1er janvier 2024 – vue d'ensemble,* 1er décembre 2023 (cité : CCMP, *Révision des CG au 1er janvier 2024,* 2023).

CENTRE NATIONAL POUR LA CYBERSÉCURITÉ

- *Évaluation de l'efficacité de la stratégie nationale de protection de la Suisse contre les cyberrisques pour les années 2018 à 2022,* 28 mars 2022 (cité : NCSC, *Évaluation de l'efficacité de la stratégie nationale de protection de la Suisse contre les cyberrisques pour les années 2018 à 2022,* 2022).
- *Liste de contrôle et instructions, Mesures de protection pour les systèmes de contrôle industriels (SCI),* décembre 2020 (cité : NCSC, *Mesures de protection pour les SCI,* 2020).

– *Rapport explicatif relatif à l'ouverture de la procédure de consultation, Modification de la loi fédérale du 18 décembre 2020 sur la sécurité de l'information au sein de la Confédération (loi sur la sécurité de l'information, LSI), Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques,* 12 janvier 2022 (cité : NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques,* 2022).
– *Rapport semestriel 2020/2 de juillet à décembre,* 11 mai 2021 (cité : NCSC, *Rapport semestriel 2020/2,* 2021).
– *Rapport semestriel 2021/1 de janvier à juin,* 2 novembre 2021 (cité : NCSC, *Rapport semestriel 2021/1,* 2021).
– *Rapport semestriel 2021/2 de juillet à décembre 2021,* 5 mai 2022 (cité : NCSC, *Rapport semestriel 2021/2,* 2022).
– *Rapport semestriel 2022/1 de janvier à juin 2022,* 3 novembre 2022 (cité : NCSC, *Rapport semestriel 2022/1,* 2022).
– *Rapport semestriel 2022/II de juillet à décembre 2022,* 11 mai 2023 (cité : NCSC, *Rapport semestriel 2022/2,* 2023).
– *Rapport semestriel 2023/I (janvier à juin),* 2 novembre 2023 (cité : NCSC, *Rapport semestriel 2023/I,* 2023).
– *Rapport sur la sécurité informatique de la Confédération 2021,* 13 avril 2022 (cité : NCSC, *Rapport sur la sécurité informatique de la Confédération,* 2021).

CHANCELLERIE FÉDÉRALE

– *Cadre juridique pour l'utilisation de services d'informatique en nuage public au sein de l'administration fédérale, Rapport en exécution du jalon 5 de la stratégie d'informatique en nuage du Conseil fédéral,* 31 août 2022 (citée : ChF, *Cadre juridique pour l'utilisation de services d'informatique en nuage public au sein de l'administration fédérale,* 2022).
– *Directives de la Confédération sur la technique législative (DTL),* 2013 (citée : ChF, *DTL,* 2013).
– *Objectifs du Conseil fédéral 2024,* 21 septembre 2023 (citée: ChF, *Objectifs du Conseil fédéral 2024,* 2023).
– *Révision partielle de l'ordonnance sur les droits politiques et révision totale de l'ordonnance de la ChF sur le vote électronique (restructuration de la phase d'essai), Rapport explicatif en vue de l'entrée en vigueur au 1er juillet 2022,* 25 mai 2022 (citée : ChF, *Révision partielle de l'ordonnance sur les droits politiques et révision totale de l'ordonnance de la ChF sur le vote électronique,* 2022).

– *Rapport « Suisse 2035, les grands défis de demain en 20 questions »,* 25 mai 2022 (citée : ChF, *Rapport « Suisse 2035, les grands défis de demain en 20 questions »,* 2022).
– *Stratégie Suisse numérique 2023,* 16 décembre 2022 (citée : ChF, *Stratégie Suisse numérique 2023,* 2022).

COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, *Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, version 2.0,* 7 juillet 2021 (cité : CEPD, *Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD,* version 2.0, 2021).

COMMISSIONS DE GESTION DES CHAMBRES FÉDÉRALES, *Rapport sur les risques à l'intention du Conseil fédéral – Etat des lieux, Rapport des Commissions de gestion des Chambres fédérales,* 30 janvier 2018 (citée : FF 2018 1433).

COMMISSION DE L'ÉCONOMIE ET DES REDEVANCES DU CONSEIL NATIONAL, *Initiative parlementaire, Réprimer durement la vente de données bancaires, Rapport de la Commission de l'économie et des redevances du Conseil national,* 19 mai 2014 (citée : FF 2014 5997).

COMMISSION EUROPÉENNE
– *Factsheet : The EU's Cybersecurity Strategy for the digital decade,* 16 décembre 2020 (citée : COMMISSION EUROPÉENNE, *Factsheet : The EU's Cybersecurity Strategy for the digital decade,* 2020).
– *Rapport de la Commission au Parlement européen et au Conseil sur le premier réexamen du fonctionnement des décisions d'adéquation adoptées sur la base de l'article 25, paragraphe 6, de la directive 95/46/CE,* 15 janvier 2024 (citée : COMMISSION EUROPÉENNE, *Rapport de la Commission au Parlement européen et au Conseil sur le premier réexamen du fonctionnement des décisions d'adéquation,* 2024).

COMMISSION FÉDÉRALE DE L'ÉLECTRICITÉ, *Cyber-Sicherheit 2019, Bericht der ElCom,* février 2019 (citée : ELCOM, *Cyber-Sicherheit 2019,* 2019).

COMMISSION INTERNATIONALE ÉLECTROTECHNIQUE, *Cyber security,* 9 mars 2018 (citée : IEC, *Cyber security,* 2018).

CONFÉRENCE DES ACHATS DE LA CONFÉDÉRATION, *Clause contractuelle type de la CA pour les cyberattaques,* 29 février 2024 (citée : CA, *Clause contractuelle type de la CA pour les cyberattaques,* 2024).

CONSEIL FÉDÉRAL

– *Capacité de défense et coopération, Rapport du Conseil fédéral en réponse aux postulats 23.3000 CPS-E du 12 janvier 2023 et 23.3131 Dittli du 14 mars 2023,* 31 janvier 2024 (cité : CF, *Capacité de défense et coopération,* 2024).
– *Culture de l'erreur : possibilités et limites de son ancrage juridique, Rapport du Conseil fédéral donnant suite au postulat 20.3463 (CAJ-E) du 25.05.2020,* 9 décembre 2022 (cité : CF, *Culture de l'erreur : possibilités et limites de son ancrage juridique,* 2022).
– *Cyberstratégie nationale (CSN),* avril 2023 (cité : CF, *CSN,* 2023).
– *Délégation du Conseil fédéral pour la sécurité, Mandat et organisation,* 25 janvier 2023 (cité : CF, *Délégation du Conseil fédéral pour la sécurité,* 2023).
– *Infrastructure numérique. Réduire les risques géopolitiques, Rapport du Conseil fédéral donnant suite au postulat 20.3984 Pult du 14.9.2020,* 15 décembre 2023 (cité : CF, *Infrastructure numérique. Réduire les risques géopolitiques,* 2023).
– *« Intelligence artificielle » – lignes directrices pour la Confédération, Cadre d'orientation en matière d'IA dans l'administration fédérale,* 25 novembre 2020 (cité : CF, *« Intelligence artificielle » – lignes directrices pour la Confédération,* 2020).
– *La FINMA et son activité de réglementation et de surveillance, Rapport en réponse aux postulats 12.4095 Graber Konrad, 12.4121 de Courten, 12.4122 Schneeberger et 13.3282 de Buman,* 18 décembre 2014 (cité : CF, *La FINMA et son activité de réglementation et de surveillance,* 2014).
– *La promotion du piratage éthique en Suisse, Rapport du Conseil fédéral en réponse au postulat 20.4594 du 17 décembre 2020,* 29 novembre 2023 (cité : CF, *La promotion du piratage éthique en Suisse,* 2023).
– *Message concernant la loi fédérale sur l'Autorité fédérale de surveillance des marchés financiers (LAUFIN),* 1er février 2006 (cité : FF 2006 2741).
– *Message concernant la loi fédérale sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités,* 4 mars 2022 (cité : FF 2022 804).
– *Message concernant la loi fédérale sur le dossier électronique du patient (LDEIP),* 29 mai 2013 (cité : FF 2013 4747).
– *Message concernant la loi sur la sécurité de l'information,* 22 février 2017 (cité : FF 2017 2765).
– *Message concernant la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT),* 27 février 2013 (cité : FF 2013 2379).
– *Message concernant la loi sur la sécurité des produits (Révision totale de la loi fédérale sur la sécurité d'installations et d'appareils techniques),* 25 juin 2008 (cité : FF 2008 6771).

- *Message concernant la loi sur le personnel de la Confédération (LPers) du 14 décembre 1998,* 14 décembre 1998 (cité : FF 1999 1421).
- *Message concernant la modification de la loi fédérale sur la libre circulation des avocats,* 26 octobre 2005 (cité : FF 2005 6207).
- *Message concernant la révision de la loi sur les télécommunications,* 6 septembre 2017 (cité : FF 2017 6185).
- *Message concernant la révision de la loi fédérale sur la protection des données personnelles (LPD) et à l'arrêté fédéral concernant l'adhésion de la Suisse au Protocole additionnel du 8 novembre 2001 à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données,* 19 février 2003 (cité : FF 2003 1915).
- *Message concernant la révision de la loi sur les télécommunications,* 6 septembre 2017 (cité : FF 2017 6185).
- *Message concernant la révision totale de la loi fédérale sur les marchés publics,* 15 février 2017 (cité : FF 2017 1695).
- *Message concernant les initiatives populaires « Moratoire Plus – Pour la prolongation du moratoire dans la construction de centrales nucléaires et la limitation du risque nucléaire (Moratoire-plus) » et « Sortir du nucléaire – Pour un tournant dans le domaine de l'énergie et pour la désaffectation progressive des centrales nucléaires (Sortir du nucléaire) » et concernant la loi sur l'énergie nucléaire,* 28 février 2001 (cité : FF 2001 2529).
- *Message relatif à l'approbation et à la mise en œuvre de la Convention de l'Europe sur la cybercriminalité,* 18 juin 2010 (cité : FF 2010 4275).
- *Message relatif à la modification de la loi sur la sécurité de l'information (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques),* 2 décembre 2022 (cité : FF 2023 84).
- *Message relatif à la modification de la loi sur les télécommunications,* 12 novembre 2003 (cité : FF 2003 7245).
- *Message relatif à la modification des bases légales concernant le développement de l'armée,* 3 septembre 2014 (cité : FF 2014 6693).
- *Message relatif à une modification de la loi sur l'armée et de l'Organisation de l'armée,* 1er septembre 2021 (cité : FF 2021 2198).
- *Message relative à la révision de la loi fédérale sur la protection des données (LPD) et à l'arrêté fédéral concernant l'adhésion de la Suisse au Protocole additionnel du 8 novembre 2001 à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données,* 19 février 2003 (cité : FF 2003 1915).

– *Message relatif à la révision de la loi sur les cartels,* 7 novembre 2001 (cité : FF 2002 1911).
– *Message sur la loi sur le renseignement,* 19 février 2014 (cité : FF 2014 2029).
– *Normes de sécurité pour les appareils connectés à Internet (Internet des objets), Rapport en réponse aux postulats Glättli 17.4295 du 15 décembre 2017 et Reynard 19.3199 du 21 mars 2019,* 29 avril 2020 (cité : CF, *Normes de sécurité pour les appareils connectés à Internet,* 2020).
– *Plan de mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022,* mai 2019 (cité : CF, *Plan de mise en œuvre de la SNPC 2018-2022,* 2019).
– *Poursuites pénales en matière de cybercriminalité. Efficacité des cantons, Rapport du Conseil fédéral donnant suite au postulat 22.3145, Andri Silberschmidt, 16 mars 2022 et 22.3017, Commission de la politique de sécurité du Conseil national, 15 février 2022,* 19 juin 2024 (cité : CF, *Poursuites pénales en matière de cybercriminalité,* 2024).
– *Rapport du Conseil fédéral donnant suite au postulat Malama 10.3045 du 3 mars 2010 Sécurité intérieure. Clarification des compétences,* 2 mars 2012 (cité : FF 2012 4161).
– *Rapport « La politique de sécurité de la Suisse »,* 14 avril 2021 (cité : CF, *Rapport « La politique de sécurité de la Suisse »,* 2021).
– *Rapport « Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense » en réponse aux postulats Dobler 19.3135 « Acquisitions de l'armée. Avons-nous la maîtrise de la cybersécurité ? » et 19.3136 « Infrastructures critiques. Avons-nous lad maîtrise des composants matériels et logiciels ? » du 18 mars 2019,* novembre 2021 (cité : CF, *Rapport « Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense »,* 2021).
– *Rapport « Obligation de déclarer les incidents graves affectant la sécurité des infrastructures critiques : solutions possibles » en réponse au postulat 17.3475 Graf-Litscher du 15 juin 2017,* 13 décembre 2019 (cité : CF, *Rapport « Obligation de déclarer les incidents graves affectant la sécurité des infrastructures critiques »,* 2019).
– *Rapport sur l'avancement des travaux concernant la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022,* état au deuxième semestre 2021, août 2021 (cité : CF, *Rapport sur l'avancement des travaux concernant la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022,* 2021).
– *Rapport sur l'avancement des travaux concernant la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022,* état au

premier semestre 2020, octobre 2020 (cité : CF, *Rapport sur l'avancement des travaux concernant la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022,* 2020).
– *Stratégie d'approvisionnement informatique de la Confédération 2018-2022,* mai 2018 (cité : CF, *Stratégie d'approvisionnement informatique de la Confédération 2018-2022,* 2018).
– *Stratégie d'informatique en nuage de l'administration fédérale,* décembre 2020 (cité : CF, *Stratégie d'informatique en nuage de l'administration fédérale,* 2020).
– *Stratégie en matière de libre accès aux données publiques en Suisse pour les années 2019 à 2023 (Stratégie Open government data, OGD),* 30 novembre 2018 (cité : FF 2019 855).
– *Stratégie nationale de protection de la Suisse contre les cyberrisques 2018-2022,* avril 2018 (cité : CF, *SNPC 2018-2022,* 2018).
– *Stratégie nationale de protection des infrastructures critiques, Approche globale pour garantir l'approvisionnement en biens et prestations essentiels,* 16 juin 2023 (cité : FF 2023 1659).
– *Stratégie nationale pour la protection des infrastructures critiques 2018-2022,* 8 décembre 2017 (cité : FF 2018 491).
– *Stratégie numérique de la Confédération 2020-2023,* septembre 2021 (cité : CF, *Stratégie numérique de la Confédération 2020-2023,* 2021).
– *Stratégie « Suisse numérique »,* 20 avril 2016 (cité : FF 2016 3801).
– *Stratégie Suisse numérique 2024,* décembre 2023 (cité : FF 2023 2830).

CONTRÔLE FÉDÉRAL DES FINANCES
– *Audit de l'efficacité de la lutte contre la cybercriminalité – Office fédéral de la police,* 1er mars 2021 (cité : Cff, *Audit de l'efficacité de la lutte contre la cybercriminalité,* 2021).
– *Audit de la protection des infrastructures critiques – Gouvernance et gestion des risques intégrale, Office fédéral de la protection de la population,* 7 février 2023 (cité : Cff, *Audit de la protection des infrastructures critiques,* 2023).
– *Audit de l'impact de l'intégration de l'exploitation de la BAC dans l'OFIT en termes de fiabilité, Office fédéral de l'informatique et de la télécommunication, Base d'aide au commandement et État-major de l'armée,* 14 décembre 2023 (cité : Cff, *Audit de l'impact de l'intégration de l'exploitation de la BAC dans l'OFIT en termes de fiabilité,* 2023).

DÉPARTEMENT FÉDÉRAL DE JUSTICE ET POLICE, *Stratégie de lutte contre la cybercriminalité 2020-2023,* décembre 2019 (cité : DFJP, *Stratégie de lutte contre la cybercriminalité 2020-2023,* 2020).

DÉPARTEMENT FÉDÉRAL DE L'ENVIRONNEMENT, DES TRANSPORTS, DE L'ÉNERGIE ET DE LA COMMUNICATION

- *Rapport explicatif concernant l'avant-projet relatif à la révision de mai 2024 de l'ordonnance sur l'approvisionnement en électricité (protection contre les cybermenaces)*, 21 septembre 2023 (cité : DETEC, *Rapport explication concernant l'avant-projet relatif à la révision de mai 2024 de l'ordonnance sur l'approvisionnement en électricité,* 2023).
- *Rapport explicatif relatif à la révision de novembre 2023 de l'ordonnance concernant les prescriptions de sécurité pour les installations de transport par conduites*, avril 2023 (cité : DETEC, *Rapport explicatif relatif à la révision de novembre 2023 de l'ordonnance concernant les prescriptions de sécurité pour les installations de transport par conduites,* 2023).
- *Rapport explicatif sur l'Ordonnance sur les domaines Internet (ODI)*, 5 novembre 2014 (cité : DETEC, *Rapport explicatif sur l'ODI,* 2014).
- *Rapport sur les recommandations du groupe d'experts sur l'avenir du traitement et de la sécurité des données – Prise de connaissance et suite de la procédure,* 15 octobre 2019 (cité : DETEC, *Rapport sur les recommandations du groupe d'experts sur l'avenir du traitement et de la sécurité des données,* 2019).

DÉPARTEMENT FÉDÉRAL DE LA DÉFENSE, DE LA PROTECTION DE LA POPULATION ET DES SPORTS

- *Änderung der Organisationsverordnung für das VBS : Staatssekretariat für Sicherheitspolitik und Bundesamt für Cybersicherheit, Erläuterung der einzelnen Bestimmungen,* 22 novembre 2023 (cité : DDPS, *Änderung der Organisationsverordnung für das VBS : Staatssekretariat für Sicherheitspolitik und Bundesamt für Cybersicherheit,* 2023).
- *Plan d'action Cyberdéfense DDPS (PACD),* 9 novembre 2017 (cité : DDPS, *PACD,* 2017).
- *Stratégie Cyber VBS,* mars 2021 (cité : DDPS, *Stratégie Cyber VBS,* 2021).
- *Stratégie de protection de la Suisse contre les cyberrisques,* 19 juin 2012 (cité : DDPS, *SNPC,* 2012).

DÉPARTEMENT FÉDÉRAL DES AFFAIRES ÉTRANGÈRES, *Stratégie de politique extérieure numérique 2021-2024,* 4 novembre 2020 (cité : DFAE, *Stratégie de politique extérieure numérique 2021-2024,* 2020).

DÉPARTEMENT FÉDÉRAL DES FINANCES, *Erläuterungen zur Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung,* 27 mai 2020 (cité : DFF, *Erläuterungen zur Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung,* 2020).

DIRECTION GÉNÉRALE DES SYSTÈMES D'INFORMATION, *Politique de Sécurité de l'Information (PSI) de l'administration cantonale de Genève,* 17 décembre 2014 (cité : DGSI, *Politique de Sécurité de l'Information,* 2014).

EGOVERNMENT, *Stratégie suisse de cyberadministration 2020-2023,* 20 novembre 2019 (cité : EGOVERNMENT, *Stratégie suisse de cyberadministration 2020-2023,* 2019).

ETHOS
- *Étude Ethos – Responsabilité numérique des entreprises du SMI Expanded,* janvier 2022 (cité : ETHOS, *Étude Ethos – Responsabilité numérique des entreprises du SMI Expanded,* 2022).
- *Étude Ethos – Responsabilité numérique des entreprises du SMI Expanded,* février 2023 (cité : ETHOS, *Étude Ethos – Responsabilité numérique des entreprises du SMI Expanded,* 2023).

EUROPOL, *Internet Organised Crime Threat Assessment IOCTA 2021,* 7 décembre 2021 (cité : EUROPOL, *Internet Organised Crime Threat Assessment IOCTA 2021,* 2021).

FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS
- *Computer Security Incident Response Team (CSIRT) – Services Framework,* version 2.1, novembre 2019 (cité : FIRST, *CSIRT – Services Framework,* 2019).
- *FIRST Privacy Policy,* version 2, avril 2020 (cité : FIRST, *FIRST Privacy Policy,* 2020).
- *Traffic Light Protocol (TLP),* version 2.0, 2022 (cité : FIRST, *Traffic Light Protocol,* version 2.0, 2022).

GENEVA CENTRE FOR SECURITY POLICY, *Guide to Developing a National Cybersecurity Strategy,* 2e édition, 26 novembre 2021 (cité : GCSP, *Guide to Developing a National Cybersecurity Strategy,* 2021).

GLOBAL CYBER SECURITY CAPACITY CENTRE
- *Computer Security Incident Response Teams (CSIRT) – An Overview,* mai 2014 (cité : GCSCC, *CSIRT – An Overview,* 2014).
- *Cybersecurity capacity review – Switzerland,* juin 2020 (cité : GCSCC, *Cybersecurity capacity review – Switzerland,* 2020).

GLOBAL FORUM ON CYBER EXPERTISE, *GFCE Global Good Practices – National Computer Security Incident Response Teams (CSIRT),* 2017 (cité : GFCE, *GFCE Global Good Practices – National Computer Security Incident Response Teams (CSIRT),* 2017).

GLOBAL PARTNERS DIGITAL, *Involving Stakeholders in National Cybersecurity Strategies: A Guide for Policymakers,* mars 2020 (cité : GLOBAL PARTNERS DIGITAL, *Involving Stakeholders in National Cybersecurity Strategies: A Guide for Policymakers,* 2020).

GROUPE D'EXPERTS « AVENIR DU TRAITEMENT ET DE LA SÉCURITÉ DES DONNÉES », *Rapport du groupe d'experts concernant le traitement et la sécurité des données,* 17 août 2018 (cité : GROUPE D'EXPERTS « AVENIR DU TRAITEMENT ET DE LA SÉCURITÉ DES DONNÉES », *Rapport du groupe d'experts concernant le traitement et la sécurité des données,* 2018).

INSTITUT FÉDÉRAL DE LA PROPRIÉTÉ INTELLECTUELLE, *Accès aux données non personnelles dans le secteur privé,* 1er mars 2021 (cité : IPI, *Accès aux données non personnelles dans le secteur privé,* 2021).

INTERNATIONAL BUSINESS MACHINES CORPORATION, *Cost of a Data Breach Report 2021,* New York 2021 (citée : IBM, *Cost of a Data Breach Report 2021,* 2021).

JACCARD Michel/ANCELLE Juliette, *Rapport explicatif concernant les Contrats Modèles de partage de données techniques,* 31 août 2020.

KASTELIC ANDRAZ, *International Cooperation to Mitigate Cyber Operations against Critical Infrastructure, UNIDIR,* 6 avril 2021.

KRAL PATRICK, *Incident Handler's Handbook, SANS Institute,* 5 décembre 2011.

LUNDELL Michel, *Incident Handling as a Service,* SANS Institute, 11 février 2009.

MELANI, *Rapport semestriel 2007/2 « Sûreté de l'information, Situation en Suisse et sur le plan international » de juillet à décembre,* 8 mai 2008 (citée : MELANI, *Rapport semestriel 2007/2,* 2008).

MELANI/GOVCERT, *APT Case RUAG, Technical Report,* mai 2016 (citées : MELANI/GOVCERT, *APT Case RUAG,* 2016).

MICROSOFT (THREAT INTELLIGENCE), *Microsoft Digital Defense Report, Building and improving cyber resilience,* octobre 2023 (citée : MICROSOFT, *Microsoft Digital Defense Report,* 2023).

MORGUS Robert et al.
- *CSIRT Basics for Policy-Makers,* mai 2015 (cités : MORGUS et al., *CSIRT Basics for Policy-Makers,* 2015).
- *National CSIRT and Their Role in Computer Security Incident Response,* novembre 2015 (cités : MORGUS et al., *National CSIRT and Their Role in Computer Security Incident Response,* 2015).

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
– *Computer Security Incident Handling Guide – Recommendations of the National Institute of Standards and Technology,* August 2012 (cité : NIST, *Computer Security Incident Handling Guide,* 2012).
– *The Cybersecurity Framework 2.0,* 2023 (cité : NIST, *The NIST Cybersecurity Framework 2.0,* 2023).
– *Framework for Improving Critical Infrastructure Cybersecurity* – version 1.1, 16 avril 2018 (cité : NIST, *Framework for Improving Critical Infrastructure Cybersecurity,* 2018).
– *Guide to Industrial Control Systems (ICS) Security – Supervisory Control and Data Acquisition (SCADA), Systems, Distributed Control Systems (DCS), and other control system configured such as Programmable Logic Controller (PLC),* NIST Special Publication 800-82, Revision 2, mai 2015 (cité : NIST, *Guide to ICS Security,* 2015).
– *Public Draft : The NIST Cybersecurity Framework 2.0,* 8 août 2023 (cité : NIST, *Public Draft : The NIST Cybersecurity Framework 2.0,* 2023).
– *The NIST Cybersecurity Framework (CSF) 2.0,* 26 février 2024 (cité : NIST, *The NIST Cybersecurity Framework (CSF) 2.0,* 2024).

OBERHOLZER Niklaus
– *Vorkommnisse im Ressort Cyber des Nachrichtendienstes des Bundes (NDB), Bericht der Administrativuntersuchung erstattet im Auftrag des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) – Auszug aus den Empfehlungen und der rechtlichen Beurteilung des Schlussberichts,* 15 août 2022 (cité : OBERHOLZER, *Bericht der Administrativuntersuchung – Auszug aus den Empfehlungen und der rechtlichen Beurteilung des Schlussberichts,* 2022).
– *Vorkommnisse im Ressort Cyber des Nachrichtendienstes des Bundes (NDB), Bericht der Administrativuntersuchung erstattet im Auftrag des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) – Zusammenfassung der wesentlichen Erkenntnisse,* 15 août 2022 (cité : OBERHOLZER, *Bericht der Administrativuntersuchung – Zusammenfassung der wesentlichen Erkenntnisse,* 2022).

OFFICE FÉDÉRAL DE L'ÉNERGIE
– *Bases pour l'introduction de systèmes de mesure intelligents auprès du consommateur final en Suisse – Exigences techniques minimales et modalités d'introduction,* 14 novembre 2014 (cité : OFEN, *Bases pour l'introduction de systèmes de mesure intelligents auprès du consommateur final en Suisse,* 2014).
– *Message relatif au premier paquet de mesures de la Stratégie énergétique 2050 (Révision du droit de l'énergie) et à l'initiative populaire fédérale « Pour*

la sortie programmée de l'énergie nucléaire (Initiative « Sortir du nucléaire »)», 4 septembre 2023 (cité : FF 2013 6771).
– *Rapport « Cyber-Sicherheit und Cyber Resilienz für die Wschweizer Stromversorgung »,* 28 juin 2021 (cité : OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »,* 2021).

OFFICE FÉDÉRAL DE LA COMMUNICATION
– *Modification de l'ordonnance sur les services de télécommunication (OST), Sécurité des informations et des infrastructures et services de télécommunication, Rapport explicatif,* 16 novembre 2022 (cité : OFCOM, *Modification de l'ordonnance sur les services de télécommunication (OST),* 2022).
– *Révision de l'ordonnance sur les domaines Internet, Rapport explicatif,* 28 août 2017 (cité : OFCOM, *Révision de l'ODI,* 2017).
– *Stratégie Suisse numérique,* septembre 2020 (cité : OFCOM, *Stratégie Suisse numérique,* 2020).
– *Suivi des lignes directrices « Intelligence artificielle » pour la Confédération – Évaluation de l'application et de l'actualité des lignes directrices*, 9 décembre 2022 (cité : OFCOM, *Suivi des lignes directrices « Intelligence artificielle » pour la Confédération,* 2022).

OFFICE FÉDÉRAL DE LA CYBERSÉCURITÉ
– *Commentaire concernant l'ordonnance sur la cybersécurité (OCyS),* mai 2024 (cité : OFCS, *Commentaire concernant l'OCyS,* 2024).
– *Conférence de haut niveau sur la paix en Ukraine : premier bilan de l'OFCS sur les travaux du réseau de suivi de la cybersituation,* 20 juin 2024 (cité : OFCS, *Conférence de haut niveau sur la paix en Ukraine,* 2024).
– *Rapport concernant les analyses de données effectuées après la cyberattaque contre l'entreprise Xplain,* 7 mars 2024 (cité : OFCS, *Rapport concernant les analyses de données effectuées après la cyberattaque contre l'entreprise Xplain,* 2024).
– *Rapport semestriel 2023/II (juillet – décembre),* 6 mai 2023 (cité : OFCS, *Rapport semestriel 2023/II,* 2024).
– *Rapport sur la sécurité informatique de la Confédération en 2023,* 26 juin 2024 (cité : OFCS, *Rapport sur la sécurité informatique de la Confédération en 2023,* 2024).
– *Stratégie de l'Office fédéral de la cybersécurité,* 6 mai 2023 (cité : OFCS, *Stratégie de l'OFCS,* 2023).

OFFICE FÉDÉRAL DE LA JUSTICE
– *Guide de législation – Guide pour l'élaboration de la législation fédérale,* 2019 (cité : OFJ, *Guide de législation,* 2019).

– *Ordonnance sur la protection la protection des données (OPDo), Rapport explicatif,* 31 août 2022 (cité : OFJ, *Rapport explicatif OPDo,* 2022).
– *Ordonnance sur les certifications en matière de protection des données (OCPD), Rapport explicatif,* 31 août 2022 (cité : OFJ, *Rapport explicatif OCPD,* 2022).
– *Circulaire N 2 : Convention sur la cybercriminalité,* 31 octobre 2012 (cité : OFJ, *Circulaire N 2 : Convention sur la cybercriminalité,* 2012).
– *Rapport d'activité 2021, Entraide judiciaire internationale,* mai 2022 (cité : OFJ, *Rapport d'activité 2021,* 2022).
– *Rapport d'activité 2022, Entraide judiciaire internationale,* mai 2023 (cité : OFJ, *Rapport d'activité 2022,* 2023).
– *Rapport sur le US CLOUD Act (loi Cloud),* 17 septembre 2021 (cité : OFJ, *Rapport sur le US CLOUD Act,* 2021).
– *Rapport sur la révision totale de l'ordonnance relative à la loi fédérale sur la protection des données, Rapport explicatif relatif à la procédure de consultation,* 23 juin 2021 (cité : OFJ, *Rapport sur la révision totale de l'ordonnance relative à la loi fédérale sur la protection des données,* 2021).

OFFICE FÉDÉRAL DE LA PROTECTION DE LA POPULATION
– *Beschreibung der Teilsektoren Kritischer Infrastrukturen in der Schweiz – Telekommunikation,* 2010 (cité : OFPP, *Beschreibung der Teilsektoren Kritischer Infrastrukturen in der Schweiz – Telekommunikation,* 2010).
– *Factsheet zum kritischen Teilsektor IT-Dienstleistungen,* juin 2012 (cité : OFPP, *Factsheet zum kritischen Teilsektor IT-Dienstleistungen,* 2012).
– *Factsheet zum kritischen Teilsektor Strassenverkehr,* décembre 2010 (cité : OFPP, *Factsheet zum kritischen Teilsektor Strassenverkehr,* 2010).
– *Factsheet zum kritischen Teilsektor Stromversorgung,* mai 2012 (cité : OFPP, *Factsheet zum kritischen Teilsektor Stromversorgung,* 2012).
– *Glossaire des risques – Formation à la gestion des risques OFFP,* avril 2013 (cité : OFPP, *Glossaire des risques,* 2013).
– *Méthode d'élaboration de l'Inventaire des infrastructures critiques (Inventaire PIC),* 24 février 2017 (cité : OFPP, *Méthode d'élaboration de l'Inventaire PIC,* 2017).
– *Protection de la population – Analyse et prévention des risques, planification, instruction, conduite et intervention 27,* mars 2017 (cité : OFPP, *Protection de la population 27,* 2017).

OFFICE FÉDÉRAL DE LA SANTÉ PUBLIQUE, *Sécurité des données dans le dossier électronique du patient, Fiche d'information,* 28 juin 2023 (cité : OFSP).

OFFICE FÉDÉRAL DE LA STATISTIQUE
– *Statistique policière de la criminalité (SPC), Rapport annuel 2021 des infractions enregistrées par la police*, Neuchâtel 2022 (cité : OFS, *SPC*, 2022).
– *Statistique policière de la criminalité (SPC), Rapport annuel 2022 des infractions enregistrées par la police*, Neuchâtel 2023 (cité : OFS, *SPC*, 2023).

ONLINE TRUST ALLIANCE
– *IoT Trust by Design – The OTA IoT Trust Framework*, 22 mai 2018 (citée : OTA, *IoT Trust by Design*, 2018).
– *2018 Cyber Incident & Breach Trends Report – Review and Analysis of 2018 Cyber Incidents and Key Trends to Address*, 9 juillet 2019 (citée : OTA, *2018 Cyber Incident & Breach Trends Report*, 2019).

ORGANISATION INTERNATIONALE DE NORMALISATION / COMMISSION INTERNATIONALE ÉLECTROTECHNIQUE, *Le recours et la référence aux normes ISO et IEC dans les politiques publiques*, 2015 (citées : ISO/IEC, *Le recours et la référence aux normes ISO et IEC dans les politiques publiques*, 2015).

ORGANISATION OF AMERICAN STATES, *Best Practices for establishing a National CSIRT*, Washington 2016 (citée : OAS, *Best Practices National CSIRT*, 2016).

PRÉPOSÉE FÉDÉRALE À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE
– *Guide pour l'examen de la licéité de la communication transfrontière de données (art. 16, al. 2, let. b et d, LPD)*, juin 2021, adapté à la LPD révisée en mai 2023 (citée : PFPDT, *Guide pour l'examen de la licéité de la communication transfrontière de données*, 2023).
– *Guide pour le traitement des données personnelles dans l'administration publique*, août 2009 (citée : PFPDT, *Guide pour le traitement des données personnelles dans l'administration fédérale*, 2009).
– *Guide pour le traitement des données personnelles dans le secteur privé*, août 2009 (citée : PFPDT, *Guide pour le traitement des données personnelles dans le secteur privé*, 2009).
– *Guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail, à l'attention de l'administration publique*, octobre 2013 (citée : PFPDT, *Guide surveillance au lieu de travail à l'attention de l'administration fédérale*, 2013).
– *Guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail, à l'attention de l'économie privée*, septembre 2013 (citée : PFPDT, *Guide surveillance au lieu de travail à l'attention de l'économie privée*, 2013).

– *Guide relatif aux mesures techniques et organisationnelles de la protection des données (TOM)*, 15 janvier 2024 (cité : PFPDT, *TOM*, 2024).
– *Transfert de données personnelles dans un pays ne présentant pas le niveau de protection des données requis, en application de clauses contractuelles types et contrats types reconnus*, 27 août 2021 (citée : PFPDT, *Transfert de données personnelles dans un pays ne présentant pas le niveau de protection des données requis, en application de clauses contractuelles types et contrats types reconnus*, 2021).
– *White Hat Hackers : Leur situation juridique, les risques qu'ils prennent et le rôle du PFPDT*, 23 juin 2023 (citée : PFPDT, *White Hat Hackers*, 2023).

PRÉVENTION SUISSE DE LA CRIMINALITÉ, *INFO 2/2021, Le magazine de la Prévention suisse de la criminalité, dossier surveillance*, 2021 (citée : PSC, *INFO 2/2021*, 2021).

RÉSEAU DE COMPÉTENCES EN INTELLIGENCE ARTIFICIELLE, *Terminologie*, version 1.0, 15 décembre 2021 (cité : CNAI, *Terminologie*, 2021).

RÉSEAU NATIONAL DE SÉCURITÉ, *Recommandations de mise en œuvre des organisations cantonales pour la cybersécurité*, 12 janvier 2021 (cité : RNS, *Recommandations de mise en œuvre des organisations cantonales pour la cybersécurité*, 2021).

RÉSEAU NATIONAL DE SOUTIEN AUX ENQUÊTES DANS LA LUTTE CONTRE LA CRIMINALITÉ INFORMATIQUE, *Cyberattaque – que faire ? Aide-mémoire à l'attention des CISO*, 21 décembre 2021 (cité : NEDIK, *Cyberattaque – que faire ?*, 2021).

SECRÉTARIAT D'ÉTAT À LA FORMATION, À LA RECHERCHE ET À L'INNOVATION, *Professions et activités réglementées en Suisse*, février 2023 (cité : SEFRI, *Professions et activités réglementées en Suisse*, 2023).

SECRÉTARIAT GÉNÉRAL DU DÉPARTEMENT FÉDÉRAL DE LA DÉFENSE, DE LA PROTECTION DE LA POPULATION ET DES SPORTS
– *Législation d'exécution relative à la loi sur la sécurité de l'information, Explications*, 8 novembre 2023 (cité : SG-DDPS, *Législation d'exécution relative à la LSI, Explications*, 2023).
– *Législation d'exécution relative à la loi sur la sécurité de l'information, Rapport explicatif*, 24 août 2022 (cité : SG-DDPS, *Législation d'exécution relative à la LSI, Rapport explicatif*, 2022).
– *Schlussbericht Aktionsplan Cyberdefense VBS*, 27 janvier 2021 (cité : SG-DDPS, *Schlussbericht Aktionsplan Cyberdefense VBS*, 2021).

SERVICE DE RENSEIGNEMENT DE LA CONFÉDÉRATION
- *La sécurité de la Suisse 2022, Rapport de situation du Service de renseignement de la Confédération,* juin 2022 (cité : SRC, *La sécurité de la Suisse,* 2022).
- *Compétences du SRC en matière d'attribution des cyberattaques,* Revue Militaire Suisse N 6, 2020 (cité : SRC ; *Compétences du SRC en matière d'attribution des cyberattaques,* 2020).
- *Le Service de renseignement de la Confédération SRC,* février 2013 (cité : SRC, *Le SRC,* 2013).

SERVICE SPÉCIALISÉ DE LA CONFÉDÉRATION POUR LA SÉCURITÉ DE L'INFORMATION, *Train de mesures pour éviter de nouvelles fuites de données, Autres domaines où il convient d'agir, Résultats de l'atelier du 20 mars 2024 sur les recommandations en matière de sécurité des informations,* 1er mai 2024 (cité : SERVICE SPÉCIALISÉ DE LA CONFÉDÉRATION POUR LA SÉCURITÉ DE L'INFORMATION, *Train de mesures pour éviter de nouvelles fuites de données,* 2024).

SERVICE SURVEILLANCE DE LA CORRESPONDANCE PAR POSTE ET TÉLÉCOMMUNICATION, *Rapport annuel 2023, Service SCPT,* avril 2024 (cité : SERVICE SCPT).

SWISSCOM, *Security Operation Center – Un SOC moderne en réponse à des menaces d'un genre nouveau,* Swisscom, 11 mai 2020 (cité : SWISSCOM, *Security Operation Center,* 2020).

SWISS PERSONALIZED HEALTH NETWORK, *SPHN/BioMedIT Information Security Policy,* version 2.0, 8 octobre 2020 (cité : SPHN).

UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS, *Guide pour l'élaboration d'une stratégie nationale de cybersécurité, Engagement stratégique pour la cybersécurité,* 2018 (citée : UIT, *Guide pour l'élaboration d'une stratégie nationale de cybersécurité,* 2018).

UNITÉ DE PILOTAGE INFORMATIQUE DE LA CONFÉDÉRATION
- *Rapport « évaluation de l'efficacité de la stratégie nationale de protection contre les cyberrisques (SNPC) »,* 30 novembre 2016 (citée : UPIC, *Rapport « évaluation de l'efficacité de la stratégie nationale de protection contre les cyberrisques (SNPC) »,* 2016).
- *Stratégie nationale de protection de la Suisse contre les cyberrisques – Plan de mise en œuvre de la SNPC,* 15 mai 2013 (citée : UPIC, *Plan de mise en œuvre de la SNPC,* 2013).

U.S. DEPARTMENT OF HOMELAND SECURITY, *Recommended Practice : Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, Industrial Control Systems Cyber Emergency Response Team,* septembre 2016 (cité : U.S. DEPARTMENT OF HOMELAND SECURITY, *Recommended Practice : Improving ICS Cybersecurity with Defense-in-Depth Strategies,* 2016).

WORLD ECONOMIC FORUM, *Cyber Resilience Playbook for Public-Private Collaboration,* janvier 2018 (cité : WEF, *Cyber Resilience Playbook for Public-Private Collaboration,* 2018).

Avant-propos

La présente étude s'inscrit dans le cadre du projet N 407740_197425/1, financé par le Fonds national suisse (FNS). La Confédération a octroyé à l'équipe de recherche un mandat dans le cadre du PNR 77 « Transformation numérique ». Ce programme de recherche national sur la transformation numérique regroupe des projets plaçant un accent sur l'éducation, l'économie, l'éthique et le droit. 1

Le projet N 407740_197425/1 se nomme « L'éthique et le droit pour promouvoir la confiance en la cybersécurité »[2]. Le projet donne une nouvelle compréhension de la cybersécurité mêlant les domaines du droit et de l'éthique. Il fournit également des informations et formule des recommandations d'éthique[3] et de droit[4]. 2

Le projet implique la collaboration entre l'Université de Lausanne, l'Université de Zurich et l'ancien Centre national pour la cybersécurité (NCSC), devenu en janvier 2024 le nouvel Office fédéral de la cybersécurité (OFCS). Le projet a été mis sur pieds dans le prolongement de la Stratégie nationale pour la protection de la Suisse contre les cyberrisques (SNPC), maintenant la Cyberstratégie nationale (CSN). Pour ce faire, le projet fournit des recommandations et des informations centrées sur les aspects non techniques de la cybersécurité. 3

Les trois objectifs principaux poursuivis par le projet sont l'identification des besoins réglementaires dans le domaine de la cybersécurité, la récolte de données par des enquêtes auprès d'infrastructures critiques et d'expertes en cybersécurité ainsi que la création d'un cadre de gouvernance concernant les aspects éthiques et juridiques de la cybersécurité. Les recherches menées dans le cadre du projet ont permis de formuler des recommandations législatives et des lignes directrices éthiques dans une perspective académique pour renforcer la CSN. 4

Cette étude contribue notamment à atteindre le premier objectif ainsi que le troisième objectif du projet. Elle analyse d'une part le cadre légal en matière de cybersécurité des infrastructures critiques et de gestion de cyberincidents en droit suisse et formule d'autre part des propositions législatives pour améliorer le cadre légal actuel. 5

2 Toutes les informations se trouvent sur PNR 77, *L'éthique et le droit pour promouvoir la confiance en la cybersécurité*.

3 Par exemple CHRISTEN Markus et al., *CERTs & Ethics: Guidelines, Four steps for a value-driven cybersecurity culture*.

4 Par exemple MEYER Pauline / MÉTILLE Sylvain, *Recommandation législative, Une proposition pour améliorer la cybersécurité des infrastructures critiques en Suisse*.

6 Quelques précisions doivent être faites. La présente étude cherche à utiliser dans la mesure du possible des expressions épicènes, à savoir incluant tous les genres[5]. Lorsque ce n'est pas possible ou lorsque la formulation serait excessivement lourde, le féminin est utilisé comme genre universel[6]. Le féminin l'emporte sur le masculin, sous réserve des citations ou des pratiques établies[7]. En cas de double désignation, la règle suivie est celle du genre le plus proche.

7 Outre ces précisions quant au langage inclusif, cette recherche s'inscrit dans un contexte fortement évolutif. La présente étude se concentre sur le droit suisse pour la cybersécurité des infrastructures critiques. La situation au niveau de la Confédération est en plein mouvement et la Suisse réorganise la cybersécurité du pays. La Loi fédérale sur la sécurité de l'information (LSI) est entrée entièrement en vigueur le 1er janvier 2024. Il en va de même pour ses ordonnances dont l'Ordonnance sur la sécurité de l'information (OSI). La loi a été révisée et sa révision a été adoptée par le Parlement en 2023. C'est pour cette raison qu'il sera fait mention dans le cadre de la présente étude de la LSI ainsi que de sa version révisée (LSI2) principalement au présent[8].

8 Par ailleurs, le Centre national pour la cybersécurité (NCSC) est l'autorité qui a été créée en 2019 au titre d'autorité principale pour la cybersécurité en Suisse[9]. Le NCSC a été transformé en Office fédéral de la cybersécurité (OFCS), qui a débuté ses tâches en janvier 2024[10]. Il sera fait principalement mention de l'OFCS, sous réserve de situations passées (à l'instar de publication de documents par l'ancien NCSC) ou lorsqu'il n'est pas certain que la réorganisation ait pour conséquence directe un maintien de la situation ou un transfert, notamment de compétences, du NCSC à l'OFCS. La présente étude fait mention des évolutions (doctrine et jurisprudence comprises) jusqu'au début du mois d'août 2024.

5 BUREAU DE L'ÉGALITÉ DE L'UNIVERSITÉ DE LAUSANNE, *Les mots de l'égalité*, p. 5.

6 Par exemple « la Préposée fédérale à la protection des données et à la transparence », « la fournisseuse » ou « les intervenantes ».

7 Cf. par exemple la locution « il s'agit » ou pour la notion de « Conseil fédéral ».

8 CF, *Le Conseil fédéral fixe l'entrée en vigueur de la loi sur la sécurité de l'information*. Il est également fait mention à plusieurs reprises du P-OCyS, dont la consultation s'est terminée mi-octobre 2024 et qui devrait entrer en vigueur avec la LSI2 en 2025.

9 NCSC, *Le Centre national pour la cybersécurité*.

10 NCSC, *Manuel Suter devient directeur suppléant du nouvel Office fédéral de la cybersécurité (OFCS)*.

Introduction générale

L'utilisation croissante des technologies de l'information et de la communication (TIC) offre des possibilités de progrès dans de nombreux domaines. Elle est aussi à l'origine de risques, de menaces et de dangers[11]. Les cybermenaces se manifestent sous la forme d'attaques malveillantes visant à compromettre données et systèmes informatiques, de vulnérabilités susceptibles de causer des dégâts (par exemple en étant exploitées par des personnes malveillantes), de manipulations accidentelles ou d'autres incidents impactant les systèmes informatiques, les informations traitées par différentes actrices ainsi que d'autres intérêts, à l'instar de la continuité des affaires, voire d'intérêts afférents à la population. 9

Les systèmes informatiques constituent des cibles de choix pour plusieurs raisons. Ils sont devenus l'un des éléments clés au centre des préoccupations politiques, juridiques, économiques ou sociales, du fait de la croissance exponentielle de leur utilisation et de la dépendance de la société à ceux-ci[12]. De plus, les développements technologiques impliquent des systèmes informatiques qui sont toujours plus complexes, interdépendants et interconnectés, ce qui les rend sensibles aux défaillances ainsi qu'aux erreurs et autres incidents. Cette dépendance à l'informatique génère notamment une hausse du nombre de cyberincidents. D'autres facteurs exercent une influence sur les cybermenaces, à l'instar des changements et hausses de tensions géopolitiques[13]. 10

La concrétisation de différentes cybermenaces a contribué à l'expression d'un besoin de sécurité dans l'utilisation de systèmes informatiques et, plus précisément, à un besoin de cybersécurité, dimension laissée pour compte aux débuts d'Internet[14]. La cybersécurité a d'abord été laissée à la technique, puis l'industrie et l'économie se sont saisies de la question de façon plus globale. De nombreux États ont pris ce sujet au sérieux, face aux différentes menaces se concrétisant dans le cyberespace. Il est devenu nécessaire de prendre 11

11 CF, *Rapport « Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense »*, 2021, p. 3. Le numérique renvoie à la notion de numérisation, qui désigne l'ensemble des développements et des possibilités d'application et conséquences notamment économiques, sociales ou politiques liés aux procédés techniques transformant une information analogique en une information numérique, cf. DFAE, *Stratégie de politique extérieure numérique 2021-2024*, 2020, p. 3. Sur l'omniprésence du numérique dans les différents secteurs d'activités, cf. JAQUIER, p. 220 ; SALAMON, p. 39.

12 DFAE, *Stratégie de politique extérieure numérique 2021-2024*, 2020, p. 12 ; MITROU, p. 4.

13 CF, *CSN*, 2023, p. 6 ; CF, *Infrastructure numérique. Réduire les risques géopolitiques*, 2023, p. 7.

14 CF, *Rapport « Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense »* 2021, p. 4 ; ChF, *Rapport « Suisse 2035, les grands défis de demain en 20 questions »*, 2022, p. 113 ; FF 2017 2791 ; GHERNAOUTI, *Cyberpower*, 2013, p. 44 ss.

conscience de la dimension juridique de ce sujet ou, en d'autres termes, de prendre conscience que la cybersécurité est un domaine juridique à part entière. La cybersécurité est au centre de différentes disciplines permettant de créer des incitations pour que l'ensemble de la société améliore sa cyberrésilience. Les États doivent assurer leur cybersécurité, de la même manière que les infrastructures critiques, les autres entreprises et la population.

12 Les cybermenaces sont susceptibles de peser sur l'entier de la société et d'entraîner des conséquences dramatiques, particulièrement lorsqu'elles visent les infrastructures critiques[15], l'un des piliers nécessaires au bon fonctionnement de la société, au bien-être de la population ou à l'économie nationale. Les infrastructures critiques sont des cibles privilégiées et les cyberattaques contre ces infrastructures sont susceptibles non seulement de perturber leur fonctionnement, mais aussi d'intimider la population ou de nuire à l'économie nationale et au fonctionnement de la société[16]. Des attaques importantes ont été médiatisées sur le plan international, avec comme exemples internationalement connus l'attaque par rançongiciel subie par Colonial Pipeline[17] ou l'attaque subie par l'entreprise américaine SolarWinds en 2020. Cette seconde attaque avait par exemple été perpétrée par le biais d'un code malicieux intégré au logiciel Orion, utilisé par de nombreuses clientes de l'entreprise. Cette attaque a été rendue possible par le téléchargement par des clientes de mises à jour vulnérables, permettant ainsi aux personnes délinquantes d'attaquer, de diverses manières, des multinationales et entités du gouvernement américain[18].

13 La Suisse, comme le reste du monde, n'est pas épargnée. Plusieurs attaques ont été perpétrées sur des infrastructures critiques dans le pays. En 2023, plusieurs organisations fournissant des prestations informatiques à la Confédération ont fait l'objet de cyberattaques, qui ont compromis des informations sensibles de la Confédération[19]. En outre, les attaques ayant ciblé les communes de Rolle et Montreux en 2021 ont eu un large écho médiatique et ont permis de prendre conscience de l'ampleur de ces phénomènes,

15 Cf. *infra* N 78 ; SKOPIK/SETTANNI/FIEDLER, p. 154. En 2021, une vague de cyberattaques a envahi certains hôpitaux français, conduisant à des paralysies de systèmes informatiques ainsi qu'à des demandes de rançons, cf. SEYDTAGHIA Anouch, *Une nouvelle vague de cyberattaques frappe les hôpitaux*.

16 NCSC, *Rapport semestriel 2022/1*, 2022, p. 6 ; SRC, *La sécurité de la Suisse*, 2022, p. 73.

17 Sur l'attaque par rançongiciel sur Colonial Pipeline, cf. notamment CISA, *The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years*.

18 GHERNAOUTI, *Cybercriminalité*, 2023, p. 74 s.

19 Voir notamment OFCS, *Rapport concernant les analyses de données effectuées après la cyberattaque contre l'entreprise Xplain*, 2024, p. 3 ; CF, *Cyberattaque contre l'entreprise Xplain: l'administration fédérale est également touchée*.

de leurs conséquences diverses et variées sur la population et sur le fait que toute organisation, notamment critique, peu importe sa taille ou son activité, est susceptible de présenter de l'intérêt pour des personnes aux intentions malveillantes[20].

14 Pour se prémunir contre la multitude de menaces qui existent et pour y réagir lorsqu'elles se concrétisent, la cybersécurité est devenue centrale dans cette transformation numérique[21]. Elle doit être implantée et respectée d'abord en termes de prévention ; l'on cherche à identifier puis protéger les infrastructures informatiques et les données traitées. Néanmoins, il est maintenant établi que, malgré toutes les mesures préventives, des cyberincidents ne peuvent être évités. Il faut accompagner les mesures préventives de mesures réactives pour parvenir à se protéger contre les cyberrisques et gérer les cyberincidents[22]. En d'autres termes, il ne s'agit pas de savoir si l'on va être victime d'un tel incident, mais quand[23]. Il est donc nécessaire de mettre en place également des mesures réactives basées sur des plans de gestion de cyberincidents établis à l'avance. Ces mesures doivent être conçues dans une perspective holistique, globale et transversale. Il faut par ailleurs considérer la cybersécurité comme évolutive en raison des nouvelles vulnérabilités découvertes, de nouveaux outils ou encore des nouvelles formes de criminalité. Elle doit continuellement s'adapter aux évolutions liées à l'utilisation en constante augmentation des nouvelles technologies par les délinquantes[24].

15 La Suisse a emboîté le pas à l'Union européenne et à d'autres États en faisant part d'une volonté politique de s'adapter à la numérisation et en utilisant la réglementation comme levier pour assurer la cybersécurité, surtout des infrastructures critiques[25]. La réflexion autour de la réglementation de

20 Voir par exemple, SEYDTAGHIA Anouch, *Cyberattaque à Rolle: un signal d'alarme pour les communes suisses* ; SEYDTAGHIA Anouch, « Si nous avons accès à d'autres villes suisses que Rolle, nous les attaquerons aussi » ; RTS, *La commune de Montreux à son tour victime d'une* cyberattaque. Pour d'autres exemples, cf. notamment CF, *Infrastructure numérique. Réduire les risques géopolitiques,* 2023, p. 7 s.

21 SALAMON, p. 15.

22 Sur les mesures, cf. notamment *infra* N 90 ss et 291 ss ; TEICHMANN/GERBER, *Les chevaux de Troie,* 2021, N 29 ss.

23 Ce propos illustre le paradigme *« assume breach »* (s'attendre à l'intrusion), cf. NCSC, *Rapport sur la sécurité informatique de la Confédération,* 2021, p. 3. Dans le même ordre d'idées, cf. notamment CF, *Rapport « Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense »,* 2021, p. 4 ; ENISA, *Baseline Capabilities of National/Governmental CERT, Part 2,* 2010, p. 20 ; JAQUIER, p. 229.

24 CF, *Rapport « Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense »* 2021, p. 3.

25 Voir notamment Interpellation 22.3749 « Faut-il différencier entre les secteurs économiques sous l'angle des exigences en matière de cybersécurité ? » déposée le 16 juin 2022

ce domaine est nécessaire, dans la mesure où les mesures juridiques et réglementaires font effectivement partie des incitations pour améliorer le niveau global de cybersécurité[26]. Partant, il est nécessaire d'adapter le cadre légal et plus largement le cadre réglementaire afin de lui donner plus de clarté, de cohérence et finalement pour aboutir à une amélioration du niveau de cyberrésilience en Suisse.

16 La présente étude poursuit deux objectifs principaux. Premièrement, elle expose une analyse du cadre légal existant à ce jour pour la cybersécurité. Pour ce faire, elle se concentre d'abord sur la cybersécurité des infrastructures critiques, dans la mesure où la loi s'applique en particulier à ces organisations. Ensuite, l'analyse du cadre légal porte sur les compétences des principales intervenantes dans la cybersécurité et plus précisément dans la gestion de cyberincidents. Il s'agit concrètement de comprendre quelles bases légales s'appliquent aux prestataires de gestion de cyberincidents ainsi qu'à l'OFCS, l'autorité principale pour la cybersécurité en Suisse, qui exploite GovCERT, l'équipe suisse de gestion de cyberincidents. Finalement, une analyse du cadre légal sur la sécurité des informations est exposée afin de comprendre comment le cadre légal en vigueur sert à la réglementation de la cybersécurité.

17 Deuxièmement, cette étude formule des propositions législatives. Une première proposition législative cherche à utiliser de façon plus appropriée la loi et la réglementation pour inciter les infrastructures critiques à améliorer leur niveau de cyberrésilience. Une seconde proposition législative vise à préciser le cadre légal applicable aux prestataires de gestion de cyberincidents et autres fournisseuses de services informatiques. Une troisième proposition législative doit permettre à la Confédération de mieux soutenir les infrastructures critiques et de développer son rôle en tant qu'autorité principale pour la cybersécurité en Suisse.

18 Afin d'atteindre ces objectifs principaux, il est nécessaire de clarifier les notions pertinentes du domaine émergeant et comprenant une multitude de perspectives et de professions. Il faut également poser le contexte politique et stratégique pour comprendre comment les autorités compétentes appréhendent la nécessité de réglementer la cybersécurité, principalement la cybersécurité des infrastructures critiques. Un tableau des compétences des différentes intervenantes doit également être dressé, de même que leurs fonctions en pratique. Cette analyse se poursuit avec l'examen du cadre légal, en termes de cybersécurité, de gestion de cyberincidents mais aussi de sécurité

par Gherard Andrey ; Motion 23.002 « Pour une meilleure sécurité des données numériques essentielles de la Suisse », déposée le 12 janvier 2023 par Josef Dittli.

26 OFPP, *Protection de la population 27*, 2017, p. 14.

de l'information et de protection des informations plus largement. En effet, la cybersécurité est étroitement liée à d'autres domaines plus réglementés, à l'instar de la sécurité de l'information et de la protection de certaines informations méritant une protection particulière. Finalement, lorsque les propositions législatives sont formulées, il est important de tenir compte des différents enjeux présents et de les concilier au mieux.

L'étude est subdivisée en trois parties. La première partie est consacrée 19
aux notions principales, aux enjeux, au contexte politique et aux actrices intervenant dans la cybersécurité en Suisse. Les notions relatives à la cybersécurité et à la gestion de cyberincidents ainsi que les enjeux principaux dans ce contexte sont traités dans le chapitre 1. Le chapitre 2 vise à dessiner le contexte politique et stratégique en Suisse qui sert de cadre pour la réglementation du domaine de la cybersécurité. Il s'agit en d'autres termes de comprendre les principales stratégies ayant un impact sur la cybersécurité en Suisse. Les compétences principales de l'État sont décrites dans le chapitre 3. Ce chapitre sert également à parcourir les compétences des intervenantes privées principales, à savoir les prestataires de gestion de cyberincidents, ainsi que les entités étrangères, européennes ou internationales collaborant avec les différentes intervenantes en Suisse.

La seconde partie porte sur l'analyse du cadre légal suisse pour la cyber- 20
sécurité. Cette partie débute avec le chapitre 4 qui dresse un tableau des bases légales applicables à la cybersécurité des infrastructures critiques, en passant en revue les différents secteurs critiques reconnus en Suisse. Ce chapitre permet également de parcourir les deux autres domaines composant la protection contre les cybermenaces, qui sont la cybercriminalité et la cyberdéfense. Le chapitre 5 met un accent sur les bases légales applicables à l'activité des prestataires de gestion de cyberincidents, en tenant compte de la diversité des structures, de la multitude des prestations possibles et de la distinction devant être opérée entre les prestataires externes, les fournisseuses internes à des autorités et l'OFCS, qui revêt un statut particulier en tant qu'autorité principale pour la cybersécurité en Suisse. Le chapitre 6 sert à l'analyse des bases légales existantes pour la protection de diverses informations, dans la mesure où c'est un domaine plus réglementé que celui de la cybersécurité. Les deux domaines s'entrecoupent dans une certaine mesure. Le chapitre 7 présente un résumé de l'état des lieux et des lacunes observées dans les chapitres précédents.

La troisième partie est consacrée à la formulation de propositions légis- 21
latives afin de développer et d'améliorer le cadre réglementaire pour la cybersécurité en Suisse. Le chapitre 8 sert d'introduction pour appréhender les différentes pistes réglementaires exploitables qui doivent être combinées.

La première proposition est consacrée au chapitre 9, qui distingue entre deux hypothèses pour la réglementation de la cybersécurité des infrastructures critiques. D'une part, il y est fait mention de l'alternative préconisée par le Conseil fédéral (CF), qui consiste en l'examen en tout temps des lacunes légales en Suisse et le comblement des lacunes le cas échéant. D'autre part, le chapitre 9 abrite la proposition d'une alternative, à savoir l'introduction d'exigences minimales légales de cybersécurité pour les infrastructures critiques. Le chapitre 10 est dédié à une seconde proposition législative qui consiste en l'introduction d'exigences de cybersécurité supplémentaires pour les fournisseuses de services informatiques, dont en particulier les prestataires de gestion de cyberincidents, afin de garantir la sécurité des prestations offertes par ces organisations. Ce chapitre sert également à proposer le développement des bases légales pour l'OFCS et son équipe d'intervention, GovCERT, afin de permettre un meilleur soutien, une réglementation plus claire et un contrôle d'application de la loi (notamment sur la base des deux chapitres précédents).

22 La présente étude s'articule autour de la cybersécurité des infrastructures critiques en Suisse et de la gestion de cyberincidents. La Suisse compte plusieurs secteurs et sous-secteurs critiques soumis à des réglementations, dont certaines sont transversales alors que d'autres sont spécifiques et disparates. Il existe une diversité de bases légales et de normes applicables, mêlant des compétences fédérales, cantonales et communales, raison pour laquelle l'analyse du cadre légal exposé dans cette recherche ne peut raisonnablement pas prétendre à l'exhaustivité.

23 La cybersécurité constitue l'un des trois domaines de la protection de la Suisse contre les cybermenaces, aux côtés de la cybercriminalité et de la cyberdéfense. La cybercriminalité est également abordée au sein de cette étude car elle est naturellement étroitement liée à la cybersécurité. Elle ne fait en revanche pas l'objet d'une attention aussi approfondie que l'examen de la cybersécurité. La cyberdéfense est brièvement mentionnée à diverses reprises, mais elle n'est pas autant approfondie que les deux autres domaines de la protection contre les cybermenaces. Le domaine de la cyberdéfense porte principalement sur le soutien, en termes de défense nationale, apporté par les autorités militaires ; l'accent n'est pas mis sur la cybersécurité civile, à savoir les mesures pouvant être mises en place par les autorités civiles en soutien aux infrastructures critiques en Suisse. Bien que la présente recherche se focalise davantage sur la cybersécurité et la réglementation dans le domaine précis de la cybersécurité, il est impossible de nier la parenté de la cybersécurité avec les deux autres domaines de la protection de la Suisse contre les cybermenaces. Partant, des considérations relatives à la cyberdéfense et à la poursuite de la

cybercriminalité guident les réflexions de la présente étude, notamment dans le cadre des questions de collaboration entre les différents acteurs et autorités.

En Suisse, la gestion de cyberincidents est prise en compte stratégiquement pour les administrations publiques, les infrastructures critiques, les autres entreprises de l'économie ou de l'industrie ainsi que la population. Néanmoins, la présente étude se préoccupe des infrastructures critiques comme bénéficiaires de prestations de gestion de cyberincidents, en raison de leur importance pratique, des risques que comportent les attaques les ciblant et de la volonté politique de réglementer surtout la cybersécurité de ces organisations. Par conséquent, la cybersécurité de la population n'est pas approfondie dans le cadre de cette étude, bien qu'elle soit parfois intégrée à la réflexion[27]. De la même façon, les incidents rencontrés par les entreprises qui ne sont pas des infrastructures critiques sont parfois abordés superficiellement, mais la présente étude ne cherche pas à résoudre le problème de la sécurité de ces dernières, qui nécessitent à l'heure actuelle davantage d'incitations non juridiques. Les propositions législatives ici recommandées peuvent néanmoins servir de modèle pour les entreprises et organisations n'étant pas considérées comme des infrastructures critiques. 24

En outre, nous verrons que l'utilisation de certaines technologies ou outils tels que l'intelligence artificielle (IA) ou l'Internet des objets (IdO) sont à l'origine de progrès comme de risques. Ces technologies sont donc abordées comme des exemples de mesures de cybersécurité ou comme des exemples pour illustrer la portée plus large que peut avoir la réglementation pour la cybersécurité. Leur réglementation au-delà d'une perspective de cybersécurité sort en revanche du cadre de la présente étude. 25

Bien que la gestion de cyberincidents soulève de nombreuses questions juridiques, toutes ne peuvent pas être analysées dans le cadre de la présente étude. Cette dernière cible particulièrement le droit suisse, raison pour laquelle les questions de droit international ou les questions plus généralement liées à l'absence de frontière d'Internet ne sont pas approfondies. Nous faisons typiquement allusion aux cas de cyberattaques dans des contextes de conflits armés, qui entrent dans le domaine de la cyberdéfense. Ces problématiques soulèvent de nombreuses questions fortement imprégnées d'influences géopolitiques. Elles supposent l'application de dispositions de droit international 26

27 Pour un exemple, voir le maliciel Flutbot diffusé à large échelle par le biais de SMS, cf. NCSC, *Rapport semestriel 2021/1,* p. 22 s. En outre, l'introduction d'exigences supplémentaires de cybersécurité pour les fournisseuses de services informatiques doit entraîner des conséquences positives également sur les prestations qu'elles offrent à toute leur clientèle et non seulement aux infrastructures critiques, cf. *infra* notamment N 1309.

alors que la présente étude porte sur le droit suisse. Les réglementations étrangères seront parfois mentionnées, à titre de comparaison ou dans les cas où elles imposent des obligations et des droits en Suisse, mais elles ne font pas non plus l'objet d'un examen rigoureux.

Première Partie :
les fondements

Chapitre 1 : les notions principales

Préambule au chapitre 1

Le domaine de la cybersécurité fait partie d'un ensemble de domaines composant en Suisse la protection contre les cybermenaces (I.A). Sa définition dépend du contexte dans lequel elle est comprise mais elle demeure dans tous les cas complémentaire à d'autres domaines pour assurer la protection de la Suisse contre les cybermenaces. En parallèle, la cybersécurité désigne un état à atteindre et pour lequel différentes incitations doivent être utilisées. Alors qu'elle a d'abord été comprise dans un sens technique, la politique et le droit l'appréhendent enfin. 27

La cybersécurité est liée à d'autres notions centrales, dont celles de cybermenace ou de différents groupes cibles. L'État n'est en effet pas confronté aux mêmes enjeux que d'autres actrices à l'instar des infrastructures critiques, des milieux économiques, des milieux académiques ou de la société civile (I.B). La notion de cybersécurité est également étroitement liée à celle de cyberincidents et de gestion de cyberincidents. Un état de cybersécurité est en effet atteint lorsqu'il est possible de gérer des cyberincidents, en les prévenant, en les détectant comme en y réagissant. Il est également nécessaire de comprendre à qui s'adresse la cybersécurité et de quelles actrices elle dépend (I.C). 28

La société doit chercher à assurer sa cybersécurité et à gérer les cyberincidents auxquels elle est susceptible d'être confrontée. Pour ce faire, il est important de tenir compte de différents enjeux. Les enjeux en question concernent des questions comme l'augmentation des cyberattaques, la collaboration ou encore les évolutions technologiques (II). 29

I. La cybersécurité et son contexte

A. La notion de cybersécurité

1. Le contexte de la protection contre les cybermenaces

a. Les trois domaines de la protection contre les cybermenaces

La cybersécurité constitue l'une des composantes de la protection contre les cybermenaces, à savoir les menaces présentes dans le cyberespace[28]. L'organisation de la protection contre les cybermenaces, anciennement protection 30

28 Le cyberespace peut être défini de plusieurs façons, voir par exemple GHERNAOUTI, qui le définit comme l'« environnement constitué par l'ensemble des équipements et logiciels informatiques, des services mis à disposition des internautes et des données

contre les cyberrisques[29], se divise actuellement entre trois domaines : la cybersécurité, la cyberdéfense et la poursuite pénale de la cybercriminalité[30]. Cette division permet de distribuer clairement les tâches et les compétences entre les autorités et les intervenantes.

31 L'Ordonnance sur les cyberrisques (aOPCy) a été adoptée en 2020 et abrogée en 2024 pour être intégrée à la Loi sur la sécurité de l'information (LSI) et à ses ordonnances, conformément à l'art. 47 al. 1 litt. a OSI. Cette ordonnance et la Cyberstratégie nationale (CSN) de 2023 définissent le domaine de la cybersécurité comme l'« ensemble de mesures visant à prévenir et à gérer les incidents et à améliorer la résilience face aux cyberrisques ainsi qu'à développer la coopération internationale à cet effet »[31]. La même stratégie indique que la poursuite pénale de la cybercriminalité englobe toutes les mesures pour lutter contre la cybercriminalité[32], prises par la police et les ministères publics de la Confédération comme des cantons[33]. Finalement, le domaine de la cyberdéfense est défini comme l'« ensemble des mesures prises par les services de renseignement et l'armée dans le but de protéger les systèmes critiques dont dépend la défense nationale, de se défendre contre les cyberattaques, de garantir la disponibilité opérationnelle de l'armée dans toutes les situations ayant trait au cyberespace et de développer ses capacités et compétences afin qu'elle puisse apporter un appui subsidiaire aux autorités civiles ; ce domaine inclut également des mesures visant à identifier les menaces et les attaquants ainsi qu'à entraver les attaques ».

manipulées », GHERNAOUTI, *Cybercriminalité,* 2023, p. 1. Pour une autre définition : « espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques », ANSSI, *Glossaire*.

29 Art. 6 aOPCy ; CF, *Plan de mise en œuvre de la SNPC 2018-2022,* 2019, p. 5.

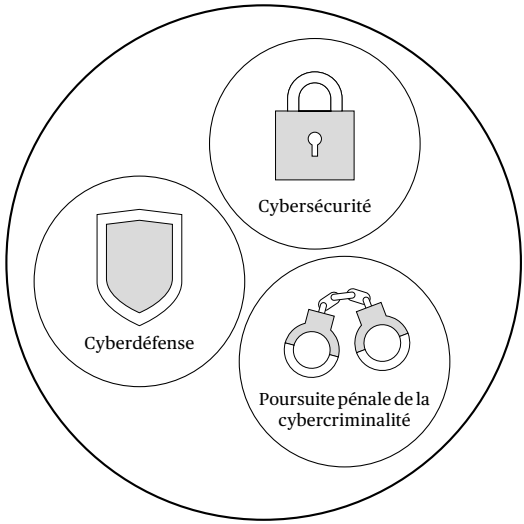
30 CF, *CSN*, 2023, p. 9.

31 CF, *CSN*, 2023, p. 9.

32 La cybercriminalité, contrairement à sa poursuite pénale, n'est pas définie dans la loi ou dans la stratégie qui cherchent par ces domaines à définir les mesures de protection contre les cybermenaces et non les menaces ; NICOLET/PEISSARD, p. 168.

33 CF, *CSN*, 2023, p. 9. Ces domaines sont également consacrés à l'art. 6 aOPCy. L'aOPCy a été en partie intégrée à la LSI et ses ordonnances, vraisemblablement sans les dispositions stratégiques à l'instar de l'art. 6 aOPCy.

Schéma 1 : les trois domaines de la protection contre les cybermenaces



b. Le domaine de la cybersécurité

La définition de la CSN de 2023 reprend celle du plan de mise en œuvre de la Stratégie nationale pour la protection contre les cyberrisques (SNPC) 2018-2022, qui la définissait déjà comme l'« ensemble des mesures visant à prévenir et à traiter les incidents ainsi qu'à améliorer la résilience face aux cyberrisques en renforçant la coopération internationale »[34]. 32

Le domaine de la cybersécurité ne se limite pas à un défi technique, mais représente une question complexe mêlant également les mesures organisationnelles, le droit, l'économie, la sécurité nationale et internationale, les relations internationales ou encore le développement durable[35]. Il doit être perçu comme un défi global[36]. La cybersécurité comporte plusieurs dimensions : une dimension politique et stratégique, une dimension culturelle et sociétale, une dimension humaine portant sur l'éducation et les compétences, une dimension juridique et réglementaire et une dimension technologique et technique[37]. Le 33

34 CF, *CSN*, 2023, p. 9 ; CF, *Plan de mise en œuvre de la SNPC 2018-2022*, 2019, p. 5.

35 GCSP, *Guide to Developing a National Cybersecurity Strategy*, 2021, p. 28.

36 FF 2017 2791 concernant l'importance de ne pas se limiter aux mesures techniques pour assurer la sécurité des moyens informatiques ; GHENAOUTI, *Cybercriminalité*, 2023, p. 164.

37 Les dimensions présentées sont tirées en partie de différentes sources : GCSCC, *Cybersecurity capacity review – Switzerland*, 2020, p. 7 et 18 ; ENISA, *National Capabilities Assessment Framework*, 2020, p. 59 ; GHERNAOUTI, *Cybercriminalité*, 2023, p. 168.

domaine de la cybersécurité comprend donc des mesures tant légales que techniques et politiques, avec l'implication de toutes les intervenantes, au niveau national comme international[38]. Dans la CSN, les autorités suisses ont mis l'accent sur la nécessité pour la Confédération de participer au développement de sa propre cybersécurité, ainsi qu'à celle des milieux économiques et de la population. Cette définition a mis l'accent également sur le rôle important occupé par les infrastructures critiques[39].

c. Le domaine de la poursuite pénale de la cybercriminalité

34 La poursuite pénale de la cybercriminalité englobe les mesures prises par les autorités de poursuite pénale, à savoir les polices et les ministères publics cantonaux et fédéraux, dans leur lutte contre la cybercriminalité[40].

35 Bien que la cybercriminalité ne soit pas, à l'inverse de la cybersécurité et de la cyberdéfense, définie légalement, elle est en tout cas constituée des actes délictuels commis dans le cyberespace[41] ; l'on fait référence ici aux infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication. Les actes compris dans cette définition doivent donc être susceptibles de constituer des infractions[42]. Plus concrètement, l'on peut faire une distinction entre la cybercriminalité au sens strict ou étroit et la cybercriminalité au sens large. Au sens étroit, elle regroupe les infractions informatiques typiques et désigne les infractions qui ne peuvent être réalisées qu'au moyen ou contre des infrastructures informatiques ou des données. La cybercriminalité au sens large vise les infractions informatiques atypiques, soit celles qui peuvent être réalisées indépendamment des technologies de l'information et de la communication (TIC)[43].

38 BAUER/VAN EETEN, p. 717.

39 CF, *Plan de mise en œuvre de la SNPC 2018-2022,* 2019, p. 5. La définition retenue dans le cadre de la SNPC, tout aussi correcte que celle figurant dans l'aOPCy ou la CSN 2023, revêt effectivement un aspect plus politique en englobant les différents outils, méthodes de gestion de risques, actions, bonnes pratiques et ainsi de suite, cf. UIT, *Guide pour l'élaboration d'une stratégie nationale de cybersécurité*, 2018, p. 13 pour une définition semblable. Pour la définition retenue dans la Directive SRI2, cf. art. 6 ch. 3 Directive SRI2 qui renvoie à l'art. 2 ch. 1 du Règlement européen sur la cybersécurité, se rapprochant des définitions susmentionnées, en adoptant davantage une approche fondée sur les cibles à risque.

40 CF, *CSN,* 2023, p. 5 ; CF, *Plan de mise en œuvre de la SNPC 2018-2022,* 2019, p. 5.

41 CF, *Poursuites pénales en matière de cybercriminalité*, 2024, p. 8 ; GHERNAOUTI, *Cybercriminalité,* 2023, p. 3 ; NICOLET/PEISSARD, p. 168.

42 ANSSI, *Glossaire* ; MITROU, p. 6.

43 À ce sujet, cf. *infra* N 557 ss ; MÉTILLE/AESCHLIMANN, p. 285 ; NICOLET/PEISSARD, p. 168. Pour une autre définition s'en rapprochant, voir SALAMON, p. 262.

d. Le domaine de la cyberdéfense

La cyberdéfense vise toutes les mesures des services civils de renseignement ainsi que de l'armée visant la protection des systèmes critiques et la défense contre les cyberattaques[44]. En d'autres termes, elle comprend « l'ensemble des mesures prises par les services de renseignement et l'armée dans le but de protéger les systèmes critiques dont dépend la défense nationale, de se défendre contre les cyberattaques, de garantir la disponibilité opérationnelle de l'armée dans toutes les situations ayant trait au cyberespace et de développer ses capacités et compétences afin qu'elle puisse apporter un appui subsidiaire aux autorités civiles. Le domaine de la cyberdéfense inclut également des mesures visant à identifier les menaces et les attaquants ainsi qu'à entraver et à bloquer les attaques »[45]. 36

Dans la définition retenue à l'art. 6 litt. b aOPCy[46], la cyberdéfense englobe les compétences visant la protection des systèmes critiques à la sécurité nationale, la défense des ressources de l'armée et le soutien subsidiaire aux autorités civiles[47]. Dans le contexte de la protection des ressources de l'armée, l'art. 1 al. 2 litt. a de l'Ordonnance sur la cyberdéfense militaire (OCMil) prévoit plus précisément que la cyberdéfense consiste en l'« action menée dans le cyberespace visant à identifier les attaques et la cyberexploration et à protéger les ressources de l'Armée suisse » (art. 1 al. 2 litt. a OCMil). Les autorités compétentes pour la cyberdéfense doivent pouvoir prendre des mesures actives pour identifier les menaces et les personnes à l'origine des attaques, ainsi qu'empêcher les attaques[48]. 37

2. La cybersécurité comme état

a. Des définitions

La cybersécurité se base naturellement sur le concept de sécurité, qui signifie simplement et théoriquement l'absence de danger ou de risques[49]. Le mot « cyber », lui, fait référence à la notion de « cybernétique » qui désigne la science des systèmes complexes, renvoyant aux questions informatiques et numériques, ainsi qu'aux systèmes et environnements les abritant[50]. En d'autres 38

44 CF, *Plan de mise en œuvre de la SNPC 2018-2022*, 2019, p. 5.

45 CF, *Rapport « Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense »*, 2021, p. 7.

46 Reprise dans DDPS, *Stratégie Cyber VBS*, 2021, p. 18.

47 CF, *Plan de mise en œuvre de la SNPC 2018-2022*, 2019, p. 5.

48 CF, *Plan de mise en œuvre de la SNPC 2018-2022*, 2019, p. 5.

49 MITROU, p. 7.

50 SALAMON, p. 14. Dans un sens similaire, GHERNAOUTI, *Cybercriminalité*, 2023, p. 4.

termes, le cyber se rapporte aux situations concernant concrètement l'utilisation d'Internet et des technologies de l'information et de la communication (TIC), ou plus généralement au cyberespace[51].

39 Il existe plusieurs définitions de la notion de cybersécurité[52]. En droit suisse, la cybersécurité se définissait comme « la situation dans laquelle le traitement des données, notamment l'échange de données entre les personnes et les organisations par l'intermédiaire d'infrastructures d'information et de communication, fonctionnent comme prévu » (art. 3 litt. a aOPCy)[53]. La notion n'est plus définie en droit suisse depuis l'abrogation de l'aOPCy.

40 Le but poursuivi par la cybersécurité est de parvenir à un état sûr[54]. Cet état sûr est relatif au bon fonctionnement du traitement d'informations par l'intermédiaire de systèmes informatiques et étend le champ d'application de la sécurité de l'information au cyberespace[55]. Concrètement, il peut s'agir de réduire la probabilité qu'une menace se matérialise, de limiter les dommages résultant d'un cyberincident, de revenir de façon efficiente à un état stable après un tel incident et ainsi de suite. L'on cherche donc ici à protéger les biens d'organisations aux niveaux humain, financier, informationnel et technique[56]. La cybersécurité doit être comprise de manière holistique : elle ne se limite pas aux aspects techniques ou informatiques mais comprend également des processus, des êtres humains et des éléments physiques[57].

41 Bien que, sur le plan national comme international, chaque autorité réglementaire compétente adopte sa propre définition de la cybersécurité et la modifie, les définitions se rapprochent et l'accent est mis au même endroit, à savoir sur la cyberrésilience et sur la résistance aux incidents ou aux perturbations. La notion de cybersécurité couvre toutes les technologies de l'information liées à Internet et aux réseaux similaires, dont font partie les moyens de communication, applications et processus ainsi que le traitement reposant sur ces réseaux[58]. À titre de comparaison, l'Agence nationale de la sécurité des systèmes d'information française (ANSSI) a défini la cybersécurité comme un « état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre

51 BOYES, p. 29. Sur l'utilisation d'Internet, cf. JAQUIER, p. 218.

52 BENHAMOU/BERNARD/DURAND, p. 38.

53 SG-DDPS, *Législation d'exécution relative à la LSI, Rapport explicatif,* 2022, p. 6 et 24.

54 Dans le même ordre d'idées, cf. SALAMON, p. 61 et 99.

55 OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »,* 2021, p. 29 et 133.

56 GHERNAOUTI, *Cyberpower,* 2013, p. 19.

57 BOYES, p. 29.

58 DFAE, *Stratégie de politique extérieure numérique 2021-2024,* 2020, p. 4.

la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense »[59]. Cette définition est plus étendue que la définition suisse. Elle ne se limite pas à ce qui est entendu en Suisse comme la cybersécurité, mais elle fait mention des domaines de la protection contre les cybermenaces.

Pour une autre comparaison, nous pouvons renvoyer aux définitions de 42
l'Institut national américain des normes et de la technologie (*National Institute of Standards and Technology,* NIST)[60]. La définition qu'il en retient est la suivante : « prévention des dommages, protection et restauration des ordinateurs, des systèmes de communications électroniques, des services de communications électroniques, des communications par fil et communications électroniques, y compris les informations qu'ils contiennent, afin de garantir leur disponibilité, leur intégrité, leur authentification, leur confidentialité et leur non-répudiation »[61]. Il l'avait définie en 2018 comme étant le « processus de protection de l'information par la prévention, la détection et la réaction aux attaques »[62]. L'Organisation internationale de normalisation (*International Organization for Standardization,* ISO) la définit comme la protection des personnes, de la société, des organisations et des États contre les cyberrisques[63].

Certaines définitions regroupent le domaine de la cybersécurité et l'état 43
de cybersécurité alors qu'une distinction existait en droit suisse. Alors que

59 ANSSI, *Glossaire*.

60 Pour des généralités au sujet du NIST, cf. *infra* N 369 s.

61 NIST, 800-53, rev. 5, p. 401.

62 NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, 2018, p. 45 (traduction effectuée par l'auteure). Pour un autre exemple, l'Union internationale des télécommunications, qui tient compte de toutes les différentes dimensions se rapportant à la cybersécurité. Sa définition est la suivante : « ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyberenvironnement et les actifs des organisations et des utilisateurs. Les actifs des organisations et des utilisateurs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication, et la totalité des informations transmises et/ou stockées dans le cyberenvironnement. La cybersécurité cherche à garantir que les propriétés de sécurité des actifs des organisations et des utilisateurs sont assurées et maintenues par rapport aux risques affectant la sécurité dans le cyberenvironnement. Les objectifs généraux en matière de sécurité sont les suivants : disponibilité ; intégrité, qui peut englober l'authenticité et la non-répudiation ; confidentialité », cf. UIT, X.1205, p. 3 ; repris par JAQUIER, p. 218.

63 ISO/IEC 27032 : 2023, p. 2.

les art. 3 litt. a et 6 litt. a aOPCy prévoyaient des définitions distinctes pour la cybersécurité et le domaine de la cybersécurité, tel n'est plus le cas depuis que l'ordonnance a été abrogée. Il n'existe plus, légalement, de définition de la cybersécurité. Il est important de disposer d'une définition de la cybersécurité simple, mais suffisamment complète. La notion de cybersécurité implique, comme nous avons pu le constater avec les différentes définitions exposées, la sécurité des moyens informatiques ainsi que des traitements informatisés d'informations. En outre, elle implique une diversité de mesures sans se limiter à des mesures techniques par exemple. Partant, la définition de l'art. 3 litt. a aOPCy est un bon début. En revanche, elle devrait être ajustée à plusieurs égards.

44 Premièrement, la notion de données est tantôt utilisée comme synonyme d'information, mais elle peut également être plus limitée et faire référence à des informations limitées à l'instar des données personnelles[64]. Pour cette raison, la définition doit mentionner le terme d'information à la place de la notion de donnée. Deuxièmement, la définition doit préciser qu'elle ne couvre pas uniquement le traitement d'informations par l'intermédiaire d'infrastructures d'information et de communication, mais également la sécurité de ces infrastructures. Troisièmement, différentes notions existent en Suisse et la notion de moyens informatiques est déjà utilisée dans la LSI. Les moyens informatiques comprennent tout « moyen relevant des techniques de l'information et de la communication, notamment les applications, les systèmes d'information et les fichiers, ainsi que les installations, les produits et les services servant au traitement électronique des informations » (art. 5 litt. a LSI). Cette notion englobe la notion des infrastructures d'information et de communication et un moyen informatique peut regrouper plusieurs systèmes ou moyens en une unité fonctionnelle[65]. Quatrièmement, la notion de cybersécurité ne se limite pas aux traitements informatisés d'informations fonctionnant « comme prévu », car une telle formulation pourrait se limiter à la continuation des affaires ou aux objectifs premiers des différents traitements d'informations sans assurer correctement l'ensemble des objectifs de sécurité. Par exemple, si un moyen informatique n'est pas suffisamment protégé et qu'une personne tierce non autorisée se limite à soustraire les données personnelles traitées par une autorité de l'administration qui peut poursuivre ses traitements, les traitements effectués par cette autorité fonctionnent comme prévu, mais une atteinte à la sécurité est à déplorer. Compte tenu de ces observations, nous proposons une définition de la cybersécurité comme suit : la

64 HUSI-STÄMPFLI, N 6 ss.

65 FF 2017 2765, p. 2826.

cybersécurité est la situation dans laquelle le traitement des informations par des moyens informatiques et les moyens informatiques fonctionnent comme prévu de façon sûre. La présente étude utilisera cette définition comme point de départ pour la notion de cybersécurité[66].

b. Les délimitations

La cybersécurité doit être distinguée de la sécurité informatique (ou la sécurité des moyens informatiques) et de la sécurité de l'information, même si elle se recoupe avec ces dernières[67]. La sécurité de l'information est une notion large, dans la mesure où elle ne se limite pas aux TIC. D'après la loi sur la sécurité de l'information (LSI), nous pouvons tirer une certaine définition de la sécurité de l'information, selon laquelle la sécurité de l'information viserait, au niveau de la Confédération du moins, la sécurité du traitement des informations visant à protéger des intérêts publics déterminés ainsi qu'à préserver la confidentialité, la disponibilité, l'intégrité et la traçabilité des informations traitées (art. 6 LSI)[68]. À un niveau international, l'ISO a adopté une définition de la sécurité de l'information, en la décrivant comme la « protection de la confidentialité, de l'intégrité et de la disponibilité de l'information », tout en précisant que d'autres composantes, à l'instar de la fiabilité ou l'authenticité, peuvent être comprises dans cette définition[69]. La sécurité de l'information comprend toutes les mesures permettant de protéger les informations traitées informatiquement ou non[70]. 45

De la même façon que la cybersécurité doit être distinguée de la sécurité de l'information, elle doit être distinguée de la sécurité des données (personnelles). La sécurité des données personnelles (art. 8 LPD) est quasiment une branche de la protection des données personnelles[71]. Elle doit être assurée pour des traitements de données personnelles effectués électroniquement ou non. En outre, la sécurité des données consacrée par la LPD et son ordonnance se limite aux mesures permettant de protéger des données personnelles. 46

66 En distinguant la notion de cybersécurité de celle du domaine de la cybersécurité.

67 JAQUIER, p. 219. Au sujet des notions de sécurité informatique et sécurité de l'information, cf. CARON, N 7 ss. La LSI distingue par exemple à ses art. 6 ss les mesures servant à la sécurité de l'information et à ses art. 16 ss les exigences relatives à la sécurité des moyens informatiques.

68 Dans le même sens, MITROU, p. 9. Les notions d'intégrité, de disponibilité et de confidentialité sont centrales qu'il s'agisse de l'activité de l'État ou d'autres organisations, voir par exemple ISACA, COBIT 5, p. 19.

69 Art. 3.28 ISO/IEC 27000 : 2018. Pour plus d'informations, voir art. 4.2.3 ISO/EIC 27000 : 2018 ; repris par JAQUIER, p. 218 s.

70 Dans un sens similaire, cf. WISCHMEYER, p. 27.

71 CR LPD FANTI/STAEGER, art. 8 N 2 ; MEIER, N 780 ; WISCHMEYER, p. 27.

En revanche, la sécurité des données et la cybersécurité sont proches et de nombreuses mesures permettent d'assurer tant la cybersécurité que la sécurité des données personnelles[72].

47 Alors que la sécurité de l'information est une notion générale couvrant les traitements de l'information quels qu'ils soient, à savoir sans se limiter aux traitements informatiques de l'information, tel n'est pas le cas de la cybersécurité ni de la sécurité informatique. Comme vu précédemment, la cybersécurité vise le bon fonctionnement du traitement de données par l'intermédiaire de systèmes informatiques et étend le champ d'application de la sécurité de l'information au cyberespace[73]. La sécurité informatique est un aspect de la cybersécurité, qui concerne uniquement les systèmes techniques (art. 3 litt. e aOPCy)[74].

48 La cybersécurité peut être considérée comme englobant les mesures techniques, personnelles et organisationnelles protégeant des composantes telles que la disponibilité, l'intégrité d'une part des informations traitées électroniquement, et d'autre part des systèmes et ressources informatiques[75]. Elle comporte donc des éléments institutionnels et ne se limite pas aux systèmes ou aux moyens informatiques comme la sécurité informatique[76]. La cybersécurité porte tant sur la sécurité informatique et la sécurité des réseaux des environnements connectés à Internet accessibles par le biais du cyberespace[77] en termes de contenants que sur la sécurité des informations informatiquement traitées en termes de contenu[78]. Les mesures prévues pour assurer la cybersécurité, la sécurité de l'information ou la sécurité des moyens informatiques sont par ailleurs souvent similaires, comme nous le verrons[79].

72 Voir par exemple MEYER/DAVIES, N 55 ss, qui exposent des mesures recommandées par le PFPDT pour assurer la sécurité des données ainsi que des mesures qui permettent de prévenir des cyberattaques.

73 Cf. *supra* N 38.

74 DFF, *Erläuterungen zur Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung*, 2020, p. 3 ; MITROU, p. 9 s.

75 WEBER/WILLI, p. 6.

76 MITROU, p. 10. La présente recherche utilise comme synonymes les notions de moyen et de système informatiques. L'accent est mis ici sur les machines et leur fonctionnement, contrairement à la notion de système d'information, où l'accent est mis sur les informations traitées par le biais du système, cf. LEGRENZI, N 70 s.

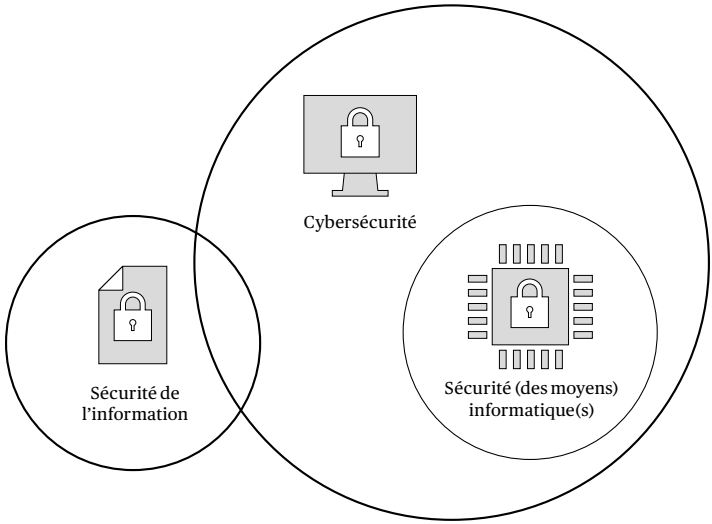
77 Le cyberespace ou l'espace numérique peut être défini comme « l'ensemble des équipements informatiques du monde et de leurs différentes formes de mises en réseau », cf. SALAMON, p. 21.

78 GHERNAOUTI, *Cybersécurité*, 2011, p. 11 ; ARPAGIAN, *chapitre 1*, p. 2.

79 Cf. en particulier *infra* N 1223 ss. La norme ISO/IEC 27032 : 2023 prévoit dans un ordre d'idées similaire que la cybersécurité comprend la sécurité sur Internet, la sécurité des réseaux et la sécurité web, cf. ISO/IEC 20732 : 2023, p. 6.

Compte tenu de ces différences et de ces similarités, nous allons concentrer la présente étude sur la cybersécurité. Par conséquent, la sécurité de l'information et la sécurité des systèmes informatiques seront seulement concernées de part et d'autre de ce travail de recherche.

Schéma 2 : le rapport entre cybersécurité, sécurité de l'information et sécurité (des moyens) informatique(s)



B. Les autres notions clés

1. La cybermenace et le cyberrisque

La cybermenace est maintenant définie dans la LSI révisée (LSI2) comme « toute circonstance ou tout événement pouvant entraîner un cyberincident » (art. 5 litt. f LSI2), définition partagée par la CSN[80]. La distinction avec la notion de cyberrisque peut être délicate. Selon la conception de l'Office fédéral pour la protection de la population (OFPP), la menace renvoie de manière générale à la notion de mise en danger, qui elle-même peut être définie comme le danger concret existant pour un bien digne de protection. Elle correspondrait donc à un événement potentiel pouvant avoir des conséquences sur un bien digne de protection et aurait comme synonyme le danger[81]. La cybermenace est une 49

80 CF, *CSN*, 2023, p. 4.

81 FF 2017 2765, p. 2774 et 2790 ; OFPP, *Glossaire des risques*, 2013, p. 44. Pour une autre définition, voir art. 3.74 ISO/EIC 27000 : 2018, où la menace est définie comme « *la cause potentielle d'un incident indésirable, qui peut nuire à un système ou à un organisme* ».

menace qui, en cas de concrétisation, affecte le bon fonctionnement de systèmes informatiques, réseaux de télécommunication et autres services et activités humaines en dépendant[82].

50 D'un point de vue terminologique, le cyberrisque était défini en droit suisse comme « le risque de survenance d'un cyberincident, son ampleur résultant du produit de la probabilité de survenance et de l'étendue des dommages » (art. 3 litt. c aOPCy)[83]. Le risque peut être défini comme le danger de subir un dommage ou une perte, souvent en lien avec un événement[84]. Le risque implique donc la question de la probabilité de sa réalisation ainsi que de la gravité des conséquences qu'il pourrait engendrer s'il venait à se concrétiser[85]. En outre, le risque sert à déterminer l'étendue d'une menace en englobant la probabilité et l'ampleur potentielle des dommages de la réalisation d'un tel événement. C'est également un paramètre permettant la comparaison entre différentes mises en danger[86]. Le Conseil fédéral (CF) utilise par ailleurs, dans ce cadre, la notion de risque comme paramètre pour déterminer l'étendue d'une menace[87]. Selon notre compréhension, la notion de risque aurait donc deux volets, dont un premier plus conceptuel (lorsque l'on parle d'identifier des risques) et un second plus mathématique (lorsque l'on parle de diminuer des risques). Le risque peut être désigné comme « un danger plus ou moins prévisible qui est fonction des menaces [...] »[88].

82 GHERNAOUTI, *Cybersécurité,* 2011, p. 11. À toutes fins utiles, la Directive SRI2, renvoyant à son art. 6 ch. 10 au Règlement sur la cybersécurité, définit la cybermenace comme « toute circonstance, tout événement ou toute action potentiels susceptibles de nuire ou de porter autrement atteinte aux réseaux et systèmes d'information, aux utilisateurs de tels systèmes et à d'autres personnes, ou encore de provoquer des interruptions de ces réseaux et systèmes », art. 2 ch. 8 Règlement sur la cybersécurité.

83 DFF, *Erläuterungen zur Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung,* 2020, p. 2. L'on peut également le définir comme le « risque de survenance d'un événement (résultant du produit de la probabilité de survenance et de l'étendue des dommages) nuisant à la confidentialité, à l'intégrité, à la disponibilité ou à la traçabilité des données ou pouvant occasionner des dysfonctionnements », cf. CF, *Rapport « Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense »,* 2021, p. 7. D'autres définitions existent, cf. DE WERRA/BENHAMOU, N 2 et références citées.

84 SURY, *Digital in Law,* 2021, p. 111.

85 FF 2017 2765, p. 2855 ; NIST, *Framework for Improving Critical Infrastructure Cybersecurity,* 2018, p. 46 ; SALAMON, p. 109. Pour plus d'informations au sujet de la notion de risque, cf. OFPP, *Glossaire des risques,* 2013, p. 56 s.

86 OFPP, *Glossaire des risques,* 2013, p. 56.

87 FF 2017 2765, p. 2776.

88 L'on voit donc le lien étroit entre les notions de risque et de menace, cf. GHERNAOUTI, *Cybersécurité,* 2011, p. 12.

La distinction entre les notions de cyberrisque et de cybermenace n'est pas effectuée dans le cadre juridique ou politique suisse en matière de cybersécurité ou, plus largement, de protection contre les cybermenaces (anciennement cyberrisques). Le cyberrisque et la cybermenace sont en tout cas liées l'une à l'autre ; le cyberrisque est causé par la cybermenace et la cybermenace est à l'origine du cyberrisque[89]. Néanmoins, à la lecture du message de la première version de la LSI, le CF utilise parfois les deux termes « menaces » et « risques » comme synonymes[90]. Il les distingue dans d'autres contextes, typiquement lorsqu'il mentionne, parmi les objectifs poursuivis par la SNPC, « la détection précoce des menaces et des dangers dans le cyberespace » d'une part et « la réduction des cyberrisques » d'autre part. Dans ce cas la distinction se rapproche de celle de l'OFPP, qui estime que le risque servirait à déterminer l'ampleur d'une menace[91]. 51

Il est possible, sur un plan purement conceptuel, d'utiliser les termes de cybermenace et de cyberrisque comme synonymes, en gardant à l'esprit que le risque est souvent plus abstrait que la menace. Sur un plan plus pratique, on peut considérer que le cyberrisque est un outil d'évaluation de la probabilité de la survenance d'un événement pouvant constituer une cybermenace, dans la mesure où, dès qu'il existe une menace, un risque relatif à l'éventualité qu'un événement non souhaité se réalise et provoque des conséquences préjudiciables existe aussi[92]. La distinction n'ayant pas de portée pratique spécifique, il n'en sera pas traité plus avant dans la présente étude. 52

2. Le cyberincident

Le droit suisse définit le cyberincident comme « un événement survenant lors de l'exploitation de moyens informatiques et pouvant avoir pour conséquence une atteinte à la confidentialité, à l'intégrité et à la disponibilité des informations ou à la traçabilité de leur traitement » (art. 5 litt. d LSI2). Le cyberincident recouvre les cyberattaques (à savoir les cyberincidents provoqués intentionnellement) comme les cyberincidents causés involontairement ou les cyberincidents liés à un dysfonctionnement des moyens informatiques. Ce qui importe selon cette définition est l'atteinte concrète à l'une des composantes de la sécurité de l'information[93]. Cette définition semble limitative. D'une part, 53

89 KÖNIGS, p. 143.

90 FF 2017 2765, p. 2772.

91 FF 2017 2765, p. 2774.

92 GHERNAOUTI, *Cybersécurité*, 2011, p. 12.

93 FF 2023 84, p. 22 ; CF, *CSN*, 2023, p. 4. Cette définition remplace la définition de l'art. 3 litt. b aOPCy, qui prévoyait qu'un cyberincident était un événement accidentel ou provoqué intentionnellement par une personne tierce non autorisée, qui nuit à la

des événements hors de l'exploitation de moyens informatiques peuvent avoir un impact négatif sur des informations traitées informatiquement. D'autre part, un incident qui aurait pour conséquence uniquement le dérangement de moyens informatiques, mais sans que les informations traitées ne soient impactées, n'entrerait pas dans cette définition.

54 Pour le NIST, l'incident est un événement compromettant potentiellement ou réellement l'intégrité, la disponibilité ou encore la confidentialité d'un système d'informations ou des informations qu'il traite, stocke ou transmet, ou l'événement qui constitue une menace imminente ou une violation des politiques de sécurité, des procédures de sécurité ou encore de politiques d'utilisation acceptable[94]. Sa définition exacte varie d'une organisation à une autre, ce qui est compréhensible du fait de l'importance de lier l'incident aux perturbations des fonctions de chacun, considération dépendant naturellement des missions de chaque organisation. Il existe plusieurs types d'incidents. Les incidents peuvent être accidentels, comme l'exposition accidentelle de données personnelles par la collaboratrice d'une entreprise. D'autres peuvent être d'origine délictuelle et constituer des cyberattaques. Les cyberincidents nécessitent une réponse appropriée[95].

55 Le cyberincident a *de facto* des conséquences négatives comme la perturbation du fonctionnement des opérations normales[96]. Partant, il convient de le distinguer de l'événement. L'événement a une portée plus large, pouvant désigner une simple occurrence observable comme un événement susceptible d'indiquer un possible incident[97]. L'ISO effectue aussi cette distinction entre un événement lié à la sécurité de l'information et un incident lié à la sécurité de l'information. Alors que l'événement est une simple occurrence, l'incident constitue un événement spécifique indésirable ou inattendu présentant une forte probabilité de menacer la sécurité de l'information et/ou de compromettre des opérations relatives à l'activité de l'organisation[98].

confidentialité, à l'intégrité, à la disponibilité ou à la traçabilité des données, ou qui peut occasionner des dysfonctionnements.

94 NIST, *Guide to ICS Security,* 2015, p. 126 ; NIST, *Computer Security Incident Handling Guide,* 2012, p. 6.

95 NIST, *Framework for Improving Critical Infrastructure Cybersecurity,* 2018, p. 45.

96 Art. 3.21 ISO/IEC 27000 : 2018, p. 12.

97 ISO/IEC 27035-1 : 2016, p. 2 ; NIST, 800-53, rev. 5, p. 402 ; NIST, *Computer Security Incident Handling Guide,* 2012, p. 6.

98 Art. 3.31 ISO/IEC 27000 : 2018. L'art. 3.30 ISO/IEC 27000 : 2018 prévoit en opposition qu'un événement lié à la sécurité de l'information est une « occurrence identifiée de l'état d'un système, d'un service ou d'un réseau indiquant une faille possible dans la politique de sécurité de l'information ou un échec des mesures de sécurité, ou encore une situation inconnue jusqu'alors et pouvant relever de la sécurité ».

Les cyberincidents comprennent des incidents accidentels ainsi que les cyber- 56
attaques, à savoir des cyberincidents d'origine malveillante. Tous les types de cyberincidents peuvent engendrer des conséquences négatives importantes, indépendamment d'une origine malveillante. Pour cette raison, la présente étude ne se limite pas aux cyberattaques. En effet, une panne de courant de grande ampleur ou un grave tremblement de terre peuvent par exemple causer d'importantes perturbations, hors manipulation malveillante[99].

3. La cyberattaque

En droit suisse, l'art. 5 litt. e LSI2 prévoit qu'une cyberattaque est « un cyber- 57
incident provoqué intentionnellement par un tiers non autorisé ». Elle consiste donc en une forme de cyberincident auquel est associée une intention malveillante[100].

À titre de comparaison, l'ISO a adopté une définition de l'attaque dans le 58
cadre de la sécurité de l'information en la définissant comme une « tentative de détruire, de rendre public, de modifier, d'invalider, de voler ou d'utiliser sans autorisation un actif, ou de faire un usage non autorisé de celuici »[101]. Alors que la définition suisse ne vise que les cyberattaques abouties ou réussies[102], la définition de l'ISO semble plus étendue en comprenant les tentatives.

Les cyberattaques peuvent notamment impliquer des accès non autori- 59
sés, des effacements ou des destructions d'informations ou de moyens informatiques ou encore des vols d'informations. Les motivations sont nombreuses et les outils très variés[103]. Une cyberattaque peut en outre être considérée comme une attaque armée[104] lorsqu'en visant une infrastructure critique, elle cherche à nuire au fonctionnement du pays et de ses institutions en vue de briser la souveraineté de l'État et la cohésion de la société, engendrant de ce fait des dommages considérables pour des personnes ou des objets[105].

Elle peut être directe ou être perpétrée à la suite d'une étape de recon- 60
naissance par l'attaquante tendant à caractériser le système et à trouver des vulnérabilités à exploiter. Dans ce second cas, l'attaque peut techniquement

99 OFPP, *Protection de la population 27,* 2017, p. 15.

100 CF, *CSN,* 2023, p. 4 ; NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures,* 2022, p. 13.

101 Art. 3.2 ISO/IEC 27000 : 2018.

102 FF 2023 84, p. 23.

103 MITROU, p. 7.

104 La notion d'attaque armée était réservée aux intrusions militaires, CF, *Rapport « La politique de sécurité de la Suisse »,* 2021, p. 34.

105 CF, *Rapport « La politique de sécurité de la Suisse »,* 2021, p. 34.

consister en l'exploitation de la vulnérabilité, des individus impliqués, des processus et autres composants et être suivie par l'étape de l'intrusion, consistant par exemple en l'exfiltration de données ou en un déni de service (*denial of service,* DoS). À noter que les attaques informatiques malveillantes qui aboutissent reviennent souvent, par la même occasion, à la réalisation d'actes réprimés par la loi[106].

4. La vulnérabilité

61 La vulnérabilité est définie à l'art. 5 litt. g LSI2 comme « une cybermenace due à des failles ou à des erreurs dans les moyens informatiques ». À titre de comparaison, l'art. 6 ch. 15 Directive SRI2 la définit comme « une faiblesse, susceptibilité ou faille de produits TIC ou de services TIC qui peut être exploitée par une cybermenace »[107].

62 Les vulnérabilités peuvent être de nature humaine, de nature systémique ou encore de nature technique. Les vulnérabilités humaines ou psychologiques peuvent être exploitées par des techniques d'ingénierie sociale. Sur le plan systémique, des vulnérabilités peuvent apparaître soit lors de l'intégration de composants correctement sécurisés individuellement au sein d'un système connexe, soit lors d'une interconnexion entre composants. Les vulnérabilités de nature technique peuvent, comme nous nous apprêtons à l'approfondir, exister au sein d'un composant ou d'un système[108].

63 Du point de vue technique, les vulnérabilités sont présentes dans des logiciels ou du matériel informatique. Elles sont causées par des erreurs de conception ou de développement, ou découlent de limites à la résistance intrinsèque d'un système[109]. Ces vulnérabilités peuvent être considérées comme des moyens de choix à exploiter pour les pirates en vue d'engendrer des dommages[110]. C'est l'un des biais par lesquels des intruses s'infiltrent dans des systèmes et réseaux informatiques.

64 Les vulnérabilités sont nombreuses et peuvent aller d'un port ouvert à la mauvaise configuration d'un service[111]. Pour illustrer cette notion avec un

106 NCSC, *Rapport semestriel 2021/1,* 2021, p. 6. Entrent effectivement dans la notion de cyberattaque les différents actes de cybercriminalité, englobant notamment la notion de cyberterrorisme.

107 FF 2023 84, p. 24. Une définition similaire est prévue par l'ISO, cf. ISO/IEC 27032 : 2023, p. 12. Pour les définitions de produit TIC et de service TIC, voir l'art. 2 ch. 13 du Règlement européen sur la cybersécurité.

108 SALAMON, p. 73 s.

109 SALAMON, p. 74.

110 EUROPOL, *Internet Organised Crime Threat Assessment IOCTA 2021,* 2021, p. 21 ; NCSC, *Rapport semestriel 2021/1,* 2021, p. 4 ; SALAMON, p. 73.

111 SHARMA/SINGH, p. 9.

exemple, une vulnérabilité dans le logiciel de partage de fichiers *Accellion File Transfert Appliance* (FTA), arrivant en fin de vie, avait permis à des actrices malveillantes l'exploitant, d'avoir accès aux données de plusieurs centaines de clientes aux quatre coins du monde, de demander des rançons et de publier les données qu'elles s'étaient procurées[112].

L'analyse de vulnérabilités désigne le processus de découverte de failles 65
pouvant être exploitées par des intruses. De nombreux outils sont par ailleurs utilisés afin d'analyser des vulnérabilités[113]. S'il n'y a pas d'indices démontrant son exploitation, l'objectif de cette gestion sera précisément de prévenir une telle exploitation[114].

La vulnérabilité doit en principe être corrigée, à défaut de quoi un inci- 66
dent est possible. Un cyberincident reviendrait dans ce contexte à l'exploitation d'une vulnérabilité dans un contexte informatique. Ainsi, lorsqu'il en va de la remédiation à un tel cyberincident, la mise en place d'un correctif pour une vulnérabilité peut tout à fait intervenir en parallèle du confinement et de l'éradication d'un logiciel malveillant (comme un rançongiciel) propagé par le biais de la vulnérabilité.

La présente étude se focalisant sur la gestion des cyberincidents, la ges- 67
tion des vulnérabilités ne sera pas approfondie. Néanmoins, les deux processus peuvent être menés en parallèle. La gestion de vulnérabilité peut par ailleurs faire partie des prestations offertes par une prestataire en plus de ses prestations de gestion de cyberincidents[115].

5. La cyberrésilience

La résilience était définie dans le contexte des cybermenaces à l'art. 3 litt. d 68
aOPCy comme « l'aptitude d'un système, d'une organisation ou d'une société à faire face à des perturbations internes ou externes et à maintenir son bon fonctionnement ou à le rétablir aussi rapidement et complètement que possible ». La résilience de la Suisse face aux cybermenaces est l'un des objectifs poursuivis par la LSI (art. 1 al. 1 litt. b LSI2) et, plus largement, par la CSN[116].

112 NCSC, *Rapport semestriel 2021/1*, 2021, p. 10.

113 Parmi les exemples cités par SHARMA/SINGH, p. 9.

114 FIRST, *CSIRT – Services Framework*, 2019, p. 31.

115 KILLCRECE ET AL., *State of Practice of CSIRT*, 2003, p. 68. Les prestations (réactives) de gestion de vulnérabilités s'articulent par ailleurs d'une façon similaire à celles de gestion de cyberincidents, dans la mesure où il s'agit principalement de détecter, d'analyser et de répondre à celles-ci, cf. ENISA, *Good Practice Guide for Incident Management*, 2010, p. 26 ; FIRST, *CSIRT – Services Framework*, 2019, p. 31 ss ; WEST-BROWN ET AL., p. 5, 25 et 28.

116 CF, *CSN*, 2023, p. 11.

69 Le Forum économique mondial (*World Economic Forum,* WEF) en retient une autre définition, se rapprochant en substance de celle retenue par le droit suisse. Il la considère comme la capacité à détecter les menaces, prévenir leur infiltration ou, du moins, limiter leur expansion, gérer leurs effets et empêcher leur récurrence. Le WEF met un accent particulier sur l'adaptabilité comme notion centrale de la résilience, comme celle de la poursuite des activités[117]. La résilience informatique doit être cherchée à tous les niveaux, remontant de la citoyenne utilisatrice finale d'un produit, aux diverses entreprises, infrastructures et autorités de l'administration. En outre, pour l'assurer, il convient de prendre tant des mesures préventives que réactives, notamment en utilisant des capacités de réponse aux incidents[118]. La cyberrésilience est la capacité ou l'aptitude à assurer la cybersécurité.

6. Les groupes cibles

a. Les autorités

70 Les groupes cibles pour la cybersécurité sont les organisations et personnes susceptibles d'affecter, d'être affectées ou de se sentir affectées par des considérations de cybersécurité[119]. Les cybermenaces visent l'ensemble de la société : il en va donc naturellement des autorités et des organisations étatiques et des infrastructures critiques, mais également de l'économie et de la population. Chaque actrice est confrontée à des menaces et doit s'acquitter de certaines obligations et assumer sa part de responsabilité[120].

71 Les autorités sont concernées par la cybersécurité de plusieurs façons. D'une part, elles sont confrontées aux cybermenaces, au même titre que les infrastructures critiques, les autres entreprises et la population. Il en va typiquement des cas d'espionnage entre États, d'attaques en DoS ou en déni de service distribué (*distributed denial of service,* DDoS)[121] pour que les sites Internet de l'État ne soient plus accessibles au public, ou encore de demandes de rançongiciels en raison du volume et du caractère sensible d'informations traitées par des autorités et organisations étatiques. L'État est concerné à tous les

117 WEF, *Cyber Resilience Playbook for Public-Private Collaboration,* 2018, p. 33.

118 NCSC, *Rapport semestriel 2021/2,* 2021, p. 6 ; HÄMERLI, p. 190.

119 Art. 3.37 ISO/IEC 27000 : 2018. La CSN parle des groupes cibles auxquels elle s'adresse, voir CF, *CSN,* 2023, p. 12.

120 CF, *CSN,* 2023, p. 12.

121 Une attaque DoS ou DDoS paralyse et empêche un système, un réseau ou un service de continuer à fonctionner selon ses conditions prévues, le plus souvent avec un refus total d'accès aux utilisatrices légitimes, cf. ISO/IEC 27035-1 : 2016, p. 16 ; OFCS, *Rapport sur la sécurité informatique de la Confédération en 2023,* 2024, p. 5 ; TEICHMANN/GERBER, *La qualification pénale des attaques DDoS en droit suisse,* 2021, N 3 s.

niveaux par la cybersécurité et la gestion de cyberincidents. En 2023, plusieurs cyberattaques visant des fournisseuses de services informatiques offrant des prestations à des autorités de la Confédération avaient causé la fuite d'informations détenues par ces dernières[122]. La même année, des attaques DDoS ont été menées contre les systèmes de l'administration fédérale[123]. L'année 2021 avait illustré ces problèmes à l'échelon communal avec plusieurs attaques ciblant des communes vaudoises[124].

D'autre part, les autorités étatiques interviennent par l'exploitation de différents leviers d'action en matière de cybersécurité. Le pouvoir exécutif est responsable de l'élaboration de stratégies pour adapter sa cybersécurité à l'évolution des TIC. Les pouvoirs législatifs et exécutifs ont la compétence d'adopter les lois, ordonnances, directives et autres normes de cybersécurité. L'État est également représenté par les institutions publiques, dont le gouvernement. Il est finalement aussi représenté par les autorités d'application de la loi à l'instar des autorités compétentes pour la prévention, la détection, l'investigation ou la poursuite d'infractions, par les autorités judiciaires ou encore par les autorités de surveillance ou de renseignements[125]. Finalement, l'État compte d'autres autorités et organisations, dont celles qui sont en charge de tout ou partie de la mise en œuvre concrète de mesures pour les cyberaspects de différentes stratégies veillant à la poursuite d'intérêts publics[126]. 72

b. Les infrastructures critiques

La sécurité nationale dépend en grande partie des services essentiels ou critiques rendus sur le territoire étatique. Ces services sont fournis par les infrastructures critiques, qui revêtent une importance capitale pour le fonctionnement de la société, l'économie et le bien-être de la population. Bien qu'il 73

122 NCSC, *Cyberattaque contre l'entreprise Concevis: l'administration fédérale est également concernée* ; OFCS, *Rapport concernant les analyses de données effectuées après la cyberattaque contre l'entreprise Xplain*, 2024, notamment p. 7. La cyberattaque ayant visé la société Xplain a par ailleurs eu d'importantes conséquences comme l'adoption d'un train de mesures pour éviter de telles fuites de données, une enquête administrative ainsi que différentes enquêtes de la PFPDT.

123 OFCS, *Conférence de haut niveau sur la paix en Ukraine*, 2024, p. 2 ; CF, *Attaque DDoS contre l'administration fédérale : plusieurs applications et sites Internet ne sont plus accessibles*.

124 Voir à titre d'exemple la page dédiée aux communiqués de presse de la commune de Montreux : *Cyberattaque contre la Commune de Montreux : Questions/réponses*.

125 ENISA, *Roadmap on the cooperation between CSIRT and LE*, 2019, p. 9 ; OAS, *Best Practices National CSIRT*, 2016, p. 18 ; SALAMON, p. 28.

126 ENISA, *Good practices in innovation on cybersecurity under the National Cyber Security Strategies*, 2019, p. 25. Par exemple et selon plusieurs législations (voir art. 12 al. 1 litt. c aOPCy ou 10 Directive SRI), l'État doit disposer d'une CERT gouvernementale pour assister soit l'administration, soit les infrastructures ou la population.

n'existe pas de définition universelle de la notion d'infrastructures critiques, le droit et les institutions suisses en ont adopté plusieurs[127]. Tout d'abord, l'art. 6 al. 1 litt. a ch. 4 de la Loi sur le renseignement (LRens) les considère comme les « infrastructures d'information, de communication, d'énergie, de transports et autres qui sont indispensables au fonctionnement de la société civile, de l'économie et de l'État ». Dans un esprit comparable, avec d'autres exemples, l'art. 5 litt. c LSI donne à la notion d'infrastructure critique la définition suivante : « l'approvisionnement en eau potable et en énergie, les infrastructures d'information, de communication et de transports ainsi que d'autres installations, processus et systèmes essentiels au fonctionnement de l'économie et au bien-être de la population »[128]. L'art. 3 litt. g aOPCy prévoyait que les infrastructures critiques sont « les processus, systèmes et installations indispensables au fonctionnement de l'économie et au bien-être de la population ». L'OFPP définit les infrastructures critiques comme des « infrastructures dont le dérangement, la défaillance ou la destruction peut avoir des conséquences graves pour la société, l'économie et les pouvoirs publics »[129].

74 Ces différentes terminologies se rapprochent, mais demeurent vagues[130], raison pour laquelle il est important de comprendre plus concrètement ce qui entre dans la notion d'infrastructure critique dans la perspective des autorités suisses. Selon la Méthode d'élaboration de l'Inventaire des infrastructures critiques (Inventaire PIC) établi par l'OFPP et selon la Stratégie nationale de protection des infrastructures critiques (Stratégie PIC), toute infrastructure qui fournit des prestations dans l'un des vingt-sept sous-secteurs critiques inclus dans les neuf secteurs critiques (autorités, santé, énergie, élimination, finances, information et communication, alimentation, sécurité publique,

127 Pour quelques exemples sur le plan international, voir ISO/IEC 27019 : 2017, p. 2 ; FF 2018 492 ; GCSP, *Guide to Developing a National Cybersecurity Strategy,* 2021, p. 41 ; UIT, p. 42. Il faut en effet tenir compte du fait que la définition de la notion d'infrastructures critiques va dépendre du contexte national économique, géopolitique et culturel, cf. GCSP, *Guide to Developing a National Cybersecurity Strategy,* 2021, p. 41.

128 Cette définition contient des notions indéterminées et prévoit des exemples. Elle ne définit pas réellement la notion d'infrastructure critiques d'une façon permettant à toutes les organisations de s'y reconnaître facilement.

129 OFPP, *Glossaire des risques,* 2013, p. 39. L'OFPP met à disposition sur son site Internet des explications par secteur, cf. OFPP, *Les infrastructures critiques*. Au vu de la diversité terminologique employée par les autorités compétentes et pour des questions de lisibilité, la présente étude utilisera la notion d'infrastructure critique pour désigner les autorités et les organisations actives dans les secteurs et sous-secteurs critiques bien qu'une infrastructure critique puisse en fonction des définitions retenues également consister en un système ou un processus.

130 FF 2023 84, p. 30.

transports publics) devrait être considérée comme critique, indépendamment de son niveau de criticité[131]. Partant, les infrastructures critiques sont celles actives dans un sous-secteur critique. Les sous-secteurs critiques sont regroupés en secteurs, mais il ne devrait pas exister d'infrastructure critique dans un secteur et sans être également dans un sous-secteur. Selon ces critères, c'est donc réellement le fait pour une organisation d'être active au sein d'un sous-secteur critique qui importe, et non pas leur niveau de criticité ou l'étendue des personnes impactées par une défaillance qui leur serait causée. Par exemple, un service infonuagique fait partie du sous-secteur critique des services informatiques, qui est compris dans le secteur critique de l'information et de la communication. Une organisation[132] active dans le transport ou dans la production d'électricité tombera dans le sous-secteur critique de l'approvisionnement en électricité compris par le secteur de l'énergie[133].

Le rattachement de la notion d'infrastructure critique à un sous-secteur 75
d'activité présente davantage de clarté et de prévisibilité pour les organisations. En revanche, cet unique rattachement couvre un cercle important d'organisations, dont certaines ne sont pas essentielles au bien-être de la population ou à l'économie nationale. Par exemple, dans le secteur critique de l'alimentation, l'on peut aisément comprendre que des entreprises comme la Coop ou la Migros soient considérées comme des infrastructures critiques pour la Suisse, car elles sont essentielles à l'approvisionnement en denrées alimentaires pour le pays. En revanche, tel n'est pas le cas d'une épicerie de quartier lorsqu'il existe plusieurs épiceries et supermarchés pour une même localité. Cette dernière peut en revanche être essentielle au bien-être d'une région rurale ou de montagne qui n'a que difficilement accès à un supermarché, mais ce n'est donc pas systématiquement le cas. Une épicerie, active dans le sous-secteur critique de l'approvisionnement en denrées alimentaires pourrait être considérée comme une infrastructure critique sur la base des critères de l'OFPP, alors qu'elle n'est que rarement susceptible d'être essentielle au bien-être de la population.

131 FF 2018 491, p. 499 ; FF 2023 1659, p. 7 ; OFPP, *Méthode d'élaboration de l'Inventaire PIC*, 2017, p. 5. Les secteurs étaient auparavant au nombre de dix, cf. OFPP, *Glossaire des risques*, 2013, p. 39 s. À noter que le domaine spatial ne fait aujourd'hui pas partie de la Stratégie PIC, contrairement au champ d'application de la Directive SRI2 dans l'UE, et qu'il serait judicieux de se pencher sur cette question.

132 L'organisation consiste en un groupe de personne ayant ses propres fonctions, responsabilités, autorités et relations pour atteindre ses objectifs, ISO/IEC 27032 : 2023, p. 3. Cette notion sera fréquemment utilisée pour désigner les infrastructures critiques en tant que titulaires de droit et obligations.

133 FF 2018 491, p. 499 ; FF 2023 1659, p. 24 s. ; OFPP, *Glossaire des risques*, 2013, p. 39.

76 Les différentes définitions existantes de la notion d'infrastructure critique se recoupent, mais présentent toutes des problèmes en termes de clarté. Une solution intermédiaire devrait exister et celle-ci devrait tenir compte tant des (sous-)secteurs critiques d'activité que du niveau de criticité[134].

77 Les sous-secteurs critiques sont considérés comme tels en raison des prestations d'importance vitale offertes par les actrices actives en leur sein pour la population et l'économie, des conséquences pour la population et l'économie qu'auraient des pannes ou des défaillances interrompant la fourniture de leurs prestations ou du danger potentiel pour l'être humain, les animaux et l'environnement que ces actrices représentent[135]. Les infrastructures critiques englobent des processus nécessitant une protection particulière face à tout dysfonctionnement susceptible d'impacter la société ; les cyberincidents les impactant sont susceptibles d'engendrer de graves dommages. La CSN considère que leur protection est hautement prioritaire et qu'elle « constitue le point de mire de toutes les mesures de la CSN »[136].

Schéma 3 : les neufs secteurs critiques et les vingt-sept sous-secteurs critiques[137]

Les secteurs critiques	Les sous-secteurs critiques
Les autorités	La recherche et l'enseignement
	Les biens culturels
	Le Parlement, le gouvernement, la justice, l'administration
L'énergie	L'approvisionnement en gaz naturel
	L'approvisionnement en pétrole
	L'approvisionnement en électricité
	Le chauffage à distance et la chaleur industrielle
L'élimination	Les déchets
	Les eaux usées
Les finances	Les services financiers
	Les services d'assurance
La santé	Les soins médicaux
	Les prestations de laboratoire
	La chimie et les produits thérapeutiques

134 Pour une proposition, cf. *infra* N 1212.

135 OFPP, *Protection de la population 27,* 2017, p. 13.

136 FF 2023 84, p. 12.

137 Schéma reprenant les secteurs et sous-secteurs critiques de la Stratégie PIC de 2023, cf. FF 2023 1659, p. 25 s.

L'information et la communication	Les services informatiques
	Les télécommunications
	Les médias
	Les services postaux
L'alimentation	L'approvisionnement en denrées alimentaires
	L'approvisionnement en eau
La sécurité publique	L'armée
	Les services d'urgences
	La protection civile
Les transports	Le transport aérien
	Le transport ferroviaire
	Le transport fluvial
	Le transport routier

Les infrastructures critiques constituent une cible de choix pour des personnes 78
à l'origine de cyberattaques. L'objectif est de saboter de telles infrastructures pour qu'elles ne puissent plus offrir leurs prestations essentielles au bon fonctionnement d'une société[138]. À titre d'exemple, une cyberattaque portant sur l'approvisionnement en électricité pourrait entraîner l'immobilisation des transports publics et des moyens de communication, des pannes de chauffages, l'impossibilité de pomper de l'eau dans les ménages et ainsi de suite[139]. Si un cyberincident touche une infrastructure critique, les effets peuvent être dramatiques et même entraîner des décès, notamment par la manipulation d'appareils médicaux de maintien de vie ou d'informations relatives à la patientèle d'un établissement hospitalier[140].

En d'autres termes, les infrastructures critiques revêtent une importance 79
capitale dans le domaine de la sécurité, du fait de leur criticité et dans la mesure où la société dépend de la disponibilité des biens et services de base et est, partant, sensible aux ruptures d'approvisionnement[141]. Compte tenu de l'importance capitale que revêtent ces infrastructures pour la société, leur protection est, comme nous le verrons, l'une des priorités et l'un des piliers de la sécurité d'un État. Leur protection implique des mesures réduisant la probabilité de survenance d'un incident ou la diminution des dommages en résultant, ainsi que l'augmentation de leur résilience[142].

138 SALAMON, p. 69.

139 OFPP, *Protection de la population 27,* 2017, p. 13.

140 OFPP, *Protection de la population 27,* 2017, p. 13 s. ; FF 2017 2765, p. 2772. Et ce, bien que ce type d'effet soit souvent indirect, SALAMON, p. 31.

141 FF 2018 491, p. 492 et 496 ; WEBER/WILLI, p. 132.

142 FF 2018 491, p. 492 ; CF, *Plan de mise en œuvre de la SNPC 2018-2022,* 2019, p. 24 ; OFPP, *Glossaire des risques,* 2013, p. 40.

c. Les autres groupes cibles

80 La cybersécurité et la protection de la Suisse contre les cybermenaces impliquent d'autres parties prenantes. On peut compter à ce titre les milieux économiques, les milieux académiques et de la recherche, la population et les organisations internationales et les organisations non gouvernementales (ONG)[143]. La SNPC 2018-2022 avait déjà, pour mieux prendre en considération tous les groupes cibles, élargi son champ d'action pour viser la protection des PME ainsi que de la population[144].

81 La protection de la population sert de finalité commune à toutes les mesures de protection d'un État contre les cybermenaces[145]. La société civile participe aux stratégies nationales de cybersécurité et bénéficie de leur mise en œuvre. La population est régulièrement l'utilisatrice finale de produits et processus issus des TIC au bout de la chaîne d'approvisionnement[146]. Elle peut également faire l'objet de cyberattaques[147]. La population doit être sensibilisée et mise en garde contre les cybermenaces. La protection des données des individus doit être garantie et ces derniers doivent pouvoir utiliser les technologies numériques en toute sécurité[148]. Des associations professionnelles ou organisations collectives (par exemple à but non lucratif) existent par ailleurs avec pour objectifs l'exercice d'une influence stratégique, réglementaire ou politique (dans un sens de *policy*) ou la meilleure implémentation de la protection contre les cybermenaces[149].

82 Les entreprises actives dans l'économie suisse et qui ne sont pas des infrastructures critiques sont aussi toujours plus dépendantes des TIC et elles bénéficient également du cadre apporté par la cybersécurité. Les petites

143 CF, *CSN*, 2023, p. 12 ; ENISA, *Good practices in innovation on cybersecurity under the National Cyber Security Strategies*, 2019, p. 25.

144 CF, *Plan de mise en œuvre de la SNPC 2018-2022*, 2019, p. 21.

145 FF 2023 84, p. 12.

146 ENISA, *Good practices in innovation on cybersecurity under the National Cyber Security Strategies*, 2019, p. 25 ; SALAMON, p. 29. La chaîne d'approvisionnement sont par ailleurs vulnérables à chaque étape, raison pour laquelle il faut tenir compte de toutes les intervenantes au long du processus, de l'achat des matières premières à la livraison des produits finis aux consommatrices. Chacune doit être consciente de sa place au sein de la chaîne de développement d'une potentielle cyberattaque, cf. BOYES, p. 29 s. ; WEBER, N 19.

147 OA, *Enquête administrative « Fuite de données »*, 2024, N 538 ss ; OFCS, *Stratégie de l'OFCS*, 2023, p. 4.

148 CF, *CSN*, 2023, p. 12.

149 CF, *CSN*, 2023, p. 12 ; OAS, *Best Practices National CSIRT*, 2016, p. 19 ; SALAMON, p. 29. Pour un exemple, voir l'organisation.

et moyennes entreprises (PME) sont toujours plus visées par des cyberattaques[150]. Ces entreprises contribuent également à l'amélioration de la cybersécurité, en participant à l'innovation et en proposant des produits et processus. Les milieux économiques ont besoin de sécurité pour être compétitifs[151].

Les milieux scientifique et académique participent aussi à ces évolutions, 83
avec la recherche visant à une implémentation appropriée de la cybersécurité par la collaboration du milieu académique et des centres de recherche spécifiques[152]. Un campus cyberdéfense[153] a par ailleurs été établi pour renforcer la collaboration entre les cantons, l'économie et le milieu scientifique, pour détecter de manière précoce les cybertendances, pour développer des technologies contre les cybermenaces et pour former les spécialistes[154].

Finalement, certaines organisations internationales et ONG participent 84
à différentes mesures permettant d'assurer la protection contre les cybermenaces[155]. Elles peuvent typiquement être actives dans la sensibilisation ou plus largement dans la collaboration internationale, notamment par le biais de leur implication dans des centres de partage et d'analyse d'informations (*Information Sharing and Analysis Centres,* ISAC)[156].

C. La gestion de cyberincidents

1. Les notions

Les cyberincidents impliquent que les organisations qui y sont confrontées 85
doivent les gérer. Si l'ISO définit la gestion des incidents liés à la sécurité de l'information comme un « ensemble de processus visant à détecter, rapporter, apprécier, gérer et résoudre les incidents liés à la sécurité de l'information, ainsi qu'à en tirer des enseignements », la gestion des cyberincidents pourrait, dans la logique de la présente étude, se limiter aux incidents détenant une composante cyber et sans s'étendre à l'entier de la sécurité de l'information[157].

150 OFCS, *Stratégie de l'OFCS,* 2023, p. 3.

151 OAS, *Best Practices National CSIRT,* 2016, p. 19 ; OFCS, *Stratégie de l'OFCS,* 2023, p. 4 ; SALAMON, p. 29. Sur un marché par ailleurs très fragmenté en raison de la diversité des solutions, cf. ENISA, *Good practices in innovation on cybersecurity under the National Cyber Security Strategies,* 2019, p. 25 s.

152 ENISA, *Good practices in innovation on cybersecurity under the National Cyber Security Strategies,* 2019, p. 26 ; OAS, *Best Practices National CSIRT,* 2016, p. 18.

153 Le CYD Campus, cf. *infra* N 252.

154 CF, *Rapport « La politique de sécurité de la Suisse »,* 2021, p. 35.

155 Cf. *infra* N 337 ss pour quelques exemples.

156 FF 2023 84, p. 15 et 32.

157 Art. 3.32 ISO/IEC 27000 : 2018.

Tout incident nécessite d'être géré, indépendamment de sa portée ou de son ampleur. Néanmoins, selon sa gravité, son déroulement ou ses impacts, les mesures déployées ne sont pas forcément similaires. Dans la mesure où des cyberincidents de faible gravité se produisent presque quotidiennement, les organisations doivent disposer de capacités désignées à cet effet, souvent internes, mais possiblement externes, pour y répondre et rétablir une situation sûre. Lorsqu'un cyberincident prend plus d'ampleur, il est souvent fait appel, comme nous le verrons[158], à une prestataire interne ou externe spécialisée dans la gestion de cyberincidents, afin de prendre les mesures qui s'imposent.

86 D'un point de vue terminologique, la langue anglaise effectue parfois une distinction entre *incident handling* et *incident response*[159] : la première notion englobe toutes les actions consistant à détecter, rapporter, évaluer, répondre et apprendre des incidents. La seconde correspond plus spécifiquement aux mesures tendant à atténuer ou à résoudre un incident, ou encore à rétablir une situation sûre, ce une fois qu'un incident s'est produit[160]. Cette distinction n'est pas toujours nette et certaines personnes et organisations considèrent que ces deux termes sont synonymes. De la même manière, certaines considèrent que la réponse aux incidents comprend les actions comprises comme faisant partie de la gestion de cyberincidents par les auteures effectuant la distinction[161]. Néanmoins, la présente étude se rapproche de la conception de l'Agence de l'Union européenne pour la cybersécurité (ENISA) et se focalise sur la gestion de cyberincidents, qui comprend les mesures préventives et réactives aux cyberincidents. La réponse aux cyberincidents couvrira dans la présente étude les mesures réactives faisant partie de la gestion de cyberincidents.

87 Certains concepts se rapprochent de la gestion de cyberincidents sans en être pour autant des synonymes. Il en va de la sorte pour la gestion de crise cyber, pour la continuité des activités *(business continuity)* et pour la reprise après sinistre *(disaster recovery)*. Nous allons brièvement examiner ces notions

158 Cf. *infra* N 272 ss.

159 Le terme de défense peut également être utilisé pour parler de défense active ou de *hackback* et de défense passive, cf. pour plus d'informations WEF, *Cyber Resilience Playbook for Public-Private Collaboration*, 2018, p. 51. Il sera utilisé au sein de la présente étude exclusivement pour parler du domaine de la cyberdéfense.

160 ISO/IEC 27035-1 : 2016, p. 2 ; ALBERTS et al., p. 3 s. ; ENISA, *Good Practice Guide for Incident Management*, 2010, p. 10, document dans lequel l'ENISA distingue l'*incident management* (qui comprend la gestion d'incident, de vulnérabilités, les annonces et alertes et autres prestations de gestion d'incident), l'*incident handling* (qui englobe, au sein de l'incident management, les étapes de la détection et de la réaction à un incident) et l'*incident response* (qui est la dernière étape de la réaction à un incident).

161 Voir notamment KILLCRECE et al., *State of Practice of CSIRT*, 2003, p. 83 ; MITROPOULOS/PATSOS/DOULIGERIS, p. 355.

afin de les comparer à la gestion de cyberincidents, qui demeure le centre de l'analyse de la présente étude.

88 La notion de gestion de cyberincidents doit être distinguée d'autres terminologies, dont la gestion de crise cyber ainsi que la reprise après sinistre ou la continuité des activités. Une crise cyber a lieu lorsqu'un cyberincident prend une ampleur telle que l'activité commerciale, la réputation, la position économique ou encore les fonctions essentielles d'une organisation sont susceptibles d'être impactées. La gestion de crise cyber consiste en une extension de la gestion d'un cyberincident majeur qui se superpose à la gestion du cyberincident qui implique un impact commercial plus large et une réelle intervention stratégique ; elle dépasse donc la gestion d'un cyberincident isolé[162]. La gestion de crise cyber atteint un niveau plus élevé et s'accompagne de l'établissement de priorités commerciales, pouvant aller jusqu'à la désactivation à long terme d'une infrastructure critique ayant pour conséquence des pertes de revenus, d'emplois et de disponibilité de certains services. Les décisions concernant la gestion de crise cyber sont souvent prises à un échelon différent de celles concernant la gestion de cyberincidents, en intégrant encore davantage de collaboratrices, de niveaux et de domaines internes à l'organisation[163].

89 De la même manière que la gestion de crise, les notions de reprise après sinistre ou de continuité des activités sont à distinguer de celle de gestion de cyberincidents. En particulier, la prestataire de gestion de cyberincidents peut détenir des compétences de planification de la reprise après sinistre et de la continuité des activités parmi ses compétences de gestion de la qualité de la sécurité. Ces compétences sont donc séparées des compétences de gestion de cyberincidents et concernent la continuité des activités de l'organisation et la reprise des opérations commerciales après des événements liés aux cybermenaces, cyberincidents et cyberattaques[164]. Elles consistent en la fourniture de conseils pour les activités en termes de résilience organisationnelle. Ces conseils sont fournis en tenant compte de l'environnement et des contraintes (typiquement liées aux ressources) existantes pour que la reprise

162 ENISA, *Good Practice Guide for Incident Management,* 2010, p. 22 ; FIRST, *CSIRT – Services Framework,* 2019, p. 28 ss. Voir au niveau étatique, GCSCC, *Cybersecurity capacity review – Switzerland,* 2020, p. 29 ; UIT, p. 41. Pour plus d'informations, voir notamment GORECKI Andrew/SULLIVAN Matthew, *Deciphering Between Incident Management and Crisis Management*.

163 FIRST, *CSIRT – Services Framework,* 2019, p. 12. La gestion de crise cyber peut également être entendue à un niveau étatique ou à un niveau transfrontière, cf. CF, *CSN,* 2023, p. 26 ; art. 9 Directive SRI2.

164 ENISA, *Good Practice Guide for Incident Management,* 2010, p. 26 ; KILLCRECE et al., *State of Practice of CSIRT,* 2003, p. 66 ; WEST-BROWN et al., p. 33.

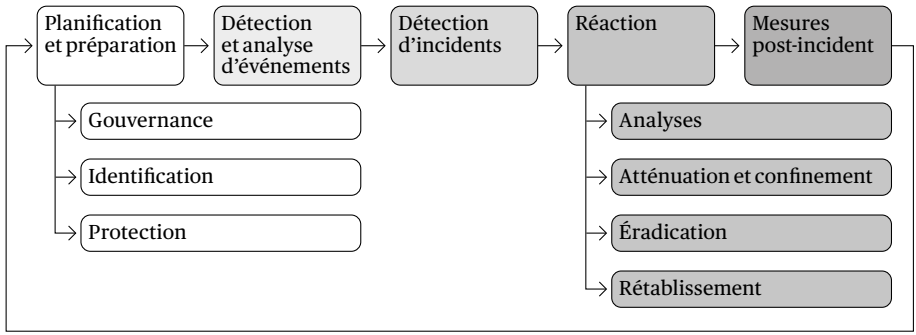
après sinistre et le plan de continuité soient mis en œuvre d'une façon permettant l'alignement avec les stratégies de gestion de cyberincidents[165].

2. Les mesures de gestion de cyberincidents

a. Un aperçu des étapes de la gestion de cyberincidents

90 Parmi les mesures généralement reconnues en pratique, l'on peut procéder à une première distinction chronologique entre les mesures préventives, détectives et réactives[166]. Il est en effet primordial de se préparer aux incidents et de réagir rapidement dès la détection d'une anomalie. Ces différents groupes de mesures de cybersécurité méritent d'être parcourus et illustrés du fait que les mesures concrètes sont très variées en pratique et qu'elles suivent le cours des évolutions technologiques[167]. Concrètement, nous allons concevoir la gestion de cyberincidents comme suit :

Schéma 4 : les principales étapes de la gestion de cyberincidents[168]



91 Naturellement, ce schéma ne représente pas une vision universelle et il ne présente pas tous les détails de la gestion de cyberincidents. Il illustre les principales étapes de la gestion de cyberincidents et de la garantie de la cybersécurité face aux cyberincidents au sein d'une organisation. Les étapes principales du cycle de vie de la gestion de cyberincidents proviennent du NIST[169]. La

165 FIRST, *CSIRT – Services Framework*, 2019, p. 57.

166 Voir par exemple ENISA, *Good Practice Guide for Incident Management*, 2010, p. 10 ; OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »*, 2021, p. 102.

167 À noter que les mesures techniques et organisationnelles ne seront pas approfondies dans le cadre d'une étude juridique comme la présente étude.

168 Ces notions et étapes seront approfondies, cf. *infra* N 291 ss.

169 NIST, *Computer Security Incident Handling Guide*, 2012, p. 21.

planification et la préparation représentent la première étape, divisée selon les nouvelles fonctions élaborées par le NIST dans son cadre relatif à la cybersécurité[170]. La réaction est divisée en différentes catégories d'action selon la perception de l'ENISA pour la gestion de cyberincidents[171].

92 Alors que les mesures centrales de la gestion de cyberincidents peuvent être divisées entre la prévention, la détection et la réaction, il existe d'autres mesures complémentaires. La collecte et l'exploitation de renseignements (ou de *threat intelligence*) constituent par exemple des mesures présentant une utilité à chaque étape de la protection contre les cybermenaces à conduire en parallèle de la stricte gestion d'un cyberincident. Les cyberassurances peuvent servir de mesures complémentaires aux mesures susmentionnées, comme les mécanismes de certification, d'évaluation ou de labellisation permettent d'attester d'un niveau de sécurité adéquat.

b. La planification et la préparation

93 Les mesures préventives doivent être mises en œuvre par toute organisation pour prévenir les cyberincidents et prévoir comment y réagir le cas échéant. La préparation d'une organisation aux cyberincidents permet en d'autres termes d'éviter ou de réduire la probabilité d'incidents. Elle peut également être perçue comme la première phase de gestion d'incidents[172]. En effet, une fois un cyberincident détecté, des mesures comme la formation et la sensibilisation ou encore comme l'analyse de risques permettent aussi de savoir comment et où attribuer les ressources ainsi que planifier les mesures de mitigation des risques découverts[173]. La planification et la préparation doivent être comprises sur un plan stratégique et sur un plan opérationnel.

94 Il est important de débuter la cybersécurité par la gouvernance. La gouvernance comprend l'établissement d'une stratégie de cybersécurité, de la stratégie de gestion de risques, de politiques, de procédures et de processus de

170 NIST, *Public Draft : The NIST Cybersecurity Framework 2.0,* 2023, p. 5 s. ; NIST, T*he NIST Cybersecurity Framework (CSF) 2.0,* 2024, p. 3.

171 ENISA, *Good Practice Guide for Incident Management,* 2010, p. 10. L'on peut aussi voir une certaine inspiration de ce qui suit : OFAE, *Norme minimale pour améliorer la résilience informatique,* 2023 ; KILLCRECE et al., *State of Practice of CSIRT,* 2003, p. 86 ; MORGUS et al., *CSIRT Basics for Policy-Makers*, 2015, p. 13. Le schéma et ses différentes phases serviront de base pour les mesures et les exigences comprises dans la présente étude.

172 Il va de soi que la cybersécurité passe en partie par une préparation adéquate, cf. BENHAMOU/BERNARD/DURAND, p. 38.

173 OFAE, *Norme minimale pour améliorer la résilience informatique,* 2023, p. 18 s. et 22 ; LUNDELL, p. 3 s. La sensibilisation, la formation du personnel sera primordiale, dans la mesure où les cyberattaques et cyberincidents ont encore souvent comme origine le facteur humain, cf. TEICHMANN/GERBER, *Les chevaux de Troie,* 2021, N 31.

cybersécurité à l'interne d'une organisation. En outre, les tâches et fonctions principales pour la cybersécurité doivent être réparties et attribuées[174]. Il est nécessaire de disposer d'une politique évolutive de sécurité contenant des principes, règles et pratiques fondamentales. Les responsabilités doivent toujours être clairement définies et l'établissement d'un inventaire des ressources (organisationnelles, matérielles et techniques) est recommandé[175]. Sur cette base, un plan de gestion aux cyberincidents doit être adopté pour connaître les étapes à suivre en cas d'événement ou, plus précisément, d'incident[176]. Parmi les processus devant être mis en place, les organisations doivent prévoir les flux de communications qui prendront place tout au long du processus de cybersécurité, poser les politiques relatives à la documentation et ainsi de suite.

95 Ensuite, il s'agit d'identifier les risques pour l'organisation, en comprenant les biens, infrastructures, systèmes, services et personnes à protéger. Les analyses de risques constituent l'un des piliers des mesures de cybersécurité préventive, dans la mesure où elles permettent, même aux organisations ne disposant que de ressources limitées, de comprendre et de décider où attribuer leurs moyens. Cette étape permet également de surveiller et modifier, si besoin, les stratégies ou processus établis durant la phase de gouvernance, celle-ci demeurant applicable sur l'ensemble du processus de gestion de cyberincidents[177].

96 Finalement, les organisations doivent utiliser des mesures de protection pour prévenir les cyberincidents et pour réduire les risques de la réalisation de cybermenaces[178]. Dans ce contexte, les mesures doivent être techniques et organisationnelles. Du point de vue technique, les mesures se rapportent directement à l'aspect technique du système informatique ; l'on peut citer à titre d'exemple la journalisation et la gestion des accès aux systèmes informatiques d'une organisation, qui permettent de surveiller les accès et de détecter des événements inhabituels, ou encore le chiffrement de données confidentielles traitées[179]. Du point de vue organisationnel, les mesures sont plus larges et se

174 ISO/IEC 27032: 2023, p. 14 ; NIST, *Public Draft : The NIST Cybersecurity Framework 2.0,* 2023, p. 5 ; NIST, *The NIST Cybersecurity Framework (CSF) 2.0,* 2024, p. 3 et 11.

175 KRAL, p. 2 ; GILLIÉRON Philippe, *L'établissement d'un plan de réponse en cas de faille de sécurité* ; LUNDELL, p. 6.

176 KRAL, p. 3.

177 NIST, *Public Draft : The NIST Cybersecurity Framework 2.0,* 2023, p. 5 et 7 ; NIST, *The NIST Cybersecurity Framework (CSF) 2.0,* 2024, p. 3 s.

178 NIST, *The NIST Cybersecurity Framework (CSF) 2.0,* 2024, p. 4.

179 Voir par exemple ISO/IEC 27001 : 2013 ; WEBER/WILLI, p. 31 s. Sur la définition des mesures techniques dans le contexte de la protection des données personnelles, cf. PFPDT, *TOM,* 2024, p. 7.

rapportent à l'environnement du système informatique ; de manière générale, il convient de disposer des moyens de formation et de collaboration pour créer une culture de cybersécurité au sein d'une organisation[180].

c. La détection

Les cyberincidents peuvent être détectés à l'aide des individus, d'outils techniques ou de moyens organisationnels[181]. Du point de vue humain, des cyberincidents peuvent être détectés grâce aux utilisatrices, internes ou externes à une organisation[182]. Sur le plan technique, plusieurs types d'outils existent[183]. À titre d'exemple, les systèmes de détection automatique sont fréquemment utilisés, procédant par de la surveillance ou du *monitoring* du trafic informatique. Les systèmes de détection et de prévention d'intrusion (*intrusion detection and prevention systems,* IDPS) permettent notamment d'empêcher des intrusions ainsi que de paramétrer des alertes pour réagir notamment lors de cyberincidents[184]. Il existe d'autres outils techniques permettant de détecter des incidents. Par exemple, un système de gestion de l'information et des événements en matière de sécurité (*security information and event management,* SIEM) permet d'identifier les comportements inhabituels ou suspects en analysant en temps réel le ficher des accès et des événements. En outre, les outils de prévention de perte de données (*data loss prevention,* DLP), vont avoir pour objectif que des données ne soient pas compromises ou perdues par un accès indu. Finalement, certains pare-feux peuvent être programmés de sorte à reconnaître des codes malicieux ou des activités suspectes[185]. 97

180 ISO/IEC 27032: 2023, p. 15 ; NIST, 800-53, rev. 5, AU-1, p. 65 ; NIST, 800-61, rev. 2, p. 24 ; WEF, *Cyber Resilience Playbook for Public-Private Collaboration*, 2018, p. 37 ; WEBER/WILLI, p. 31 ss ; WEST-BROWN et al., p. 29 ss. Pour une definition des mesures organisationnelles à titre de comparaison en protection des données, cf. PFPDT, *TOM*, 2024, p. 7.

181 ISO/IEC 27035-3 : 2020, p. 7 ; NIST, *Public Draft : The NIST Cybersecurity Framework 2.0*, 2023, p. 6.

182 Les personnes impliquées pourraient détecter de manière proactive, à savoir si elles cherchent activement des événements, ou de manière réactive, en rapportant un événement découvert pendant une utilisation autre d'un système ou d'une application, cf. ISO/IEC 27035-3 : 2020, p. 10.

183 OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »*, 2021, p. 154. Pour d'autres exemples d'outils de détection proactive, voir ISO/IEC 27035-3 :2020, p. 8 ss. Pour plus de détails, voir ISO/IEC 27039 : 2015 ; NIST, 800-61, rev. 2, p. 27 s.

184 MEYER/DAVIES, N 50.

185 ISO/IEC 27035-3 : 2020, p. 7 ; OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »*, 2021, p. 134 ; MITROPOULOS/PATSOS/DOULIGERIS, p. 357 s. ; SALAMON, p. 122 s. ; WEBER/WILLI, p. 35.

98 Sur le plan organisationnel, il s'agit principalement de disposer de services compétents spécifiquement pour la détection d'incidents[186]. Concrètement, ces services vont effectuer de la surveillance ou du *monitoring*. La mise en œuvre de méthodes dites des « quatre yeux » est bénéfique pour s'assurer que la surveillance est justifiée et correctement menée, de même que les contrôles relatifs à d'éventuelles portes dérobées *(backdoors)* ou à l'utilisation frauduleuse d'accès[187].

d. La réaction et les mesures post-cyberincident

99 Les mesures réactives doivent être prises lorsqu'un cyberincident a été détecté, en vue d'éradiquer la source du problème, réduire le risque à un niveau acceptable et limiter les dommages entraînés. Ces mesures doivent être prises sur la base du plan d'intervention prévu[188]. Une fois le cyberincident maîtrisé, les organisations restaurent une situation sûre. La restauration comprend le fait de reprendre les opérations de l'organisation, de limiter l'impact final et global d'un cyberincident et de prévoir les communications à effectuer au sujet du cyberincident et la gestion de ce dernier dans leur ensemble ainsi qu'au sujet du retour à la normale[189]. Il est également essentiel de prendre du temps pour tirer les leçons du cyberincident et de sa gestion, afin d'améliorer la résilience future de l'organisation.

100 Sur le plan technique, il s'agit d'abord de collecter et analyser les différents éléments à disposition, pour ensuite limiter l'étendue du cyberincident, éradiquer le problème et réduire les dommages avant de recouvrer une situation sûre, en documentant le tout pour en tirer finalement les enseignements qui s'imposent[190]. Sur la base de l'analyse du cyberincident, il convient bien souvent en pratique de confiner ce dernier. Par exemple, dans un cas de propagation d'un logiciel malicieux, il est souvent préconisé de le contenir

186 ISO/IEC 27035-3 : 2020, p. 7.

187 WEBER/WILLI, p. 35. Le principe des quatre yeux importe plus largement lorsqu'il s'agit pour des personnes et des organisations d'accéder à des informations, cf. par exemple OA, *Enquête administrative « Fuite de données »,* 2024, p. 104.

188 NIST, *Public Draft : The NIST Cybersecurity Framework 2.0,* 2023, p. 6 ; NIST, T*he NIST Cybersecurity Framework (CSF) 2.0,* 2024, p. 22 ; WEBER/WILLI, p. 35. Pour plus d'informations au sujet des mesures réactives effectuées par les prestataires de gestion de cyberincidents, cf. *infra* N 296 ss.

189 NIST, *Public Draft : The NIST Cybersecurity Framework 2.0,* 2023, p. 6 ; NIST, *The NIST Cybersecurity Framework (CSF) 2.0,* 2024, p. 22.

190 AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung,* 2018, p. 27 ; ENISA, *Good Practice Guide for Incident Management,* 2010, p. 51 ; WEST-BROWN et al., p. 26, 79 ss.

afin qu'il n'infecte pas davantage de systèmes informatiques[191]. À la suite du confinement, des mesures techniques sont prises afin d'éradiquer la source de l'incident[192]. Une fois cette opération réussie, le système doit être restauré et nettoyé, ainsi que les données récupérées[193].

Sur le plan organisationnel, des mesures s'imposent également. Il convient 101
d'appliquer le plan de gestion établi à l'avance. En outre, toutes les mesures prises doivent être documentées et il est important de collecter les informations sur l'incident et sa gestion afin principalement d'en tirer les bons enseignements, d'améliorer le plan de gestion de cyberincidents, de prévenir la survenance d'événements similaires et de se préparer à des conséquences juridiques[194]. La communication au sein de l'organisation lésée doit être menée efficacement pour que toutes les collaboratrices puissent prendre les mesures pour éviter, par exemple, la dispersion d'un logiciel malicieux, ou pour que les personnes qualifiées puissent approuver les différentes mesures[195].

Certaines communications externes doivent en pratique aussi être 102
faites, qu'elles soient obligatoires ou facultatives. Il faut parfois procéder à une annonce de violation de la sécurité des données à la PFPDT (art. 24 al. 1 LPD), à une information aux personnes concernées (art. 24 al. 4 LPD), au signalement à l'OFCS (art. 74b ss LSI) ou aux obligations d'annonce sectorielles (par exemple art. 29 al. 2 LFINMA). Certaines de ces annonces aboutissent à des recommandations sur les mesures à prendre[196]. Des communications plus larges sont aussi susceptibles d'être faites, par exemple pour une organisation importante en pratique qui devrait effectuer un communiqué de presse.

191 NIST, 800-61, rev. 2, p. 35 s. ; KRAL, p. 6 s. ; LUNDELL, p. 8 ; MITROPOULOS/PATSOS/DOULIGERIS, p. 359 s.

192 ISO/IEC 27035-3 : 2020, p. 22 ; KRAL, p. 7 s. ; LUNDELL, p. 9 ; MITROPOULOS/PATSOS/DOULIGERIS, p. 360 s. ; WEST-BROWN et al., p. 29.

193 ISO/IEC 27035-3 : 2020, p. 23 ; OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »,* 2021, p. 154 ; NIST, 800-53, rev. 5, IR-4, p. 153 ; NIST, *Computer Security Incident Handling Guide,* 2012, p. 37 ; OFJ, *Rapport sur la révision totale de l'ordonnance relative à la loi fédérale sur la protection des données,* 2021, p. 19 ; GILLIÉRON Philippe, *L'établissement d'un plan de réponse en cas de faille de sécurité* ; MITROPOULOS/PASTOS/DOULIGERIS, p. 361 ; WEBER/WILLI, p. 36.

194 COBIT 5, BAI01.13 ; ISO/IEC 27035-1 : 2016, p. 12 ; NIST, 800-53, rev. 5, CP-2, p. 116-118 et IR-4, p. 152 ; NIST, *Computer Security Incident Handling Guide,* 2012, p. 31 et 38 ss ; ENISA, *How to set up CSIRT and SOC,* 2020, p. 22 ; KRAL, p. 9 ; MITROPOULOS/PATSOS/DOULIGERIS, p. 362.

195 ISO/IEC 27035-2 : 2016, p. 13 ; NIST, 800-61, rev. 2, p. 33 s.

196 DE WERRA/BENHAMOU, N 7. Pour plus d'informations sur les annonces susceptibles d'être effectuées par une prestataire de gestion de cyberincidents, cf. *infra* N 318 ss.

e. Des mesures complémentaires

(i) Le traitement de renseignements sur les cybermenaces

103 Les personnes compétentes pour la gestion de cyberincidents détiennent souvent des compétences relatives au traitement de renseignements sur les cybermenaces ou de *cyber threat intelligence* (CTI)[197]. L'enchaînement des phases de CTI conduit à des résultats composés d'indicateurs techniques (comme des échantillons de logiciels présumés malveillants ou des indicateurs de compromis) ou non techniques (comme des discussions sur des forums de pirates informatiques) qui peuvent être collectés sur la base notamment d'analyses de traces ou de recherches de renseignements de source ouverte (*open source intelligence,* OSINT)[198]. Le résultat du traitement de renseignements prend la forme d'un rapport de renseignement servant à connaître, décrire et comprendre des cybermenaces. Il permet également de résoudre des cas concrets, présenter des phénomènes, ou encore planifier des vecteurs d'attaque pour réaliser l'activité[199]. Il est important que les rapports de renseignements soient précis *(accurate),* opportuns *(timely),* exploitables et intégrés à des processus pour qu'ils puissent être exploités dans un délai dans lequel ils sont utiles et adaptés[200].

104 Les compétences relatives au traitement ou à l'exploitation de renseignements sur les cybermenaces ne font pas partie des compétences de gestion de cyberincidents mais y sont parallèles. Lorsqu'elles existent, elles doivent être exercées à toutes les étapes de la gestion d'un cyberincident, entre lesquelles l'on peut faire des allers-retours. Les compétences de traitement de la CTI ne sont par ailleurs pas forcément attribuées aux membres de la prestataire de gestion de cyberincidents, mais peuvent l'être à d'autres personnes expertes[201]. Néanmoins, lorsque ces compétences incombent à la prestataire de gestion de cyberincidents, elles sont dispersées tout au long du processus de gestion de cyberincidents.

105 Il existe trois catégories de CTI, relatives aux finalités poursuivies : tactique, opérationnelle et stratégique[202]. La finalité tactique sera atteinte par

197 Sur le cycle des renseignements ou l'« *intelligence cycle* », cf. notamment CENTRAL INTELLIGENCE AGENCY, *The intelligence cycle*.

198 Sur les analyses inter-incidents permettant d'obtenir de la CTI, cf. ISO/IEC 27035-3 : 2020, p. 19. Sur les étapes de CTI, cf. JOHANSEN, p. 435.

199 WEF, *Cyber Resilience Playbook for Public-Private Collaboration*, 2018, p. 22 ; HÄMERLI, p. 191 ; SALAMON, p. 82 ss.

200 JOHANSEN, p. 430.

201 ISO/IEC 27037 : 2012, p. 12.

202 JOHANSEN, p. 432.

l'utilisation des renseignements dans la pratique, typiquement de gestion de cyberincidents. Les informations collectées par CTI devraient également avoir un impact à d'autres niveaux, à savoir opérationnel ou stratégique. Les informations transmises par la CSIRT aux supérieures devraient effectivement contribuer à appréhender les menaces pesant sur l'organisation et à les mettre à jour[203].

(ii) La cyberassurance

106 La cyberassurance peut être définie comme l'assurance visant à couvrir les cyberrisques et les cyberincidents[204]. Les cyberassurances ont pour vocation à couvrir les cyberrisques ; elles couvrent certains cyberrisques et apportent aux organisations preneuses d'assurance une aide dans la gestion de cyberincidents, typiquement en cas d'atteinte à la réputation, de vol de données, de virus, d'usurpation d'identité ou encore en termes de responsabilité[205]. Elles servent à couvrir une variété de risques susceptibles d'engendrer des dommages financiers. Elles sont donc complémentaires aux mesures techniques et organisationnelles[206]. La compagnie d'assurance peut prendre en charge certains dommages causés par l'organisation preneuse d'assurance comme certains dommages que cette dernière subit[207]. La cyberassurance permet à l'organisation preneuse d'assurance de transférer certains risques à une tierce personne. Certaines compagnies d'assurance participent à la prévention au sein des preneuses d'assurance et à l'amélioration de la gestion des risques en plus de couvrir des dommages engendrés par la survenance d'un cyberincident[208]. Les cyberassurances peuvent présenter un intérêt pour les infrastructures critiques, les autres entreprises voire les individus.

107 Il n'existe en Suisse aucune obligation légale de conclure une cyberassurance[209]. C'est un marché libéral sur lequel différentes compagnies offrent une grande diversité de prestations. Les offres varient en fonction des compagnies d'assurance. En d'autres termes, les événements couverts varient d'une police

203 ISO/IEC 27035-2 : 2016, p. 26 ; KIME, p. 8 s. et 17 ss.

204 DE WERRA/BENHAMOU, N 3.

205 NCSC, *Rapport semestriel 2021/1,* 2021, p. 25 s. ; FEM, p. 57 ; DE WERRA/BENHAMOU, N 48 ; WEBER/WILLI, p. 36.

206 WEF, *Cyber Resilience Playbook for Public-Private Collaboration,* 2018, p. 57 ; DE WERRA/BENHAMOU, N 3 ; SURY, *Digital in Law,* 2021, p. 156 ; WEBER/WILLI, p. 205.

207 SURY, *Digital in Law,* 2021, p. 156.

208 ENISA, *National Capabilities Assessment Framework,* 2020, p. 87.

209 Contrairement à certaines obligations notamment de conclure une assurance RC en matière d'incendie pour immeubles ou de circulation routière, cf. DE WERRA/BENHAMOU, N 27 s. Nous sommes néanmoins en présence de contrats soumis aux règles de la LCA, cf. DE WERRA/BENHAMOU, N 44.

d'assurance à l'autre[210]. En outre, les assurances se limitent rarement aux remboursements de pertes économiques, mais offrent d'autres prestations, à l'instar de conseils juridiques ou d'autres services annexes comme l'analyse de risques[211]. Il n'existe pas non plus d'harmonisation entre les formes utilisées par les compagnies de cyberassurance : certaines se limitent à des conditions générales (CG) d'une assurance non spécifique incluant la couverture de certains cyberrisques *(silent cyber risk),* d'une police autonome et ainsi de suite[212].

108 Bien que des cyberassurances soient de plus en plus conclues en pratique, nous attirons l'attention sur les questions que soulève leur portée limitée et sur le fait qu'elles ne peuvent pas se substituer aux autres mesures de cybersécurité[213]. En effet, il n'est tout d'abord pas toujours évident de prédire l'ensemble des dommages pouvant découler d'un cyberincident[214]. Ensuite, du fait que les dommages remboursés par les compagnies d'assurance ne sont pas forcément les mêmes, certains risques ne sont pas forcément couverts, ou par le biais de montants plafonnés ou limités à une certaine période[215]. En outre, les compagnies d'assurance ont facilement tendance à imposer à leurs clientes des exclusions ou limitations pour certains types de dommage et le seuil de diligence attendu de la preneuse d'assurance n'est pas toujours clair[216]. Ces différents constats fondent une certaine réticence de la part des potentielles preneuses d'assurance[217]. Au sujet des événements couverts, certaines compagnies assurent le paiement de rançons[218], pratique qui pourrait inciter les délinquantes à se focaliser sur les entreprises assurées pour avoir plus de

210 Voir par exemple le comparatif publié par « À bon entendeur », *Dangers du net : que valent les assurances contre les cyberrisques*.

211 ENISA, *Cyber Insurance : Recent Advances, Good Practices and Challenges,* 2016, p. 14 ss ; ces prestations, en principe dévolues aux équipes de gestion de cyberincidents, peuvent en partie incomber à une compagnie d'assurance.

212 ENISA, *Cyber Insurance : Recent Advances, Good Practices and Challenges,* 2016, p. 14 ; DE WERRA/BENHAMOU, N 45 ss.

213 DE WERRA/BENHAMOU, N 82 ; LEMNITZER, p. 122 ; SURY, *Digital in Law,* 2021, p. 159 s. ; YOUNG et al., p. 44.

214 DE WERRA/BENHAMOU, N 58 ; YOUNG et al., p. 45.

215 DE WERRA/BENHAMOU, N 50 sur l'indemnisation plafonnée ou limitée dans le temps en cas de clause pour la protection des données personnelles.

216 DE WERRA/BENHAMOU, N 60 sur l'étendue du devoir de diligence attendu de la preneuse de cyberassurance.

217 ENISA, *Cyber Insurance : Recent Advances, Good Practices and Challenges,* 2016, p. 21 ; ASSOCIATION POUR LE MANAGEMENT DES RISQUES ET DES ASSURANCES DE L'ENTREPRISE, *Lumière sur la cyberassurance,* édition 2021, p. 19 et 36 ; LEMNITZER, p. 121.

218 Ce qui a par ailleurs été admis par le TF qui a récemment imposé à une compagnie d'assurance de couvrir le paiement d'une rançon car elle n'avait pas apporté la preuve que le paiement aurait servi les intérêts d'un groupe de pirates informatiques sous sanction américaine malgré la clause de limitation et d'exclusion de responsabilité en cas de sanctions, cf. TF, 4A_206/2023 du 17 août 2023, c. 5.

chances d'obtenir un paiement. Les entreprises doivent donc bien réfléchir avant de conclure une cyberassurance, notamment en termes de coûts et d'impact sur le reste de leur cybersécurité[219]. Par ailleurs, l'on peut craindre que certaines entreprises négligent les mesures techniques et organisationnelles pour se reposer sur l'assurance. Il faut néanmoins reconnaître que la conclusion d'un contrat de cyberassurance est susceptible d'inciter certaines preneuses d'assurance à investir davantage dans leur dispositif de sécurité, dans la mesure où certaines compagnies d'assurance ne concluent qu'avec des clientes démontrant un niveau de sécurité qu'elles jugent « suffisant ». D'autres mécanismes similaires existent, en passant par la diminution des primes pour les organisations certifiées ou par l'exclusion de la couverture pour faute (ou du moins pour faute grave) de l'assurée par de nombreuses polices d'assurance[220].

Compte tenu de ces avantages et inconvénients propres au système dans son fonctionnement actuel, il convient selon nous de ne pas s'appuyer de façon trop importante sur les cyberassurances en tant que mesure de sécurité, bien qu'il faille reconnaître qu'il s'agit d'une mesure complémentaire et compensatrice importante en pratique[221]. 109

(iii) Les évaluations, labels et certifications

L'évaluation consiste, dans ce contexte, en l'appréciation du niveau de sécurité d'un système ou d'un produit informatique sur la base de critères définis. La certification est la confirmation de l'accomplissement d'exigences prescrites, octroyée par un organisme indépendant accrédité[222]. Elle peut également être définie comme la confirmation formelle des résultats d'une évaluation. Les mécanismes de certification ont une valeur importante en pratique et certaines réglementations autorisent voire obligent le recours à de tels mécanismes[223]. Contrairement à la certification, le label est en principe apposé pour attester de certaines fonctions en dehors d'un cadre formel. Le label est en principe encadré par les lois du marché[224]. 110

219 NCSC, *Rapport semestriel 2021/1*, 2021, p. 26 ; YOUNG et al., p. 55. Sur les compagnies d'assurance prenant ou non en charge les prétentions en cas de rançongiciel, cf. DE WERRA/BENHAMOU, N 52 et références citées.

220 LEMNITZER, p. 121 ; YOUNG et al., p. 46.

221 Pour des recommandations au sujet des cyberassurances, cf. DE WERRA/BENHAMOU, N 61 ss ; LEMNITZER, p. 124 ss.

222 DEFR, *L'accréditation et la certification : en quoi se distinguent-elles ?* (consulté le 20.3.2024).

223 Cf. par exemple l'art. 13 LPD et l'OCPD, ou les art. 11 ss LDEP.

224 Il en va de la sorte pour le label conventionnel, que l'on peut opposer au label obligatoire, composé de normes étatiques devant être respectées par tout prestataire, cf. DE WERRA/BENHAMOU, N 75.

111 Les organismes compétents octroient parfois un label ou une certification sur la base d'auto-déclarations de la part des entreprises (qui attestent du respect de certaines fonctions), d'audits internes ou d'audits externes. Les labels ou les certifications sont aussi parfois octroyées sur la base d'analyses complémentaires de risques et de plusieurs tests, notamment dits de « pénétration » ou de simulation de cyberattaques, d'une activité de conseil et de formations et campagnes de sensibilisation du personnel, par exemple pour résister à des tentatives d'hameçonnage (ou *phishing*)[225].

112 L'évaluation permet principalement aux entreprises de connaître leur niveau de sécurité, d'assurer la confiance dans le fonctionnement de leur organisation, de s'autoresponsabiliser (en limitant l'intervention de l'État) et d'attester plus facilement d'un niveau adéquat de sécurité notamment dans le cadre d'actions en responsabilité[226]. Les labels et les certifications permettent aux organisations en bénéficiant d'inspirer une confiance plus élevée de la part notamment d'une clientèle, en fournissant des prestations sous le couvert du label ou de la certification. Les organisations peuvent, de la même manière que par l'évaluation, connaître leur niveau de sécurité. Les labels et les certifications permettent également aux différents secteurs et aux organisations labellisées, respectivement certifiées, de s'autoresponsabiliser (typiquement dans les cas où le label est octroyé sur la base d'auto-déclarations de conformité). La certification et certains labels peuvent présenter des avantages supplémentaires, en permettant aux organisations certifiées ou labellisées de contracter avec une compagnie d'assurance cyber ou de bénéficier de rabais sur les primes de cyberassurance[227]. Les compagnies d'assurance recommandent en tout cas régulièrement aux preneuses d'assurance de certifier leurs produits ou systèmes[228]. Finalement, la certification étant en principe encadrée par une base légale, elle fait l'objet d'un processus établi et reconnu par les organismes et autorités compétentes, ce qui implique une plus grande fiabilité et une plus grande confiance dans ce mécanisme.

113 Les évaluations et certifications sont parfois réglées en droit suisse pour des domaines spécifiques. Tel est le cas notamment pour la protection des

225 WEBER/WILLI, p. 206. Sur l'exemple de la certification ISO/IEC 27001, cf. ENISA, *Recommendations on European Data Protection Certification*, 2017, p. 38 s.

226 FF 2003 1915, p. 1947 s. ; WEBER/WILLI, p. 206.

227 En dehors de la cybersécurité, les certifications actuellement admises peuvent également présenter d'autres avantages tels que la possibilité pour une responsable du traitement privé en protection des données de renoncer à mener une analyse d'impact, cf. art. 22 al. 5 LPD ; FF 2017 6656, p. 6678.

228 ENISA, *Cyber Insurance : Recent Advances, Good Practices and Challenges*, 2016, p. 22, où est notamment citée la certification ISO 2700x.

données personnelles à l'art. 13 LPD et dans son ordonnance y relative (OCPD), pour la signature électronique (Loi sur la signature électronique), pour le dossier électronique du patient (art. 11 ss LDEP) ou encore pour la mise en circulation de dispositifs médicaux (art. 21 ss ODim). Il n'existe à l'heure actuelle pas d'obligation légale de certification pour la cybersécurité. Partant, les différentes organisations et entités traitant des informations par le biais de systèmes informatiques peuvent certifier leurs produits, leurs processus informatiques ou encore leurs collaboratrices sur une base volontaire. Différents référentiels internationaux sont reconnus par tous les secteurs confondus. Tel est le cas pour la certification ISO 27001, dont bénéficie notamment l'Office fédéral de l'informatique et de la télécommunication (OFIT) en Suisse[229]. Parallèlement, un marché plus local se développe sur le territoire helvétique afin de répondre au mieux à la demande existante, qui est composée de nombreuses PME. Toujours plus de petites organisations, non spécialisées, optent pour des labels en plein développement, ceux-ci étant plus accessibles pour de telles organisations[230].

D. Une conclusion

En Suisse, le domaine de la cybersécurité fait partie de la protection contre les cybermenaces, avec les domaines de la poursuite pénale de la cybercriminalité et de la cyberdéfense. Le domaine de la cybersécurité englobe l'ensemble des mesures servant à assurer la cybersécurité comme état. La cybersécurité comme état peut se définir de différentes façons, mais le droit suisse ne la définit plus. Il faut comprendre la cybersécurité comme regroupant la sécurité des moyens informatiques et la sécurité des informations traitées par le biais de moyens informatiques. Pour cette raison, la présente étude la définit comme la situation dans laquelle le traitement des informations, par des moyens informatiques, et les moyens informatiques fonctionnent comme prévu de façon sûre. 114

D'autres notions sont centrales. Les notions de cybermenace, de cyberrisque ou de cyberincidents et de cyberattaques doivent être définies afin de comprendre les composantes de la cybersécurité. La clarté des définitions varie entre les notions abordées, ce que l'on peut voir avec le terme d'infrastructure critique qui est central dans la présente étude. Sans en donner une définition plus claire déjà ici[231], la présente étude comprend les infrastructures 115

229 Au sujet de la certification ISO 27001 : 2013 de l'OFIT, cf. OFIT, *Certification*.

230 Voir notamment les labels Cyber-Safe et Digital Trust. Pour un exemple d'obtention du label Cyber-Safe, cf. OFCS, *Rapport semestriel 2023/II*, 2024, p. 10 s.

231 Question approfondie ci-dessous, cf. *infra* N 1211.

critiques comme les organisations et autorités actives dans les secteurs critiques de la Stratégie PIC. Parmi ces notions centrales, la gestion de cyberincidents couvre dans la présente étude les mesures préventives et réactives aux cyberincidents, ainsi que les mesures complémentaires qui peuvent exister.

116 Il s'agit maintenant de parcourir certains enjeux centraux lorsque l'on parle de cybersécurité, afin de comprendre les défis qui gravitent autour de ces questions et de mieux appréhender l'importance de la cybersécurité.

II. Un bref aperçu des principaux enjeux

A. Les enjeux globaux

1. La protection des informations

117 Il existe une diversité d'enjeux à prendre en considération dans la cybersécurité[232]. Une des finalités principales de la cybersécurité est d'assurer la sécurité des différentes informations traitées par le biais de moyens informatiques[233]. La sécurité des informations implique que les traitements d'informations doivent assurer la confidentialité, l'intégrité, la disponibilité et la traçabilité de ces informations (voir notamment l'art. 6 al. 2 LSI dans le contexte de la sécurité de l'information au sein de la Confédération)[234]. La confidentialité implique que seules les personnes autorisées doivent avoir accès aux informations à sécuriser. *A contrario,* les personnes non autorisées ne doivent pas pouvoir accéder aux informations. L'intégrité est préservée si les données sont exactes. Les informations doivent en outre être disponibles ou accessibles par les personnes autorisées et leur traitement doit être traçable[235].

118 Les informations à sécuriser peuvent être techniques, constitutives de données personnelles ou encore couvertes par des secrets. Comme nous le verrons[236], plusieurs instruments légaux imposent le traitement sécurisé de différents types d'informations qui coexistent[237]. Dans une perspective pratique, cette sécurité est assurée par des mesures aussi bien organisationnelles que techniques[238].

232 FF 2017 2765, p. 2772.

233 Sur l'interaction entre cybersécurité et sécurité de l'information, cf. *supra* N 45.

234 Les mêmes objectifs sont poursuivis par le principe de sécurité des données personnelles, cf. art. 2 OPDo ; OFJ, *Rapport explicatif OPDo,* 2022, p. 23.

235 FF 2017 2765, p. 2827 s. ; HUSI-STÄMPFLI, N 29.

236 Cf. *infra* N 817 ss.

237 À titre d'exemple, les prescriptions de la LSI s'appliquent de façon complémentaire à la LPD et à l'OPDo, FF 2017 2789. Les autorités compétentes au sens de la LSI et au sens de la LPD doivent coopérer, voir par exemple art. 41 OPDo.

238 CARON, N 44.

2. L'augmentation, la professionnalisation et la complexification des attaques

Bien qu'il soit difficile d'obtenir des informations reflétant parfaitement la réalité, une augmentation des cyberattaques est à déplorer ces dernières années[239]. Plusieurs raisons peuvent expliquer cette évolution. Parmi celles-ci figure naturellement l'utilisation croissante des TIC. L'augmentation des cibles potentielles donne lieu à une augmentation des cyberattaques, avec les adaptations des modes opératoires, la professionnalisation et la complexification des cyberattaques. 119

Concernant d'abord les cibles potentielles, plus il existe de systèmes connectés, plus important sera le nombre de vulnérabilités à exploiter, de même que le nombre de cibles ; c'est l'une des conséquences de l'interconnectivité et de l'interdépendance croissantes entre les réseaux et systèmes informatiques[240]. Ce facteur d'opportunité d'attaques constitue l'une des raisons à l'origine de l'explosion du nombre de cas de cybercriminalité ces dernières années, en permettant aux délinquantes de cibler une multitude de victimes simultanément[241]. 120

L'utilisation de technologies émergentes a pour conséquence l'augmentation des cibles potentielles et, en parallèle, un développement des modes opératoires des attaquantes. Les nouveaux outils favorisent la perpétration de cyberattaques, par exemple au moyen de l'utilisation de l'intelligence artificielle dont se servent des personnes malveillantes notamment pour cibler des personnes physiques ou morales, par l'utilisation croissante d'objets connectés par des victimes potentielles, par l'impunité permise par le cyberespace ou par l'exploitation de nouvelles cryptomonnaies comme cibles d'infractions ou comme outils de paiements dans la réalisation de cyberattaques[242]. 121

La professionnalisation et la complexification des attaques s'entremêlent et favorisent conjointement l'augmentation du nombre de cas. La cybercriminalité s'est fortement professionnalisée ces dernières années. Des rôles spécifiques sont aujourd'hui attribués à des commanditaires (ou à des *sponsors*) décidant d'attaques, à des organisations opératrices qui conduisent celles-ci, à des entreprises développant des outils malveillants ou encore à 122

239 Voir notamment NCSC, *Rapport semestriel 2021/1,* 2021, p. 4 et 19 ; OFS, *SPC,* 2022, p. 58 ; SOLOVE/HARTZOG, p. 17 ss.

240 DSOUZA, p. 205 ; SALAMON, p. 89.

241 DSOUZA, p. 204 ; NICOLET/PEISSARD, p. 164.

242 CSIS/MCAFEE, *Economic Impact of Cybercrime – No Slowing Down*, 2018, p. 5 et 14 ; GHERNAOUTI, *Cybercriminalité,* 2023, p. 19 ss.

des organisations et personnes hébergeant des contenus malveillants[243]. Certaines organisations criminelles se développent et deviennent de réelles entreprises existantes, mettant à disposition des réseaux malveillants des outils, afin de perpétrer des cyberattaques. Internet est donc aujourd'hui utilisé comme un réel réseau de commerce pour la cybercriminalité *(cybercrime-as-a-service),* dont une grande partie se déroule sur les marchés et forums du *dark web,* mais sans s'y limiter[244]. Sur ce marché grandissant offert par Internet, des spécialistes mettent à disposition du public des outils déjà programmés, et les individus possédant moins de capacités techniques peuvent s'en servir afin de perpétrer des attaques[245]. Il existe donc une multitude de personnes physiques et morales malveillantes, à l'instar d'opératrices de *botnets,* d'organisations soutenues par des États, de pirates informatiques ou *hackers* ou encore d'organisations criminelles et terroristes[246]. Le nombre de vendeuses augmente, le prix des informations fluctue en fonction de facteurs tels que la taille de l'entreprise, sa localisation ou son chiffre d'affaires[247]. Il en existe donc pour tous les types d'acheteuses malveillantes. À titre d'exemple sur les différentes données mises en vente, il existe des *zero day exploit markets,* des réseaux de vente de kits d'exploitation, de données soustraites ou de codes de *ransomwares (ransomware as-a-service)* au même titre que des services légaux de réseau privé virtuel (*Virtual Private Network,* VPN), ce qui permet à des individus ne possédant ni le temps ni l'expertise technique de procéder à des infractions en ligne[248]. L'écriture de *malwares* est maintenant automatisée et de nouveaux éléments sont générés chaque jour. Au-delà de ces améliorations techniques de bout en bout, il y a l'ingénierie sociale, souvent utilisée comme

243 SALAMON, p. 63 s.

244 ChF, *Rapport « Suisse 2035, les grands défis de demain en 20 questions »,* 2022, p. 113 ; EUROPOL, *Internet Organised Crime Threat Assessment IOCTA 2021,* 2021, p. 17 et 35 ss ; OFCS, *Rapport concernant les analyses de données effectuées après la cyberattaque contre l'entreprise Xplain,* 2024, p. 3 ; GHERNAOUTI, *Cybercriminalité,* 2023, p. 145 ss ; NICOLET/PEISSARD, p. 165 s. ; SALAMON, p. 89 s. ; CC-DRIVER, *Cybercrime-as-a-Service on the Internet*. Les réseaux informatiques tels que Tor ou le *dark web* sont effectivement utilisés par de nombreuses délinquantes, cf. CSIS/MCAFEE, *Economic Impact of Cybercrime – No Slowing Down,* 2018, p. 12 s.

245 BERTHIER, N 3.

246 DSOUZA, p. 205 ; GHERNAOUTI, *Cybercriminalité,* 2023, p. 98 ss.

247 SRC, *La sécurité de la Suisse,* 2022, p. 77.

248 NCSC, *Rapport semestriel 2021/1,* 2021, p. 15 ; SRC, *La sécurité de la Suisse,* 2022, p. 75 s. ; CSIS/MCAFEE, *Economic Impact of Cybercrime – No Slowing Down,* 2018, p. 12 s. ; SKOPIK/SETTANNI/FIEDLER, p. 155 ; TEICHMANN/GERBER, *La qualification pénale des attaques DDoS en droit suisse,* 2021, N 1. Il arrive que les acteurs malveillants bénéficient, par le biais d'espionnage notamment, d'accès aux informations leur permettant d'améliorer leurs outils, cf. BERTHIER, N 5.

première phase dans le déroulement d'une cyberattaque. Les techniques d'ingénierie sociale s'améliorent et les actrices malveillantes redoublent d'efforts en vue de créer des appâts toujours plus crédibles et réalistes afin de piéger la population ou des collaboratrices d'organisations toujours plus informées[249].

3. La coopération

a. Au niveau national

La cybersécurité est une tâche commune aux différents groupes cibles[250] sur le plan national et sur le plan international[251]. La coopération nationale s'entend sur plusieurs niveaux. On l'entend typiquement à un niveau stratégique. Pour qu'une stratégie en matière de sécurité soit efficace, elle doit prendre en compte les besoins de tous les groupes cibles[252]. Par exemple, l'État doit inclure les infrastructures critiques, les milieux économiques, les milieux scientifiques ainsi que la population dans les échanges, recherches et avancées stratégiques comme opérationnelles permettant l'élaboration de la CSN[253]. Les milieux économiques, par exemple, sont particulièrement actifs dans le domaine de la cybersécurité, raison pour laquelle leur participation présente une plus-value. Leur présence est nécessaire à des fins de responsabilisation et de délimitation entre les droits et les obligations de chaque partie. Parmi les milieux scientifiques, le milieu académique doit naturellement aussi être inclus dans la recherche. La population doit également participer, faire l'objet de campagnes de sensibilisation et être en mesure d'accéder à l'information, dès lors que les personnes physiques sont régulièrement les utilisatrices finales à protéger et qu'elles demeurent souvent vulnérables. 123

La collaboration s'entend également sur un plan opérationnel. La gestion de cyberincidents comporte typiquement un aspect collaboratif important, dans la mesure où les personnes confrontées à des cyberincidents coopèrent avec les autorités compétentes et parfois également avec des prestataires externes. La gestion de ce type d'incidents repose sur les nombreux échanges entre les différentes intervenantes[254]. À titre d'exemple, les prestataires de 124

249 NCSC, *Rapport semestriel 2021/2,* 2022, p. 32 ss ; BERTHIER, N 4.

250 Au sujet des différents groupes cibles, cf. *supra* N 70 ss.

251 CF, *CSN,* 2023, p. 12.

252 GCSP, *Guide to Developing a National Cybersecurity Strategy,* 2021, p. 29 ; GHERNAOUTI, *Cybercriminalité,* 2023, p. 212. Pour des listes exemplatives, cf. GCSCC, *Cybersecurity capacity review – Switzerland,* 2020, p. 16 s. ; GLOBAL PARTNERS DIGITAL, *Involving Stakeholders in National Cybersecurity Strategies: A Guide for Policymakers,* 2020, p. 4.

253 CF, *Plan de mise en œuvre de la SNPC 2018-2022,* 2019, p. 6 s. ; WEBER/WILLI, p. 166.

254 Voir notamment ENISA, *Good Practice Guide for Incident Management,* 2010, p. 85 ; GCSCC, *Cybersecurity capacity review – Switzerland,* 2020, p. 32 ; GHERNAOUTI, *Cybercriminalité,* 2023, p. 170 ss.

gestion de cyberincidents ont facilement tendance à coopérer avec le *Computer Emergency Response Team* (CERT) national, avec d'autres équipes analogues ou avec un secteur entier pour traiter au mieux ces événements problématiques, surtout lorsqu'il en va de la protection des infrastructures critiques ou de cyberincidents à large échelle[255].

125 La collaboration intrasectorielle et intersectorielle est primordiale. Pour illustrer ce propos, les partenariats public-privés (PPP) prennent une place toujours plus importante[256]. Les PPP sont des accords, des coopérations ou des collaborations entre des autorités et des organisations privées[257]. La Suisse a en effet pris note du fait que les États ne pouvaient pas assurer seuls la cybersécurité du pays, sur le plan national comme international. L'intégration des actrices privées est devenue l'une des priorités et ces dernières revêtent une importance centrale du fait de la fourniture de produits et services[258]. Les PPP sont cruciaux pour protéger les organisations d'un secteur (prenant directement part ou non aux PPP) et pour répondre à des intérêts mutuels et communs. Par exemple, le secteur public doit être intéressé par la possibilité de créer des synergies, accéder aux informations et autres ressources du secteur privé, ainsi que par la possibilité de mieux comprendre les différents secteurs et industries. En même temps, le secteur privé accède aux informations et aux connaissances de l'administration et influence positivement certaines pratiques. Les PPP permettent de satisfaire des intérêts communs, à l'instar du partage de connaissances, d'expertise et de bonnes pratiques, du souhait d'atteindre un bon niveau de résilience au sein de l'écosystème cyber ou de l'augmentation de la confiance entre les partenaires sur le court comme sur le long terme[259]. Pour que la résolution de cyberincidents puisse porter ses fruits, elle doit être appréhendée dans une perspective pluridisciplinaire. Plusieurs organisations interviennent en effet dans leur sphère de compétence propre, pour régler une partie de la situation. C'est dans cet ordre d'idées qu'un accent doit être mis sur la coopération[260]. En outre, à l'issue d'un processus de gestion d'un cyberincident, il est bénéfique et opportun de partager les informations, à l'interne d'une organisation, comme à l'externe, avec

255 ENISA, *Good Practice Guide for Incident Management*, 2010, p. 85.

256 Voir par exemple dans le secteur bancaire le FS-CSC, qui compte des établissements bancaires comme des autorités telles que la FINMA ou le NCSC, cf. SWISS FINANCIAL SECTOR CBYER SECURITY CENTRE, *We shape the future of cybersecurity*.

257 ENISA, *PPP*, 2017, p. 7.

258 DFAE, *Stratégie de politique extérieure numérique 2021-2024*, 2020, p. 13.

259 ENISA, *PPP*, 2017, p. 11 et 13. Il est toutefois nécessaire que les objectifs des différents PPP soient clairs, GCSP, *Guide to Developing a National Cybersecurity Strategy*, 2021, p. 44.

260 SKOPIK/SETTANNI/FIEDLER, p. 155.

d'autres réseaux de prestataires de gestion de cyberincidents par exemple, afin d'aboutir à un panorama plus complet des cybermenaces[261]. Un exemple suisse typique de PPP est celui de MELANI, qui s'est développée dans le cadre de la SNPC 2018-2022 avec son cercle de clientes fermé et composé d'infrastructures critiques. Ce partenariat, conservé à la suite de l'organisation de la cybersécurité dans la Confédération et mettant en lumière la nécessité d'instaurer des PPP en matière de protection des infrastructures critiques, a eu pour objectif de permettre aux membres de joindre leurs forces, capacités et connaissances pour lutter contre les cyberincidents[262].

b. Au niveau international

La cybersécurité porte sur le cyberespace et est à ce titre impactée par l'absence de frontières imposée par Internet. Partant, les cyberincidents ne se limitent pas toujours à une portée locale ou nationale. Les stratégies, plans d'action et plans de mises en œuvre doivent être conçus dans une perspective transnationale et internationale[263]. Au vu de ce constat, une étroite coopération est à concevoir, que ce soit à un stade stratégique ou à un stade opérationnel, afin de pouvoir cerner au mieux les diverses menaces et protéger au mieux les infrastructures de tout État. La compréhension et la lutte contre les cyberattaques doit être internationale[264]. 126

Cette collaboration ne peut se faire que moyennant le respect des différentes législations et intérêts respectifs de chaque pays. Bien que cette collaboration se heurte à plusieurs défis, politiques, techniques ou juridiques, il convient d'adopter des instruments adéquats pour ces formes étendues de coopération, tant sur le plan international que sur les plans nationaux[265]. 127

261 NIST, *Computer Security Incident Handling Guide,* 2012, p. 47.

262 CF, *Plan de mise en œuvre de la SNPC 2018-2022,* 2019, p. 39 s. Sur les PPP et plus particulièrement les plateformes d'échanges d'informations, cf. *infra* N 336 ss. Il est important d'établir de tels partenariats dans ce contexte, dans la mesure où de nombreuses infrastructures critiques sont détenues par le secteur privé, cf. ENISA, *Good practices in innovation on cybersecurity under the National Cyber Security Strategies,* 2019, p. 35 ; GCSCC, *Cybersecurity capacity review – Switzerland,* 2020, p. 66. Il existe naturellement une multitude d'autres PPP, à l'instar de *Swiss Cyber Experts,* qui a pour but l'analyse de cyberattaques pour contribuer à la cybersécurité en Suisse. Pour des exemples étrangers, cf. ENISA, *PPP,* 2017, p. 14 ss.

263 FF 2017 2765, p. 2873 ; CF, *SNPC 2018-2022,* p. 50, 61 ss ; DSOUZA, p. 205 ; SKOPIK/SETTANNI/FIEDLER, p. 157.

264 Sur les mesures prévues en Suisse pour optimiser la collaboration du pays sur le plan international, voir CF, *SNPC 2018-2022,* p. 61 ss ; GCSCC, *Cybersecurity capacity review – Switzerland,* 2020, p. 25.

265 À titre d'exemples pour les problèmes juridiques, l'on peut citer les paradis digitaux ou encore le manque d'harmonisation entre les lois ou les pouvoirs d'investigation, cf. DSOUZA, p. 205 s. ; GHERNAOUTI, *Cybercriminalité,* 2023, p. 21.

Cette coopération doit être illustrée par des mesures stratégiques, par des conventions comme par des réseaux de coopération pratiques[266]. L'échange d'informations, l'entraide judiciaire et l'assistance administrative permettent d'avancer, d'identifier plus rapidement des cybermenaces (dont par exemple l'utilisation de logiciels malicieux ou *malwares*)[267], de démanteler des groupes criminels[268], d'accélérer et de préciser la prise de décision et l'implémentation de mesures préventives, détectives et réactives.

4. La subsidiarité de l'intervention étatique

128 Alors que le fédéralisme implique une subsidiarité de l'intervention de la Confédération au profit des cantons et des communes (art. 5*a* de la Constitution fédérale, Cst.), la non-intervention de l'État dans l'activité privée doit être appréciée à la lumière de l'art. 6 Cst., selon lequel chaque personne est responsable de contribuer selon ses forces à l'accomplissement des tâches de l'État et de la société. L'art. 6 Cst. pose le principe de la responsabilité individuelle et traduit l'idée de subsidiarité de l'intervention étatique. Il implique donc que, de manière générale, l'État n'intervienne que de manière subsidiaire pour aider les particuliers[269]. De ce principe découlent des conséquences tant réglementaires que pratiques. L'État détient un rôle subsidiaire et partenarial, ce qui implique une intervention uniquement lorsque les actrices privées ne peuvent pas résoudre elles-mêmes les problèmes ou que la société est gravement menacée. Dans ce cas, l'État peut prendre des mesures de réglementation, d'incitation ou de soutien[270].

129 Ainsi, l'État n'intervient en pratique que pour apporter un soutien lorsque les entreprises et organisations directement concernées et compétentes ne

266 Pour des exemples stratégiques et conventionnels, cf. notamment CF, *Plan de mise en œuvre de la SNPC 2018-2022*, 2019, p. 61 ss ; GCSCC, *Cybersecurity capacity review – Switzerland*, 2020, p. 63. Au sujet de la coopération pratique entre équipes de gestion de cyberincidents ou autres autorités, voir les exemples de FIRST ou EGC (auxquels GovCERT, la CERT nationale et gouvernementale suisse, est affiliée) ; ENISA, *Good Practice Guide for Incident Management*, 2010, p. 84 ss ; GCSP, *Guide to Developing a National Cybersecurity Strategy*, 2021, p. 39 et 47 ss.

267 Un logiciel malveillant ou un *malware* est un programme ou une portion de programme insérée dans un autre programme avec l'intention de modifier son comportement original, en principe pour effectuer une activité malveillante. Ces logiciels peuvent être divisés en plusieurs catégories, dont font notamment partie les virus, vers ou encore les chevaux de Troie *(Trojan horses)*, cf. ISO/IEC 27035-1 : 2016, p. 17.

268 Voir à titre exemplatif le démantèlement d'EMOTET par Europol, Eurojust et d'autres autorités nationales, cf. EUROPOL, *World's most dangerous malware EMOTET disrupted through global action*.

269 CR Cst.-CHATTON, art. 6 N 2 et 20. Au sujet des controverses quant à son caractère normatif, cf. CR Cst.-CHATTON, art. 6 N 16 s.

270 CF, *CSN*, 2023, p. 12 ; BSK BV-BIAGGINI, art. 5*a* N 19.

parviennent pas à assurer leur protection[271]. En d'autres termes, chaque organisation est tenue d'assurer sa propre sécurité.

Dans le cadre de la gestion de cyberincidents, tant les autorités étatiques 130
que des intervenantes privées disposent de compétences et fournissent des prestations. L'autorité principale pour la cybersécurité est l'OFCS, qui exploite son équipe d'intervention informatique GovCERT. L'OFCS et GovCERT proposent notamment, conjointement, une assistance aux infrastructures critiques dans la gestion d'incidents et sont susceptibles d'accomplir des prestations proches de celles offertes par les prestataires de gestion de cyberincidents[272]. Partant, il est nécessaire de s'assurer que la liberté économique et la libre concurrence sont assurées (art. 94 al. 1 Cst.).

Nous verrons par la suite comment le principe de subsidiarité s'ap- 131
plique[273]. Celui-ci implique des réserves pour la Confédération en lien avec les compétences législatives des cantons. Des conséquences sont également entraînées par l'interaction entre les compétences réglementaires de la Confédération et celles des secteurs potentiellement autoréglementés. Nous verrons également comment se joue l'interaction entre l'intervention de l'État et des autres prestataires de gestion de cyberincidents.

B. Les enjeux concrets

1. Les coûts

La cybersécurité représente un investissement certain pour les groupes cibles, 132
qui doit être anticipé dans un budget influençant la prise de décision. Pour établir ce budget, il faut prendre en compte les mesures légales, techniques et organisationnelles, ainsi que le renforcement des capacités et la coopération[274].

Il est également important de tenir compte du coût engendré par un cyber- 133
incident[275]. Lorsqu'il en va de cyberattaques, la cybercriminalité engendre un coût certain pour la société, pour les États ainsi que pour les victimes

271 CF, *CSN*, 2023, p. 12 ; OFPP, *Protection de la population 27*, 2017, p. 15.

272 Sur l'OFCS, GovCERT et leurs compétences, cf. *infra* N 212 ss, 225 ss et 703 ss.

273 Cf. *infra* N 1151 s.

274 Voir notamment CSIS/MCAFEE, *Economic Impact of Cybercrime – No Slowing Down*, 2018, p. 7.

275 *Industrial Business Machines Corporation* (IBM) avait estimé que le coût moyen total d'un incident était passé de $ 3.87 millions à $ 4.24 millions pour les différentes organisations entre 2020 et 2021, combinant les informations de 537 organisations à travers 17 pays et régions et compte tenu que, naturellement, le coût est souvent inférieur lorsque l'organisation dispose de bonnes mesures de sécurité, cf. IBM, *Cost of a Data Breach Report 2021*, 2021, p. 4 et 11.

de cyberattaques[276]. Selon le Département fédéral des affaires étrangères (DFAE), les cyberattaques avaient déjà causé, en 2018, des dommages dépassant 45 milliards de dollars à l'échelle mondiale[277]. Un autre rapport reprend une hypothèse selon laquelle le coût de la cybercriminalité pourrait s'élever à 10,5 mille milliards de dollars d'ici 2025[278]. La croissance de ces coûts pourrait être due, entre autres, à l'évolution rapide des outils et techniques technologiques, à l'augmentation d'utilisatrices d'Internet ou encore à la facilitation par le biais des TIC de commettre des infractions[279].

134 Les éléments faisant partie de ces montants sont divers. Ils peuvent provenir tout d'abord des pertes liées directement à des infractions à caractère économique. Ils découlent également des coûts liés à la sécurité, aux assurances, aux mesures réactives ainsi qu'aux paiements éventuels de rançon en cas de rançongiciels *(ransomwares),* englobant finalement aussi d'autres dommages[280]. La cybersécurité permet de lutter contre la cybercriminalité et d'en diminuer les conséquences financières.

135 Les cyberincidents peuvent conduire à d'autres dommages plus difficilement chiffrables. La divulgation de données personnelles concernant des personnes souffrant de maladies à ce jour stigmatisées peut entraîner des atteintes réputationnelles aux personnes concernées à qui l'on retire le pouvoir de décider d'en informer ou non leur entourage ou qui subissent, de manière plus générale, des dommages psychologiques[281]. En outre, certaines cyberattaques peuvent léser la confiance accordée par la population aux autorités, comme cela a été le cas lors de la découverte du cyberincident en Suisse causée par une tentative d'implémentation du vote électronique[282]. Même si ces dommages sont difficilement chiffrables en tant que tels, il convient d'en tenir compte dans les mesures de sécurité à implémenter.

276 Voir par exemple les statistiques pour les coûts des cyberattaques supportés par les entreprises anglaises : *Average annualized costs of cyber attacks for companies in the United Kingdom (UK) in 2015, by industry sector.*

277 CSIS/MCAFEE, *Economic Impact of Cybercrime – No Slowing Down*, 2018, p. 6 ; DFAE, *Stratégie de politique extérieure numérique 2021-2024*, 2020, p. 12, citant OTA, *2018 Cyber Incident & Breach Trends Report*, 2019, p. 7.

278 MICROSOFT, *Microsoft Digital Defense Report*, 2023, p. 100 et référence citée.

279 CSIS/MCAFEE, *Economic Impact of Cybercrime – No Slowing Down*, 2018, p. 4.

280 CSIS/MCAFEE, *Economic Impact of Cybercrime – No Slowing Down*, 2018, p. 6.

281 Voir par exemple ICO, Monetary Penalty Notice contre HIV Scotland, 18 octobre 2021 ; pour un commentaire de la décision, cf. MEYER Pauline, *Divulgation d'adresse électroniques : l'association HIV Scotland et la nécessité de sécuriser les courriels de masse*. Au sujet des dommages psychologiques résultant de cyberincidents, cf. KILOVATY, p. 14 s.

282 Egovernment, *Stratégie suisse de cyberadministration 2020-2023*, 2019, p. 5 ; CC-DRIVER, *The Real Cost of Cybercrime and Cyberattacks* ; WUTHRICH Bernard, *La « faille considérable » du vote électronique*.

Le coût de la cybersécurité constitue régulièrement un frein pour les organisations. Il est attendu que chacune d'entre elles effectue un calcul relatif au coût de la cybersécurité pour sa structure. Les organisations (dont une importante majorité utilise les TIC) doivent comprendre que la cybersécurité ne saurait être facultative et que toute infrastructure informatique est susceptible de faire l'objet d'un cyberincident. Par conséquent, un budget suffisant doit être alloué à cette fin[283]. 136

Dans la mesure où les cyberincidents ne peuvent pas être totalement empêchés, les plans d'action, les processus de cybersécurité et les mesures de réaction aux cyberincidents entraînent des coûts à prendre en considération[284]. Les personnes intervenant dans la gestion de cyberincidents doivent bénéficier des ressources suffisantes pour remplir leurs fonctions[285]. Pour une organisation, le coût engendré pour l'engagement d'une prestataire de gestion de cyberincidents dépend de la nature et de la structure de cette dernière ainsi que d'autres facteurs, à l'instar de coûts opérationnels ou relatifs au nombre de personnes employées (qui doivent être appropriés par rapport aux besoins et à la taille de l'organisation)[286]. La création d'un service spécialisé au sein d'une organisation n'entraîne probablement pas les mêmes coûts que l'externalisation de ces prestations[287]. Finalement, chaque cyberincident est susceptible d'entraîner par la suite des coûts spécifiques[288]. 137

2. La chaîne d'approvisionnement

La chaîne d'approvisionnement doit garantir la sécurité des produits, des prestations et des systèmes TIC tout au long de leur cycle de vie. Chaque étape d'une chaîne d'approvisionnement est vulnérable. C'est pourquoi il faut tenir compte des intervenantes tout au long de la chaîne, de l'achat des matières 138

283 SARRAZIN Claude, *Cybersécurité : Misez sur la prévention !,* Gestion HEC Montréal, vol. 44, nº 3, p. 81 s. Pour des exemples de modèles, basés sur le cadre NIST prenant en compte les coûts (et bénéfices) en matière de cybersécurité, cf. notamment GORDON Lawrence A./LOEB Martin P./ZHOU Lei, *Integrating cost-benefit analysis into the NIST Cybersecurity Framework via the Gordon-Loeb Model,* Journal of Cybersecurity 2020, p. 1 ss ; RADZIWILL Nicole/BERNTON Morgan, *Cybersecurity Cost of Quality : Managing the Cybersecurity Risk Management,* Software Quality Professional, vol. 19, N 3, septembre 2017.

284 Qui dépendront de plusieurs éléments, comme le soulèvent BAUER/VAN EETEN, p. 709 s.

285 Il en va de la sorte pour les organisations privées mais également pour les prestataires de gestion de cyberincidents étatiques, MORGUS et al., *National CSIRT and Their Role in Computer Security Incident Response,* 2015, p. 11.

286 KILLCRECE et al., *State of Practice of CSIRT,* 2003, p. 54 et 71.

287 NIST, *Computer Security Incident Handling Guide,* 2012, p. 15.

288 À ce sujet, KILLCRECE et al., *State of Practice of CSIRT,* 2003, p. 55 ss.

premières à la livraison des produits finis à la consommatrice. Chaque intervenante doit être consciente de sa place au sein de la chaîne de développement face à une potentielle attaque[289]. Cette chaîne de valeur commune mérite une protection dans la mesure où elle peut constituer un levier intéressant pour des attaquantes. Ces dernières peuvent agir de manière ciblée, engendrer des dommages collatéraux sur d'autres aspects de la chaîne ou attaquer une cible par des rebonds et des relais[290].

139 Certains mécanismes existent pour assurer la sécurité de la chaîne d'approvisionnement, principalement au sein de la Confédération et pour certains produits. Les produits cryptographiques[291] acquis et exploités par la Confédération sont essentiellement achetés par l'Office fédéral de l'armement (armasuisse), qui est soutenu par le service de cryptologie de la Base d'aide au commandement (BAC) de l'armée. Les autorités compétentes effectuent des contrôles cryptologiques approfondis, pendant l'acquisition ou durant les changements de systèmes (par exemple après une mise à jour du logiciel) tout au long du cycle de vie du système[292].

3. Mieux vaut prévenir que guérir

140 La cybersécurité doit être comprise comme un ensemble de processus stratégiques, dans le sens où chaque organisation doit disposer d'une stratégie établie et évolutive prévoyant les différents processus de cybersécurité[293]. Il n'est pas suffisant de se limiter à des mesures concrètes lors de la confrontation à des cyberincidents spécifiques, mais il est nécessaire d'établir des stratégies, de déterminer à l'avance les risques, d'implémenter des règles, des plans d'action, des procédures et des mesures en prévention afin de protéger au mieux les systèmes informatiques et les informations traitées par le biais de

289 BOYES, p. 29 s.

290 SALAMON, p. 69. La chaîne d'approvisionnement est donc toujours plus intéressante pour les cyberdélinquantes, cf. OFCS, *Rapport semestriel 2023/II*, 2024, p. 27.

291 Ces produits servent à protéger les informations en termes de confidentialité, d'intégrité, d'authenticité ou d'obligation ; en font notamment partie les appareils ou logiciels de chiffrement, CF, *Rapport « Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense »*, 2021, p. 19.

292 CF, *Rapport « Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense »*, 2021, p. 19. L'on pourrait réfléchir à de tels processus pour l'acquisition et l'exploitation par d'autres infrastructures critiques, notamment privées, afin de garantir la sécurité et la maîtrise de la chaîne d'approvisionnement de certains systèmes. Un tel procédé requerrait une analyse approfondie et détaillée qui dépasse les limites de la présente étude.

293 Voir par exemple ENISA, *How to set up CSIRT and SOC*, 2020, p. 23 ss ; NIST, *Public Draft : The NIST Cybersecurity Framework 2.0*, 2023, p. 5 ; NIST, *The NIST Cybersecurity Framework (CSF) 2.0*, 2024, p. 16 ; BORBOËN Yan / KÜDERLI Urs / NEHER Lorenz, *Les cyber-risques sont un enjeu au plus haut niveau de l'entreprise !*.

ceux-ci. Des plans d'action et des processus en cas de cyberincidents ou de crises cyber doivent en outre être testés et il est important de bénéficier en amont de méthodes de détection, de réaction et de prises de décision en cas de cyberincidents pour pouvoir gérer ces derniers de manière efficace et efficiente[294]. Penser la cybersécurité dans la planification, la préparation et la prévention, permet d'augmenter la sécurité globale des organisations, de réduire les risques et les dommages potentiels sur les activités, de réagir d'une façon plus appropriée en cas de cyberincidents ou encore de faciliter des investigations subséquentes[295].

C'est un défi auquel doit répondre chaque organisation, compte tenu de 141
ses risques et de ses besoins de protection. Concrètement, des mesures techniques et organisationnelles doivent être considérées pour une prévention adéquate[296]. Les approches fondées sur les risques impliquent des analyses de risques et des besoins ainsi que la mise en place de nombreuses autres mesures organisationnelles et techniques pour prévenir au maximum les cyberincidents. Des mesures comme la formation sont typiquement centrales, car un manque de connaissances est encore aujourd'hui à déplorer et les individus occupent un rôle central pour la mise en place de mesures efficaces en matière de cybersécurité[297].

4. Une question de confiance

La question de la confiance doit se poser à tous les échelons, surtout lorsque 142
l'État détient un rôle. D'une part, les milieux économiques et les infrastructures critiques doivent être entendues et pouvoir faire confiance aux autorités, lors des relations avec ces dernières ou lors de l'élaboration de réglementations[298]. D'autre part, il est nécessaire pour l'État de bénéficier de la confiance de la population. Celle-ci doit être informée sur les processus informatiques que l'État compte implémenter, typiquement lorsque ces derniers permettent des traitements de données de citoyennes. La transparence permet aux administrées d'avoir connaissance de leurs droits et de les exercer, à commencer par leur droit à la sphère privée[299].

294 ISO/IEC 27035-1 : 2016, p. 5.

295 ISO/IEC 27035-1 : 2016, p. 5 s.

296 Voir par exemple FF 2017 2765, p. 2791 et 2830.

297 Voir à ce sujet l'interview de Dr Edward Humphreys, animateur d'un groupe de travail ISO, NADEN Clare, *The cybersecurity skills gap, Why education is our best weapon against cybercrime*.

298 ENISA, *NCSS Good Practice Guide,* 2016, p. 41.

299 Pour des informations supplémentaires à ce sujet, voir notamment, en lien avec les services d'*e-government,* GCSCC, *Cybersecurity capacity review – Switzerland,* 2020, p. 38 s. ; GCSP, *Guide to Developing a National Cybersecurity Strategy,* 2021, p. 31.

143 Par ailleurs et comme déjà soulevé[300], la collaboration est centrale lorsqu'il en va de la gestion concrète de cyberincidents. Les entités ou services compétents à l'instar des prestataires de gestion de cyberincidents doivent, pour assurer un échange d'information fiable et utile, bénéficier de la confiance des personnes internes aux organisations comme de la confiance des partenaires externes. Cette confiance est primordiale pour les prestataires de gestion de cyberincidents qui se trouvent au centre des questions de cybersécurité et qui collaborent étroitement avec de nombreuses interlocutrices, dont leurs collaboratrices, les services analogues suisses ou étrangers ou encore les autorités[301]. Les prestataires de gestion de cyberincidents nécessitent cette confiance bilatérale ou multilatérale à un niveau local, sectoriel ou national. La confiance est en outre bi- voire multidirectionnelle[302]. Les prestataires de gestion de cyberincidents sont tenues de se montrer transparentes sur la manière de fonctionner et doivent, avec les autres organisations disposant de compétences analogues, faire des efforts continus. La confiance se construit souvent sur la base de longues relations informelles prônant des échanges qualitatifs et réciproques d'informations, qui sont habituellement formalisées en pratique par des accords juridiques comme les accords de confidentialité[303]. L'adhésion à des associations et l'organisation d'événements peut également améliorer la confiance dans le domaine[304].

5. La cybersécurité et l'éthique

144 L'État doit s'engager à garantir le respect des valeurs fondamentales, des droits humains et de la dignité humaine en renforçant la prise de conscience quant à l'importance que revêt l'autodétermination informationnelle[305]. Les questions que la cybersécurité pose en termes d'éthique et des valeurs[306] fondamentales la composant ne peuvent pas être traitées au sein de la présente

300 Cf. *supra* N 123 ss.

301 ISO/IEC 27035-2 : 2016, p. 13 et 20.

302 KILLCRECE et al., *Organisational Models for CSIRT,* 2003, p. 125. Par exemple, il sera parfois techniquement possible pour une prestataire de gestion de cyberincidents d'accéder à des données auxquelles la cliente ne souhaite pas lui attribuer d'accès et la relation de confiance entre les deux protagonistes aura pour conséquence que la cliente pourra se fier à sa prestataire qui n'y accédera pas sans son consentement.

303 ENISA, *Baseline Capabilities of National/Governmental CERT, Part 2,* 2010, p. 40 ; CFCE, *GFCE Global Good Practices – National Computer Security Incident Response Teams (CSIRT),* 2017, p. 14 ; MORGUS et al., *CSIRT Basics for Policy-Makers*, 2015, p. 19 ss.

304 GFCE, *GFCE Global Good Practices – National Computer Security Incident Response Teams (CSIRT),* 2017, p. 15.

305 GROUPE D'EXPERTS « AVENIR DU TRAITEMENT ET DE LA SÉCURITÉ DES DONNÉES », *Rapport du groupe d'experts concernant le traitement et la sécurité des données,* 2018, p. 6 s.

306 Au sujet de la notion de valeur en éthique, voir notamment VAN DE POEL, p. 46 ss.

étude, mais il convient tout de même de souligner l'importance de ces valeurs et leur lien avec les droits fondamentaux dans le droit relatif à la cybersécurité. Les normes éthiques ont fait leur apparition au fil de l'évolution de la société, en formant la base du vivre ensemble[307]. Les valeurs doivent guider l'élaboration des lois, leur application et les comportements des différentes actrices de l'écosystème.

Des valeurs fondamentales, dont la protection de la vie privée, l'égalité de traitement, l'autodétermination ou encore la solidarité, sont touchées par la cybersécurité. L'une des expressions des règles d'éthique réside donc dans la reconnaissance de droits et libertés fondamentales, qui constituent un cadre de référence éthique répandu et reconnu au niveau international. Les cybermenaces soulèvent des questions éthiques dans la mesure où toujours plus de domaines de la vie et de la société sont vulnérables aux cyberattaques et cyberincidents. Cependant, les valeurs fondamentales ne doivent pas être atteintes pour des motifs liés à la cybersécurité[308]. La cybersécurité doit au contraire comprendre les valeurs éthiques. Ces dernières doivent faire l'objet d'une réflexion de la part de chaque organisation et elles doivent être intégrées dans des plans pour pouvoir être assurées au mieux durant la gestion de cyberincidents[309]. 145

Alors que certaines mesures, à l'instar de l'authentification, peuvent servir à protéger par exemple la sphère privée, d'autres mesures peuvent être plus intrusives et soulever des questions de respect des valeurs éthiques, se recoupant parfois avec les droits fondamentaux et la protection de la personnalité[310]. Par exemple, le *web monitoring* est une mesure par laquelle l'on surveille la disponibilité d'un site Internet[311]. La surveillance peut également porter sur les accès de personnes à certains systèmes informatiques. Par de telles mesures de surveillance, la protection de la sphère privée, consacrée à l'art. 13 Cst., peut être compromise[312]. En outre, des suites peuvent être données à 146

307 GROUPE D'EXPERTS « AVENIR DU TRAITEMENT ET DE LA SÉCURITÉ DES DONNÉES », *Rapport du groupe d'experts concernant le traitement et la sécurité des données,* 2018, p. 175.

308 GROUPE D'EXPERTS « AVENIR DU TRAITEMENT ET DE LA SÉCURITÉ DES DONNÉES », *Rapport du groupe d'experts concernant le traitement et la sécurité des données,* 2018, p. 175 ss.

309 CHRISTEN/KNIEPS, p. 3 ss.

310 Et les défis éthiques doivent par ailleurs être anticipés dans la mesure du possible, cf. CHRISTEN/KNIEPS, en particulier p. 5 s.

311 Au sujet de différents cas de figure et différentes relations entre sécurité et sphère privée, cf. VAN DE POEL, p. 62. Concernant les questions de surveillance massive, d'équité et démocratie, voir notamment VAN DE POEL, p. 67.

312 Pour d'autres exemples, voir MÉTILLE, *Mesures techniques de surveillance et respect des droits fondamentaux – en particulier dans le cadre de l'instruction pénale et du renseignement,* 2011, p. 104 ss.

l'utilisation de cette mesure dont des blocages, de la censure ou encore du profilage[313]. La liberté d'expression, la protection de la sphère privée ou l'égalité de traitement peuvent potentiellement être restreintes et doivent être mises en balance avec le but poursuivi par la mesure concrète de cybersécurité[314]. Il est important de réfléchir en amont, tant dans le secteur privé que dans le secteur public, aux valeurs susceptibles d'être compromises par la mise en œuvre de mesures en adoptant par exemple des codes de conduite ou d'éthique. Il faut aussi systématiquement pondérer les intérêts en présence afin de s'assurer du respect des droits fondamentaux qui ne peuvent être restreints que moyennant le respect des conditions constitutionnelles et légales s'appliquant[315].

6. Les évolutions technologiques : vecteurs de progrès comme de risques

a. Quelques évolutions technologiques

147 De nombreux nouveaux outils sont aujourd'hui développés et exploités au service de la sécurité, pour mener des cyberattaques ou pour d'autres activités quotidiennes licites. De nombreuses organisations vivent aujourd'hui avec l'Internet industriel des objets (IIdO), avec la collecte de mégadonnées ou de données massives *(big data),* avec des systèmes d'intelligence artificielle (IA) ou avec l'utilisation de solutions en nuage *(cloud computing)*[316].

b. Concrètement

(i) L'intelligence artificielle

148 L'IA n'est pas définie de façon univoque. Elle implique un croisement des sciences, théories et techniques en vue de permettre à une machine ou à un système d'imiter les capacités cognitives d'un être humain ; il s'agit davantage d'une technologie que d'une intelligence à proprement dite[317]. En Suisse, le réseau suisse de compétences en intelligence artificielle (CNAI) définit l'intelligence artificielle comme « la création ou la programmation d'un ordinateur

313 Art. 5 litt. f LPD ; CHRISTEN/LOI, p. 76.

314 CHRISTEN/LOI, p. 76 ss ; VAN DE POEL, p. 61.

315 C'est par ailleurs pour assurer le respect des droits fondamentaux que l'État devra toujours garder en tête l'art. 36 Cst., la LPD, la LSCPT et les autres instruments assurant une protection aux personnes ciblées par des interventions étatiques susceptibles de leur causer du tort.

316 OTA, *IoT Trust by Design*, 2018, p. 1 ; BHATTACHARJEE, p. 8 ; TSCHIDER, p. 95. Pour de plus amples considérations sur les aspects réglementaires en lien avec la cybersécurité et ces évolutions, cf. *infra* N 1367 ss.

317 Voir dans le même sens CNAI, *Terminologie*, 2021, p. 7 ; art. 3 par. 1 AI-Act ; CONSEIL DE L'EUROPE, *L'IA, c'est quoi ?*. Voir aussi pour des généralités *supra* N 147 ss.

de telle sorte qu'il soit capable d'exécuter des fonctions qui reposent normalement sur des facultés humaines ou biologiques, comme la perception visuelle, la reconnaissance vocale, la traduction, la traduction visuelle et l'aptitude à jouer »[318]. Outre une multitude de questions éthiques, ce sont les possibilités de décisions basées sur l'IA par les systèmes IA[319] et leurs techniques d'apprentissage automatique[320] qui soulèvent principalement des questions juridiques.

Dans le contexte de la cybersécurité auprès des infrastructures critiques, 149
l'IA est à l'origine de risques particuliers dans la mesure où elle fait aujourd'hui partie du quotidien d'une majorité d'organisations. Elle est régulièrement employée dans des produits utilisés par des infrastructures critiques comme l'IIdO) par le biais des instruments de mesure intelligents *(smart grids* ou *meters)* ou encore des IDPS.

(ii) L'Internet des objets

L'Internet des objets (IdO) désigne les technologies permettant d'interconnec- 150
ter des objets physiques et virtuels et de les faire collaborer en recourant à des technologies de l'information et de la communication (TIC)[321]. L'IdO et l'IIdO permettent par exemple l'interconnectivité de composants physiques (à l'instar des composants mécaniques ou encore des boîtiers), de composants intelligents (comme les capteurs, logiciels et systèmes d'exploitation) et de composants de connectivité (dont les ports, ou les ports permettant la réception

318 CNAI, *Terminologie,* 2021, p. 7. L'IA peut être définie comme la « recherche de moyens susceptibles de doter les systèmes informatiques de capacités intellectuelles comparables à celles des êtres humains », incluant en principe l'apprentissage automatique et le traitement automatique du langage naturel, cf. BENSOUSSAN/BENSOUSSAN, p. 3 et référence citée. En d'autres termes et plus simplement, il est possible de la définir comme l'apprentissage automatique informatisé, dont le modèle est ensuite intégré à des systèmes informatiques, cf. CF, *Rapport « La politique de sécurité de la Suisse »,* 2021, p. 5. Pour d'autres éléments de définitions, voir JACCARD, p. 134 ss.

319 « Un système IA est un système automatique capable d'établir des prévisions, d'émettre des recommandations ou de prendre des décisions en relation avec des problèmes clairement définis par l'être humain, et qui, ce faisant, exerce une influence sur des environnements réels ou virtuels », CNAI, *Terminologie*, 2021, p. 7.

320 CNAI, *Terminologie*, 2021, p. 8 ss.

321 CNAI, *Terminologie*, 2021, p. 11. Il est défini par l'Union internationale des télécommunications (UIT) comme l'» infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution », cf. UIT-T, Y.2060 (06/2012), Présentation générale de l'Internet des objets, p. 1. Le CNAI le définit comme englobant « les technologies d'une infrastructure globale de la société de l'information, qui permet d'interconnecter des objets physiques et virtuels et de les faire collaborer en recourant à des technologies de l'information et de la communication », CNAI, *Terminologie,* 2021, p. 11.

ou transmission d'informations avec ou sans fil), qui leur permettent d'écouter (voire surveiller) leur environnement ainsi qu'interagir avec les humains, d'autres appareils ou des personnes tierces[322].

151 L'IdO est important, dans la mesure où la mise en réseau des objets progresse très rapidement. Dans les secteurs critiques plus spécifiquement, la question concerne les systèmes de contrôle industriel gérés, surveillés et interconnectés grâce à l'IdO[323]. Au sein de certains secteurs critiques, l'IdO est concrétisé typiquement par le développement et l'exploitation de systèmes de contrôle industriel. L'IIdO, qui consiste en la transformation des opérations d'une entreprise par l'ajout de connectivité aux systèmes ou processus combinant typiquement la technologie informatique (IT), la technologie opérationnelle (OT), la robotique, la collecte de données massives *(big data),* l'IA, parfois l'utilisation du *cloud computing* et les processus de production[324].

152 Les questions réglementaires principales liées à l'IdO ont trait à la sécurité dans la conception et la fabrication de tels objets ainsi qu'à la conservation d'un niveau adéquat de sécurité une fois les objets utilisés par les destinataires finales. En effet, la sécurité de tels appareils est encore régulièrement négligée durant l'entier de leur cycle de vie[325].

(iii) L'informatique en nuage

153 L'informatique en nuage ou le *cloud computing* « désigne la mise à disposition de ressources informatiques (serveurs, capacité mémoire, base de données, éléments de réseaux, logiciels, fonctions d'analyse, fonctions intelligentes, etc.) via Internet »[326]. L'utilisation du *cloud* permet un accès réseau sur demande pratique à des ressources informatiques configurables, mises en commun pour une multitude d'utilisatrices. Les accès aux ressources sont rapides et ne nécessitent pas d'interaction formelle avec la prestataire[327].

154 Bien que cette technologie permette le développement et l'utilisation de nouvelles applications technologiques susceptibles de renforcer la cybersécurité, elle est aussi à l'origine de nouveaux risques[328]. L'utilisation de l'informatique en nuage conduit typiquement à des risques liés à des traitements de données à l'étranger par certains prestataires et, plus largement, à des risques

322 ENISA, *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures,* novembre 2017, p. 18 ss ; KORFF, p. 129 ; TSCHIDER, p. 92 et 94.

323 CF, *CSN,* 2023, p. 7.

324 Cf. *supra* N 147 ss.

325 CF, *CSN,* 2023, p. 7.

326 CNAI, *Terminologie,* 2021, p. 11.

327 JOTTERAND, p. 4.

328 CF, *CSN,* 2023, p. 7.

induits par la position de dominance de certaines actrices sur ce marché avec, simultanément, une forte dépendance des organisations à quelques prestataires[329]. Il y a effectivement, lors de l'utilisation de solutions en nuage, une perte de maîtrise par l'organisation ou la personne traitant initialement des informations par ce biais[330]. La perte de maîtrise n'implique pas *de facto* davantage de risques ; les services infonuagiques sécurisent parfois bien mieux les informations traitées par une organisations faisant appel à leurs services, en comparaison avec cette dernière. La perte de maîtrise liée à l'informatique en nuage entraîne cependant des répercussions sur la cybersécurité, sur la protection au sens plus large des données et des informations ou encore sur le respect d'éventuels secrets.

c. Des sources de progrès et de risques

L'évolution des TIC et des outils existants influence de façon prépondérante 155
les possibilités inhérentes au cyberespace. Comme la majorité des avancées technologiques, l'IdO permet une automatisation pratique par la création de réseaux intelligents et interconnectés capables de faire face à des complexités croissantes. Au-delà des objets du quotidien pour la population, elle permet également une automatisation de nombreux processus industriels, permettant par exemple aux infrastructures, critiques ou non, de surveiller et contrôler les productions par le biais de l'IIdO[331]. En termes de cybersécurité, les outils et moyens traditionnels ne suffisent aujourd'hui plus pour contrer ces cyberattaques et gérer ces cyberincidents toujours plus sophistiqués et pouvant se répandre à large échelle. Pour se protéger efficacement, il est nécessaire d'adapter les outils en exploitant correctement les systèmes d'IA, les mégadonnées et ainsi de suite. Les systèmes d'IA peuvent typiquement permettre de détecter plus rapidement des vulnérabilités ou d'identifier plus aisément des cyberattaques[332].

Au-delà des progrès que permettent ces outils, l'automatisation de tous 156
ces processus augmente et diversifie les risques auxquels sont confrontées les organisations, notamment en permettant une complexification des cyber-

329 CF, *CSN*, 2023, p. 7.

330 Voir à ce sujet le rapport du Comité européen de la protection des données sur l'utilisation par l'administration publique de solutions d'informatique en nuage, CEPD, *Use of could-based services by the public sector,* 17 janvier 2023, p. 10 ss ; MEYER Pauline, *L'administration publique responsable dans l'utilisation de service en nuage*.

331 BERGER/BÜRGER/RÖGLINGER, p. 1.

332 ENISA, *Roadmap on the cooperation between CSIRT and LE,* 2019, p. 38 ; OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »,* 2021, p. 26 s. ; ALANI, p. 86 et 89 ss ; NGAMBEKET Guy, *Smart Objects and Their Privacy Implications, ISACA,* 22 janvier 2021 ; SALAMON, p. 37.

attaques, en se trouvant à l'origine de nouvelles vulnérabilités ou en étendant leur portée (en raison de la décentralisation et de l'interdépendance des différents systèmes et réseaux)[333]. Le risque d'éventuelles interruptions involontaires et autres incidents détient également une nouvelle dimension et l'interconnectivité entre les différentes machines implique que les cyberattaques peuvent se diffuser plus facilement[334]. Une cyberattaque ciblant l'une de ces technologies peut engendrer une atteinte aux données, mais aussi des dommages matériels voire physiques, par exemple si des verrous intelligents viennent à être compromis[335]. Ces technologies peuvent également être utilisées comme des outils, par exemple pour diffuser un logiciel malveillant à plus large échelle ou encore pour procéder à de l'espionnage ou à du sabotage[336].

157 Nous voyons donc que l'utilisation et l'implémentation de l'IdO (et de l'IIdO), de l'IA et des mégadonnées dans la société posent des questions pratiques lorsqu'il en va de la protection contre les cybermenaces. De manière générale, déjà, et simplement dans le cadre de la numérisation, ces questions doivent être accompagnées politiquement et juridiquement, au moyen d'incitations à l'instar des lignes directrices relatives à l'IA dans l'administration. L'État aspire, par ce biais, à placer l'être humain au centre des préoccupations, à mettre en place des conditions propices au bon développement de ces technologies, à assurer notamment la transparence et la sécurité des systèmes et des informations qu'ils permettent de traiter, à clarifier les responsabilités, à encourager la participation active de la Suisse en matière de gouvernance et à impliquer tous les acteurs sur les plans national et international[337]. En matière de protection contre les cybermenaces, il est particulièrement important de disposer d'un arsenal légal permettant la mise en place de mesures utilisant ces techniques et outils contre les attaques basées sur ces mêmes technologies, que ce soit sur le plan de la cybersécurité, de la lutte contre la cybercriminalité ou de la cyberdéfense.

333 FF 2018 491, p. 500 s. ; OFCOM, *Stratégie Suisse numérique*, 2020, p. 11 ; SALAMON, p. 71 ; WEBER/WILLI, p. 130 s.

334 CF, *CSN*, 2023, p. 7 ; OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »*, 2021, p. 26 ; OTA, *2018 Cyber Incident & Breach Trends Report*, 2019, p. 8 ; BERGER/BÜRGER/RÖGLINGER, p. 1.

335 OTA, *IoT Trust by Design*, 2018, p. 1 ; BERGER/BÜRGER/RÖGLINGER, p. 1 et 3. Pour voir un exemple de l'interdépendance entre infrastructures critiques, cf. KASTELIC, p. 11.

336 C. 51 AI-Act ; ENISA, *Roadmap on the cooperation between CSIRT and LE*, 2019, p. 38 ; OFCS, *Rapport semestriel 2023/II*, 2024, p. 18 et 37 ; OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »*, 2021, p. 128 ; SALAMON, p. 37.

337 CF, *« Intelligence artificielle » – lignes directrices pour la Confédération*, 2020, p. 3 ss.

C. Une synthèse

Pour assurer la cybersécurité d'une façon appropriée, il est nécessaire de tenir compte et d'assurer le respect d'une multitude d'enjeux. Tout d'abord et de façon générale, la sécurité des informations traitées par le biais de systèmes informatiques est étroitement recoupée avec la cybersécurité et les mesures de cybersécurité qui doivent par ailleurs permettre d'assurer la sécurité des informations. Ensuite, la cybersécurité s'inscrit dans une demande croissante liée à l'augmentation et à la professionnalisation des cyberattaques, qui implique que des mesures adaptées doivent être prises pour assurer la résilience face à la diversité et la complexité des attaques perpétrées par des personnes ayant des intentions malveillantes. En outre, la collaboration est essentielle, que ce soit sur le plan national ou sur le plan international. Sur le plan national, la collaboration doit se faire sur le plan stratégique impliquant l'intégration des points de vue et des défis de tous les groupes cibles, à savoir des autorités, des infrastructures critiques, des autres entreprises, des milieux scientifiques et de la population. La collaboration doit aussi porter sur l'aspect opérationnel de la cybersécurité, parce qu'une multitude d'organisations et de personnes sont confrontées aux mêmes menaces et que les différents groupes cibles disposent de compétences servant également autrui. Finalement, l'État ne peut pas intervenir comme bon lui semble pour la cybersécurité, mais doit respecter l'autonomie des cantons, l'autonomie sectorielle et la responsabilité propre de chaque personne et de chaque organisation. Ce constat se répercute tant dans ses compétences réglementaires que dans son soutien dans la gestion de cyberincidents. 158

Certains enjeux ont également une portée plus concrète. Premièrement, la cybersécurité engendre un certain coût que les différents groupes cibles doivent budgéter. En effet, les autorités doivent investir dans leur cybersécurité comme pour d'autres initiatives. Les organisations et la population sont aussi tenues d'agir de même s'agissant de leur cybersécurité. Cela étant, ces investissements doivent contribuer à prévenir et réduire les coûts élevés engendrés par la cybercriminalité. Deuxièmement, une attention particulière doit être accordée à l'interconnexion des services, des systèmes et des produits dans le cadre de la chaîne d'approvisionnement. La protection de la chaîne d'approvisionnement doit chercher à garantir la sécurité des produits, des prestations et des systèmes TIC tout au long de leur cycle de vie. Troisièmement, les autorités, organisations et individus doivent prendre conscience de l'importance de la prévention des cyberincidents. Bien que de tels incidents soient inévitables, les mesures de prévention sont cruciales tant pour diminuer la probabilité de faire l'objet de cyberincidents que pour augmenter les 159

moyens permettant de les gérer au mieux lorsqu'ils se réalisent. Quatrièmement, la confiance est au centre de la collaboration pour la cybersécurité. Non seulement la population doit faire confiance à l'État lorsqu'il agit, mais toutes les intervenantes dans la gestion de cyberincidents doivent s'accorder une confiance réciproque pour pouvoir collaborer et échanger en toute sécurité pendant la gestion de cyberincidents. Cinquièmement, certaines mesures de cybersécurité sont susceptibles de porter atteinte à des valeurs éthiques. Les intervenantes dans la gestion de cyberincidents sont tenues de les respecter dans la mesure du possible ; les prestataires de gestion de cyberincidents et les organisations doivent mettre en place des cultures de cybersécurité pour une éthique fondée sur leurs valeurs, en anticipant au mieux les événements dommageables. Sixièmement, de nouvelles technologies continuent à être développées. Elles peuvent servir de surfaces d'attaques ou d'outils pour la lutte contre les incidents. Partant, la cybersécurité doit les prendre en compte et il faut pouvoir exploiter leurs opportunités.

III. Une conclusion au chapitre 1

160 Le chapitre 1 de la présente étude sert à poser les notions de base et les enjeux de la cybersécurité des infrastructures critiques et de la gestion de cyberincidents. Il commence par donner une définition de la cybersécurité plus précise que la définition issue du droit suisse avant janvier 2024 (I.A). Les autres notions clés sont ensuite définies, à l'instar des notions de cyberincident, de cybermenace ou encore d'infrastructure critique (I.B). Un premier aperçu des différentes étapes et mesures de la gestion de cyberincidents est donné (I.C)[338] ; il sert à effectuer une distinction entre les mesures préventives, détectives et réactives et à appréhender quelques mesures complémentaires, telles que la cyberassurance ou des mécanismes d'évaluation.

161 Les enjeux ensuite parcourus sont nombreux. Ils doivent être pris en considération dans la cybersécurité sur le plan stratégique comme sur le plan opérationnel. Certains enjeux sont globaux, comme c'est le cas s'agissant de l'augmentation des cyberattaques ou de la subsidiarité de l'intervention étatique (II.A). D'autres enjeux sont moins abstraits et s'ancrent davantage dans les pratiques concrètes de cybersécurité à l'attention de tous les groupes cibles : les coûts, les mesures à mettre en place, les valeurs que ces mesures doivent respecter ou encore à la confiance nécessaire entre les différentes intervenantes (II.B).

338 Elles seront ensuite approfondies, cf. *infra* N 291 ss.

Maintenant que les fondements relatifs à la cybersécurité et à la gestion de cyberincidents ont été posés, il est important de mettre un accent sur la Suisse et de comprendre comment le pays s'est saisi de ce sujet. 162

Chapitre 2 : le contexte stratégique

Préambule au chapitre 2

La Suisse a pris diverses mesures au fil du temps pour intégrer au mieux les TIC dans l'activité de l'État et de la société, mettre en place un cadre politique ainsi que les législations nécessaires. La transformation numérique étant en marche depuis plusieurs années, divers instruments politiques ont été adoptés afin d'encadrer l'orientation de l'État. 163

Les stratégies, contrairement aux constitutions, lois et ordonnances, n'ont pas de vocation légale. Elles n'imposent pas des droits et des obligations dont la non-conformité est assortie de sanctions, mais fixent un cadre stratégique sur lequel un plan d'action est adopté en vue d'atteindre les objectifs de la stratégie au travers de la mise en place de mesures par une diversité d'intervenantes. Les stratégies nationales sont adoptées en Suisse par le pouvoir exécutif, en principe dans un processus collaboratif impliquant les autorités et les organisations concernées. Elles reflètent une volonté politique et constituent le support ou le cadre guidant l'élaboration d'instruments légaux et d'autres mesures afin de répondre à des objectifs stipulés, souvent dans un délai défini. La notion de stratégie nationale est un concept reconnu internationalement. Elle peut être définie comme un outil poursuivant un objectif d'amélioration de la sécurité et de la résilience des services et infrastructures nationales. Elle permet une approche établissant une série d'objectifs et de priorités nationales à atteindre dans un laps de temps donné. Elle fournit un cadre stratégique pour l'approche de la cybersécurité d'un État[339]. 164

En Suisse, la transformation numérique est matérialisée par la Stratégie Suisse numérique (I.A). Découlant de cette stratégie, la CSN est la stratégie nationale pour la protection de la Suisse contre les cybermenaces (I.B) et elle interagit avec d'autres stratégies (I.C). D'autres outils stratégiques sont en effet complémentaires et entrecroisés avec la CSN, dont la Stratégie PIC (II.A), les stratégies pour la poursuite pénale de la cybercriminalité ou pour la cyberdéfense (II.B), ou encore d'autres stratégies et instruments politiques (II.C). 165

339 ENISA, *National Cyber Security Strategies*, 2012, p. 4.

I. La transformation numérique et les stratégies s'y rapportant

A. La Stratégie Suisse numérique

166 Dans le cadre de sa transformation numérique, la Suisse a adopté plusieurs stratégies nationales pour mobiliser les compétences en la matière ainsi que pour assurer un passage au numérique transparent, sûr et de confiance. La transformation numérique a une portée générale ; elle englobe d'autres considérations que la cybersécurité, à l'instar de la cyberadministration ou du contrôle de la gestion informatique. La cybersécurité s'impose comme une pratique transversale, applicable partout où le numérique est utilisé. La Stratégie Suisse numérique, principale stratégie pour la transformation numérique de la Confédération, indique comment la Suisse doit tirer le meilleur parti possible des opportunités de ce processus. Elle compte la sécurité comme l'un de ses domaines d'application[340].

167 La Stratégie Suisse numérique, revue en 2023 est la stratégie faitière pour les questions numériques en Suisse. Elle arrête les lignes directrices pour la transformation numérique de la Suisse (art. 15 de l'Ordonnance sur la coordination de la transformation numérique et la gouvernance de l'informatique dans l'administration fédérale, OTNI)[341]. Outre ces lignes directrices, la stratégie invite toute la société à concevoir des projets de mise en œuvre et des thèmes transversaux (ce qui ressort également de l'art. 15 OTNI). Les ressources doivent être mobilisées auprès des autorités, fédérales, cantonales ou encore communales, mais également auprès du secteur privé, du monde scientifique et de la société civile[342]. Elle vise une implémentation de la technologie égalitaire facilitant la vie quotidienne.

168 Concrètement, la stratégie de 2023 est structurée en cinq dimensions, soit la formation et les compétences, la sécurité et la confiance, les conditions-cadres, l'infrastructure ainsi que les services numériques des autorités. Particulièrement importante dans le contexte de la cybersécurité, la dimension « sécurité et confiance » vise à ce que la population en Suisse puisse évoluer en sécurité dans le monde numérique. Dans la dimension « infrastructure », les autorités doivent encourager et exploiter une infrastructure fiable et résiliente, tant sur le plan physique que numérique[343].

340 CF, *CSN*, 2023, p. 8.

341 ChF, *Stratégie Suisse numérique 2023*, 2022, p. 1.

342 OFCOM, *Stratégie Suisse numérique*, 2020, p. 3.

343 ChF, *Stratégie Suisse numérique 2023*, 2022, p. 2 s.

Malgré son caractère très général, la stratégie est accompagnée par un plan d'action fixant des objectifs à atteindre dans le cadre de la transformation numérique[344]. L'on y trouve des objectifs de sécurité, dans la mesure où il est nécessaire que le développement de solutions innovantes et de standardisation permette aux citoyennes d'être protégées contre l'utilisation abusive du numérique[345]. À ce titre, la disponibilité, l'intégrité, la confidentialité et la traçabilité des informations doivent être garanties. Alors que la numérisation est à l'origine de nombreux risques, elle peut également contribuer à gérer plus efficacement et rapidement les incidents et les crises. La résilience et la protection doivent s'étendre, au-delà des infrastructures critiques, à toute la vie publique. Une protection efficace exige une étroite collaboration entre les secteurs et les institutions compétentes. La cybersécurité doit être assurée par toute la société. Elle concerne donc la Confédération, les cantons, les infrastructures critiques, les autres entreprises et la société. Une collaboration est également nécessaire sur le plan international[346]. 169

La stratégie de 2024 poursuit ces efforts en mettant encore davantage l'accent sur la cybersécurité. Celleci fait partie des trois thèmes prioritaires. Elle est placée sous la responsabilité de l'OFCS, des cantons, des hautes écoles et des milieux économiques. C'est afin de répondre aux exigences posées par le cadre de la Stratégie Suisse numérique qu'a été adoptée la CSN[347]. 170

B. La Cyberstratégie nationale

La CSN, adoptée en 2023 par le CF, fait suite à la SNPC 2018-2022. Elle « établit le cadre stratégique régissant la prévention et la détection précoce des cyberrisques, ainsi que la réaction et la résilience en cas de cyberincident » (art. 5 aOPCy). Cette stratégie se rapporte à la Stratégie Suisse numérique et elle est renouvelée tous les quatre à cinq ans. La CSN pose la cybersécurité comme prérequis pour la transformation numérique[348]. Elle poursuit des objectifs de protection efficace de la Suisse contre les cybermenaces et de résilience en cas de cyberincidents[349]. La CSN aborde les cybermenaces auxquelles est 171

344 MONTAVON, p. 27 ; STRATÉGIE SUISSE NUMÉRIQUE, *Plan d'action*.

345 OFCOM, *Stratégie Suisse numérique*, 2020, p. 5, 10. La sécurité a été l'un des fils conducteurs de la stratégie « Suisse numérique », cf. FF 2016 3801, p. 3803 s. pour la Stratégie Suisse numérique de 2016 ; FF 2018 6009, p. 6014 s, 6033 pour celle de 2018.

346 OFCOM, *Stratégie Suisse numérique*, 2020, p. 12.

347 FF 2023 2830, p. 5.

348 CF, *CSN*, 2023, p. 4.

349 CF, *Plan de mise en œuvre de la SNPC 2018-2022*, 2019, p. 4.

confrontée la Suisse, inclut la diversité des mesures à entreprendre pour garantir la cybersécurité et précise les compétences des différentes actrices. C'est en son sein qu'est traitée de façon spécifique la question des cybermenaces.

172 Une première SNPC avait été adoptée pour la période 2012-2017 et une seconde pour les années 20182022[350]. En 2018, sept objectifs ont guidé la mise en œuvre de la stratégie : (i) fonder les compétences nécessaires pour repérer et évaluer les cyberrisques, (ii) mettre en place des mesures de prévention efficaces, (iii) avoir les capacités requises pour gérer les cyberincidents, (iv) augmenter la résilience des infrastructures d'importance vitale, (v) accroître la collaboration de l'État avec la société et les milieux économiques, (vi) augmenter la coopération internationale et finalement (vii) tirer des leçons des cyberincidents[351]. Ces objectifs se retrouvaient dans un plan d'action qui les concrétisait par une trentaine de mesures touchant à la fois à la cybersécurité, à la cyberdéfense et à la poursuite de la cybercriminalité, ce qui impliquait la mobilisation de compétences bien définies. Le NCSC a été mis sur pied sur la base de la SNPC 2018-2022 car il a été constaté, à l'issue de la SNPC 2012-2017, que la répartition des responsabilités manquait de clarté[352]. L'aOPCy a également été adoptée dans le contexte de la SNPC 2018-2022. Elle a servi de fondement légal pour les compétences du guichet national unique en matière de cybersécurité (qui existait déjà avant l'introduction de l'ordonnance sous le couvert de MELANI), mais également de l'autorité principale pour la cybersécurité en Suisse, le NCSC (auquel MELANI a été intégrée), et de GovCERT, l'équipe gouvernementale de gestion technique des cyberincidents.

173 Parmi les autres mesures de la SNPC 2018-2022 figurait par exemple l'élargissement du groupe cible de MELANI, en y incluant la protection des PME et de la population, et non plus seulement les infrastructures critiques et l'administration publique[353]. Le besoin de légiférer s'étant finalement fait ressentir, la stratégie avait prévu l'établissement de standards minimaux pour la sécurité TIC dans certains domaines critiques et la cyberdéfense a été intégrée à la SNPC[354].

350 GCSCC, *Cybersecurity capacity review – Switzerland*, 2020, p. 7.

351 CF, *Plan de mise en œuvre de la SNPC 2018-2022*, 2019, p. 4 ; GCSCC, *Cybersecurity capacity review – Switzerland*, 2020, p. 7 s.

352 UPIC, *Rapport « évaluation de l'efficacité de la stratégie nationale de protection contre les cyberrisques (SNPC) »*, 2016, p. 66 s. ; CF, *Plan de mise en œuvre de la SNPC 2018-2022*, 2019, p. 7.

353 Les compétences du NCSC sont toutefois plus étendues lorsqu'il en va des infrastructures critiques que des PME ou de la population.

354 UPIC, *Rapport « évaluation de l'efficacité de la stratégie nationale de protection contre les cyberrisques (SNPC) »*, 2016, p. 23 et 61 ; CF, *Plan de mise en œuvre de la SNPC 2018-2022*, 2019, p. 31 et 81.

Cette stratégie renouvelée avait aussi pour but d'augmenter la compréhension de ces concepts en dehors des principaux groupes cibles, ce qui n'était auparavant pas satisfaisant[355]. C'est finalement en partie dans ce cadre qu'un projet d'obligation de signaler les cyberattaques ciblant les infrastructures critiques a été élaboré.

La nouvelle CSN a été adoptée en 2023 ; sa teneur et sa mise en œuvre 174
seront examinées en 2028[356]. Elle fixe le cadre stratégique principalement pour la prévention dans le domaine de la cybersécurité, la détection précoce des cybermenaces ainsi que la réaction aux cyberincidents et la résilience (art. 2 al. 1 du Projet d'Ordonnance sur la cybersécurité, P-OCyS). La stratégie poursuit cinq objectifs stratégiques : (i) la responsabilisation de l'ensemble des groupes cibles, (ii) la fiabilité des infrastructures et des services numériques, (iii) la détection, la prévention, la gestion et la défense efficaces contre les cyberincidents, (iv) la lutte et la poursuite pénale efficaces contre la cybercriminalité et (v) le rôle de premier plan de la Suisse dans la coopération internationale[357]. L'orientation choisie par le CF dans la CSN est pertinente et elle englobe des objectifs importants dans la protection de la Suisse contre les cybermenaces.

La responsabilisation de tous les groupes cibles doit passer non seulement 175
par la formation, la recherche et l'innovation, mais aussi par la sensibilisation, le développement des compétences pour suivre et évaluer les cybermenaces ainsi que par l'analyse des tendances, des risques et des dépendances. La fiabilité des infrastructures et des services numériques est garantie par l'identification et la gestion de vulnérabilités, la normalisation et la réglementation ainsi que le renforcement de la collaboration entre autorités. L'objectif de détection, prévention, gestion et défense efficaces contre les cyberattaques, implique la gestion des cyberincidents par toutes les autorités, organisations et personnes concernées, l'attribution des cyberattaques aux personnes à l'origine de ces actes ainsi que le développement des compétences de gestion de crise et de cyberdéfense. La poursuite pénale de la cybercriminalité est assurée par un renforcement de la collaboration des autorités compétentes, par leur formation ainsi que par une meilleure vue d'ensemble des cas. Finalement, pour que la Suisse détienne un rôle de premier plan dans la coopération

355 UPIC, *Rapport « évaluation de l'efficacité de la stratégie nationale de protection contre les cyberrisques (SNPC) »*, 2016, p. 72 s. ; CF, *Plan de mise en œuvre de la SNPC 2018-2022*, 2019, p. 69 ss.

356 CF, *CSN*, 2023, p. 35.

357 CF, *CSN*, 2023, p. 11 ss.

internationale, la « Genève internationale »[358] dans le domaine doit être renforcée. L'engagement de la Suisse dans les réglementations internationales pour le cyberespace et la coopération bilatérale avec des partenaires stratégiques et des centres de compétence internationaux sont mises en avant pour atteindre les objectifs liés à la coopération internationale[359].

C. Les autres stratégies de la Suisse numérique

176 D'autres stratégies ont été adoptées dans le cadre de la transformation numérique suisse. Il s'agit principalement de la Stratégie suisse de cyberadministration, de la Stratégie suisse d'informatique en nuage, de la Stratégie *Open Government Data* (OGD) et de la Stratégie numérique de la Confédération[360].

177 L'adoption de la Stratégie suisse de cyberadministration vise à garantir le succès de la transformation numérique avec l'établissement d'un plan d'action pour la coordination entre les différents échelons de l'État, à savoir la Confédération, les cantons et les communes. La numérisation de l'administration est dirigée par l'idée que les opportunités du numérique doivent être exploitées lorsque c'est possible[361]. La sécurité de l'information et la protection de la sphère privée dans l'implémentation des services électroniques sont considérées comme prioritaires, notamment par l'échange sécurisé de données entre autorités et l'identification sécurisée[362].

178 De la même façon, la sécurité de l'information doit être garantie lors de la mise en œuvre de la Stratégie OGD, qui se concentre sur le libre accès aux données publiques en Suisse. Elle doit aussi être garantie dans le cadre de la Stratégie informatique en nuage, qui vise à garantir une bonne utilisation de services en nuage (privé et public) et, surtout, leur mise en place par l'administration fédérale ou dans le cadre de la stratégie informatique de la Confédération. Cette stratégie constitue l'instrument de pilotage opérationnel servant

358 Soit la plateforme principale en Suisse pour des débats internationaux sur la cybersécurité, cf. CF, *CSN*, 2023, p. 11.

359 CF, *CSN*, 2023, p. 13 ss.

360 Sur ces différentes stratégies, voir MONTAVON, p. 27 s. et 32 ss. À noter que la Stratégie numérique de la Confédération s'appelait auparavant la Stratégie informatique de la Confédération, CF, *Stratégie numérique de la Confédération 2020-2023*, 2021, p. 3. Certaines stratégies sont concrétisées par d'autres stratégies en fonction des axes qu'elles poursuivent ; celles-ci visent parfois des considérations de cybersécurité, à l'instar de la Stratégie d'approvisionnement informatique de la Confédération qui découle de la Stratégie numérique de la Confédération, cf. CF, *Stratégie d'approvisionnement informatique de la Confédération 2018-2022*, 2018, p. 12 s. et 16.

361 EGOVERNMENT, *Stratégie suisse de cyberadministration 2020-2023*, 2019, p. 10.

362 EGOVERNMENT, *Stratégie suisse de cyberadministration 2020-2023*, 2019, p. 4 ss.

à la mise en œuvre des stratégies pertinentes pour l'informatique de l'administration fédérale. La Stratégie informatique en nuage donne aussi des orientations pour la gestion informatique de l'administration fédérale[363].

179 Ces stratégies ne se concentrent pas, à l'inverse de la CSN, sur la cybersécurité ou plus généralement sur la protection contre les cybermenaces, raison pour laquelle elles ne seront pas approfondies dans la présente étude. Néanmoins, ces instruments mentionnent toujours l'importance de la cybersécurité, de la sécurité de l'information ou de la protection des données, en renvoyant parfois à la CSN ou à la législation applicable[364].

D. En résumé

180 Les autorités suisses se sont saisies de la question de la transformation numérique et la Stratégie Suisse numérique a été adoptée. Elle constitue la stratégie principale en Suisse pour la transformation numérique. Cette stratégie prévoit divers objectifs dont la garantie de la cybersécurité.

181 Pour concrétiser sur le plan politique l'orientation de la Confédération en matière de cybersécurité ainsi que les mesures à prendre, le CF a adopté deux SNPC qui se sont succédé. Depuis 2023, la CSN adoptée est en place. Elle poursuit les objectifs principaux visant à assurer la protection de la Suisse contre les cybermenaces. La CSN prévoit en effet des objectifs et des mesures de cybersécurité, de lutte contre la cybercriminalité et de cyberdéfense en impliquant une diversité de groupes cibles.

182 D'autres stratégies ont été adoptées dans le cadre de la transformation numérique, à l'instar de la Stratégie suisse de cyberadministration ou de la Stratégie numérique de la Confédération, qui prévoient des objectifs de sécurité. Elles mentionnent l'importance du sujet et renvoient à la CSN malgré qu'elles ne précisent en principe pas la mise en place de mesures de cybersécurité.

363 FF 2019 855, p. 858 ; CF, *Stratégie d'informatique en nuage de l'administration fédérale,* 2020, p. 5 ; DDPS, *Prüfbericht « Cloud-Computing » – IKT-Prüfung I 2019-05,* 11 décembre 2019, p. 5 s. ; CF, *Stratégie numérique de la Confédération 2020-2023,* 2021, p. 4 et 19.

364 La Stratégie suisse d'informatique en nuage prévoit une mesure pour assurer justement la protection de l'information et des données compte tenu des instruments légaux en la matière et la Stratégie numérique de la Confédération précise que des adaptations légales sont en cours pour assurer la cybersécurité et mentionne la SNPC, cf. CF, *Stratégie d'informatique en nuage de l'administration fédérale,* 2020, p. 14 s. ; CF, *Stratégie numérique de la Confédération 2020-2023,* 2021, p. 8 et 26.

II. D'autres stratégies pour la protection contre les cybermenaces

A. La Stratégie pour la protection des infrastructures critiques

183 Les infrastructures critiques représentent l'un des groupes cibles centraux de la CSN, raison pour laquelle la Stratégie PIC est importante dans ce contexte. Elle a vocation à instaurer, conjointement à la CSN, des principes, des mesures et un champ d'action à l'attention des secteurs critiques. Afin de définir les secteurs d'infrastructures critiques et d'assurer des normes protectrices secteur par secteur, une première Stratégie PIC avait été adoptée en 2012. Elle a été actualisée en 2017 puis en 2023[365]. Cette stratégie se concentre sur les mesures permettant de réduire la probabilité qu'un incident se réalise et les dommages qu'il peut engendrer auprès d'une infrastructure critique. La finalité poursuivie est celle d'éviter des pannes de grande ampleur et de limiter les dommages à la suite d'un événement dommageable[366]. La Stratégie PIC de 2023 définit en outre des mesures visant à améliorer la résilience sectorielle et intersectorielle ; elle concerne tant les niveaux communal et cantonal que fédéral. Elle poursuit plusieurs objectifs, dont la résilience des infrastructures critiques, de sorte à éviter des pannes graves et à garantir un rétablissement du bon fonctionnement en cas d'incident, ainsi que la préparation des autorités à réagir aux pannes et le soutien efficace pour maîtriser les incidents[367].

184 La Stratégie PIC prévoit également des mesures de sécurité non seulement préventives, préparatoires ou liées à l'engagement visant à éviter des pannes, mais aussi permettant de garantir le maintien du bon fonctionnement en cas d'incident, ou à réduire les dommages. À cette fin peuvent être prises par exemple des mesures techniques (à l'instar d'une séparation des systèmes informatiques), organisationnelles (comme l'exécution de contrôle d'accès, la mise en place d'un état-major de crise ou la formation du personnel), ou encore juridiques[368].

185 La sécurité des infrastructures critiques étant l'un des aspects principaux de la CSN, la Stratégie PIC et celle-ci sont étroitement liées. Elles poursuivent des objectifs communs, en particulier lorsqu'il en va de la cyberrésilience des infrastructures critiques[369].

365 FF 2023 1659, p. 3 ; GCSCC, *Cybersecurity capacity review – Switzerland*, 2020, p. 28.

366 FF 2013 1659, p. 9 ; GCSP, *Guide to Developing a National Cybersecurity Strategy*, 2021, p. 41.

367 FF 2013 1659, p. 3 s. et 10.

368 FF 2013 1659, p. 8.

369 FF 2013 1659, p. 4 s. ; CF, *CSN*, 2023, p. 8.

B. La Stratégie de lutte contre la criminalité

Une stratégie de lutte contre la criminalité a été adoptée pour la période 2020–2023. Elle met l'accent sur la cybercriminalité, qui est quasi omniprésente[370]. La cybercriminalité n'est pas considérée comme un domaine d'infractions à proprement parler, mais plutôt comme un phénomène transversal présentant pour chaque type d'infractions des défis particuliers[371]. Les trois piliers de la stratégie sont la prévention, la coopération et la répression[372]. Pour une mise en œuvre efficace, il est nécessaire que cette stratégie soit coordonnée avec les autres projets nationaux, dont la CSN fait partie[373]. 186

Le croisement entre la poursuite pénale de la cybercriminalité et la cybersécurité est nécessaire. De manière générale, il va de soi que lors d'une attaque malveillante, les mécanismes pénaux peuvent s'enclencher en raison de la réalisation d'infractions. Il n'est toutefois pas toujours évident, pour les autorités de poursuite pénale, de détecter des cyberattaques sans être prévenues, souvent par la personne lésée. Une plainte pénale peut alors être nécessaire afin de démarrer une procédure pénale, qui demeure l'unique moyen de condamner les personnes à l'origine d'infractions. En revanche, le dépôt de plainte ne suffit pas pour écarter directement tout danger et les buts principaux de la procédure pénale ne sont pas de rétablir des situations sûres. Il est par conséquent important que les personnes lésées puissent être informées à propos des vecteurs d'attaques et qu'elles puissent bénéficier d'un soutien, de sorte à protéger les systèmes informatiques ainsi que d'identifier les cyberattaques déjà survenues[374]. 187

C. Le cadre stratégique pour la cyberdéfense

Le Département fédéral de la défense, de la population et des sports (DDPS) intervient à plusieurs reprises dans la CSN. En parallèle, il a adopté un plan d'action Cyberdéfense (PACD) en 2017 pour la mise en œuvre de la CSN au sein du département. Le PACD a tout d'abord eu comme but d'optimiser et renforcer 188

370 DFJP, *Stratégie de lutte contre la cybercriminalité 2020-2023,* 2019, p. 2. La cybercriminalité prend en importance aussi au-delà des frontières suisses, cf. ENISA, *Baseline Capabilities of National/Governmental CERT, Part 2,* 2010, p. 35.

371 Cette conception serait liée au fait que bon nombre d'infractions « classiques » sont perpétrées dans le cyberespace, DFJP, *Stratégie de lutte contre la cybercriminalité 2020-2023*, 2019, p. 3.

372 DFJP, *Stratégie de lutte contre la cybercriminalité 2020-2023,* 2019, p. 1.

373 DFJP, *Stratégie de lutte contre la cybercriminalité 2020-2023*, 2019, p. 1s.

374 FF 2017 2765, p. 2801.

les moyens à disposition du DDPS pour lui permettre d'affronter, dans le cadre de ses tâches et en tant qu'infrastructure critique, les « cyberconflictualités », au quotidien comme en cas de crise ou de conflit. Ensuite, il devait permettre de mettre en œuvre concrètement les cyberaspects relatifs à la Loi fédérale sur le renseignement (LRens) et à la Loi fédérale sur l'armée et l'administration militaire (LAAM)[375]. Concrètement, il s'agissait tout d'abord pour le DDPS de « protéger, défendre et assurer la résilience en tout temps et toute circonstance de ses systèmes et infrastructures TIC contre les cybermenaces et cyberattaques »[376]. Le principe de responsabilité propre à chaque entité est important et implique que le DDPS est tenu, au même titre que les autres autorités, d'assurer la protection de ses processus, systèmes et infrastructures[377]. Le DDPS conduit également les opérations de renseignement ou les opérations militaires se déroulant dans le cyberespace et apporte un appui aux autorités civiles, en particulier lorsque des cyberattaques visent des infrastructures critiques[378].

189 La mise en œuvre du plan d'action a permis de nombreux progrès dans le domaine de la cyberdéfense. Elle a permis la création de nouvelles fonctions permettant de mettre en place une surveillance des réseaux ainsi que l'adoption l'OCMil. La mise en œuvre du plan d'action a également démontré que le SRC pouvait rapidement détecter, prévenir et « attribuer » les attaques[379]. L'ensemble des objectifs fixés n'ont cependant pas été atteints et le cyberespace continue d'évoluer. Partant, une Stratégie cyber 2021-2024 a été adoptée par le DDPS sur la base du plan d'action et pour faire suite à ce dernier[380]. La stratégie est consacrée aux menaces, aux défis et aux tendances à venir dans le cyberespace à l'échelle mondiale. Elle prévoit des mesures permettant de les appréhender au mieux et fonde la contribution du DDPS à la sécurité de la Suisse, tout en tenant compte des objectifs fixés par la SNPC 2018-2022[381].

375 DDPS, *PACD,* 2017, p. 4.

376 DDPS, *PACD,* 2017, p. 12.

377 DDPS, *PACD,* 2017, p. 14.

378 DDPS, *PACD,* 2017, p. 12.

379 DDPS, *Stratégie Cyber VBS,* 2021, p. 20 ss.

380 ARMÉE SUISSE, *Conception générale cyber,* 2023, p. 24 ; DDPS, *Stratégie Cyber VBS,* 2021, p. 2.

381 CF, *Rapport sur l'avancement des travaux concernant la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022,* 2021, p. 6 ; DDPS, *Stratégie Cyber VBS,* 2021, p. 1 s. ; CF, *Plan de mise en œuvre de la SNPC 2018-2022,* 2019, p. 55 ss.

En 2023, la Conception générale cyber de l'armée suisse a en parallèle été adoptée. Elle met d'une part en évidence les défis du cyberespace et de l'espace électromagnétique (CYBEEM) ainsi que des TIC. Elle décrit d'autre part les capacités que l'armée doit développer d'ici 2035[382]. 190

D. La Stratégie de politique extérieure numérique

La Stratégie de politique extérieure numérique est un prolongement de la politique extérieure de la Suisse. Elle vise à appréhender le rôle que le pays souhaite occuper en assurant une bonne gouvernance numérique, la cybersécurité, l'autodétermination numérique ainsi que sa prospérité et son développement durable[383]. 191

En termes de cybersécurité plus précisément, la stratégie poursuit deux objectifs. Elle vise d'une part à assurer un bon niveau de sécurité pour les citoyennes et citoyens, institutions, entreprises et organisations, en Suisse comme à l'étranger (sur le plan physique comme sur le plan informationnel). Elle cherche d'autre part à garantir un accès à Internet aussi libre, ouvert et sûr que possible[384]. Elle se focalise sur la concrétisation de normes de droit international, sur l'intégration des actrices privées et sur l'implémentation de mesures de confiance et des bons offices[385]. 192

E. La politique de gestion de risques de la Confédération

La sécurité, pour être efficace, doit encore reposer sur une bonne gestion des risques[386]. En 2005, la Confédération a adopté dans ce contexte un système qui s'orientait sur les risques encourus par la Confédération[387]. Elle a élaboré dans ce cadre des directives ainsi qu'un manuel afin d'harmoniser les pratiques en matière d'appréciation et de recensement des risques[388]. La gestion de ces 193

382 ARMÉE SUISSE, *Conception générale cyber*, 2023, p. 7 ; CF, *CSN*, 2023, p. 8.

383 DFAE, *Stratégie de politique extérieure numérique 2021-2024*, 2020, p. 3 s. ; NCSC, *Rapport semestriel 2020/2*, 2021, p. 28.

384 DFAE, *Stratégie de politique extérieure numérique 2021-2024*, 2020, p. 12.

385 DFAE, *Stratégie de politique extérieure numérique 2021-2024*, 2020, p. 13 ; NCSC, *Rapport semestriel 2020/2*, 2021, p. 28.

386 Voir par exemple FF 2018 491, p. 516.

387 FF 2018 491, p. 498 et 499.

388 FF 2018 1433, p. 1437. Les risques sont considérés dans ce contexte comme « des événements et développements qui ont une certaine probabilité de se produire et qui ont des conséquences négatives majeures d'ordre financier et non financier sur l'atteinte

derniers est liée à d'autres questions, dont celle de la sécurité informatique. Les directives et le manuel de gestion des risques de la Confédération prévoient une série de mesures afin de gérer ceux liés à l'informatique. Ces instruments soulèvent des questions telles que celles de la responsabilité et de la collaboration permettant de gérer ces risques transversaux[389].

F. En résumé

194 Certaines stratégies hors de la Stratégie Suisse numérique présentent un intérêt pour la protection de la Suisse contre les cybermenaces et pour la cybersécurité en Suisse. La Stratégie PIC est étroitement liée à la CSN dans la mesure où la cybersécurité des infrastructures critiques est un élément essentiel de la protection de la Suisse contre les cybermenaces et, en même temps, un élément crucial de la protection des infrastructures concernées.

195 Les stratégies dans les domaines de la lutte contre la cybercriminalité et de la cyberdéfense sont également importantes car elles constituent les instruments politiques applicables aux domaines voisins et complémentaires à celui de la cybersécurité. La cybersécurité, la lutte contre la cybercriminalité et la cyberdéfense composant les trois domaines de la protection de la Suisse contre les cybermenaces, il est important d'avoir une vision globale de ces stratégies. La Stratégie de lutte contre la criminalité met aujourd'hui un accent sur la cybercriminalité quasi omniprésente. Le cadre stratégique pour la cyberdéfense sert en outre à appréhender les défis liés au cyberespace dans le cadre des compétences de l'armée ou d'autres autorités telles que le SRC.

196 D'autres instruments politiques sont adoptés en parallèle et sont susceptibles de revêtir un intérêt dans l'analyse du cadre stratégique autour de la cybersécurité en Suisse. La Stratégie de politique extérieure numérique vise à assurer un bon niveau de sécurité pour la société en Suisse comme à l'étranger sur le plan informationnel ainsi qu'à garantir un accès sûr à Internet. La politique de gestion des risques de la Confédération tient également compte de la sécurité informatique. Les directives et le manuel de gestion de risques de la Confédération prévoient par conséquent des mesures pour gérer les risques liés à l'informatique. Il va de soi que d'autres instruments et prises de

des objectifs et l'exécution des tâches dans l'administration fédérale », cf. ch. 2 al. 1 des Directives du Conseil fédéral du 24 septembre 2010 sur la politique de gestion des risques par la Confédération, FF 2010 4275, p. 5965.

389 AFF, *Manuel de gestion des risques de la Confédération,* 2022, p. 37.

position politiques peuvent toucher à la cybersécurité ou à un aspect de la protection de la Suisse contre les cybermenaces[390].

III. Une conclusion au chapitre 2

Il est nécessaire de comprendre comment la Confédération se saisit de la cybersécurité au niveau politique. En effet, les instruments politiques qu'elle adopte illustrent l'orientation qu'elle prend afin d'assurer la protection du pays contre les cybermenaces. Ils permettent aussi de comprendre quelles ressources doivent être mobilisées. 197

La Suisse s'est penchée sur la transformation numérique et son orientation politique démontre que le pays l'appréhende de façon globale. Les instruments adoptés devraient permettre de profiter des opportunités qu'offre la transformation numérique tout en tentant de maîtriser au mieux les risques qu'elle occasionne. Le cadre suisse servant à appréhender la transformation numérique dans son ensemble est la Stratégie Suisse numérique (I.A). Elle a un caractère général et regroupe la CSN ainsi que les stratégies OGD, d'informatique en nuage ou encore de cyberadministration. La CSN est l'instrument politique principal pour la protection de la Suisse contre les cybermenaces. C'est dans cette stratégie que le CF prévoit les objectifs poursuivis et les mesures à mettre en place par les différents groupes cibles afin de renforcer leur cyberrésilience (I.B). Les autres stratégies issues de la Stratégie Suisse numérique se concentrent sur diverses considérations s'éloignant des questions de cybersécurité (I.C). 198

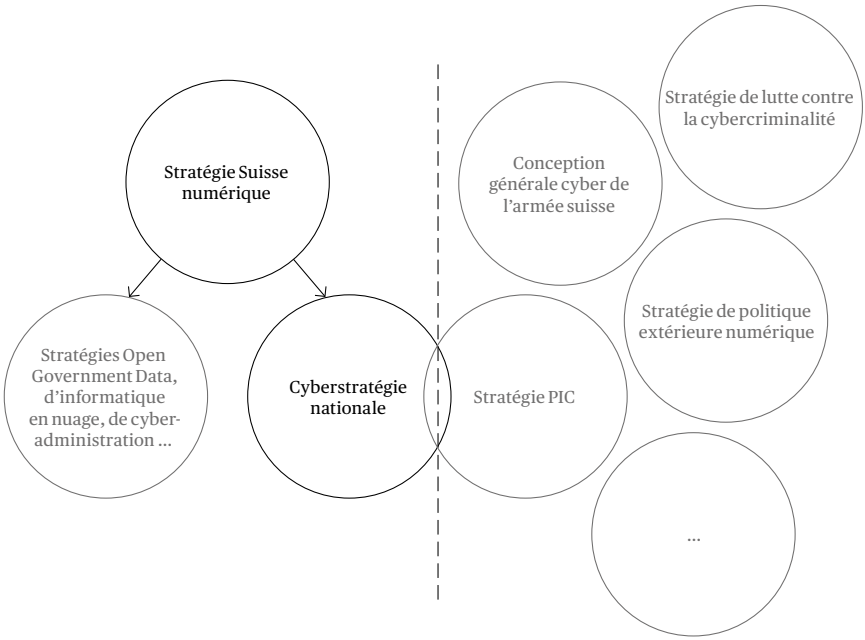
En parallèle aux stratégies issues de la Stratégie Suisse numérique, d'autres instruments politiques sont déterminants s'agissant de la cybersécurité, en particulier concernant les infrastructures critiques. La Stratégie PIC doit être coordonnée avec la CSN car les deux stratégies constituent la documentation principale pour la cybersécurité des infrastructures critiques (II.A). Au-delà de cette stratégie, d'autres instruments politiques revêtent une certaine importance et doivent être mentionnés pour appréhender la cybersécurité et, plus largement, la protection contre les cybermenaces de la façon la plus globale. Il s'agit typiquement de la Stratégie de lutte contre la cybercriminalité, 199

390 Le CF s'est par ailleurs saisi de la question des cyberrisques, en visant pour 2024 l'objectif d'anticiper les cyberrisques et de soutenir à cette fin les mesures pour protéger la population, l'économie et les infrastructures critiques, ChF, *Objectifs du Conseil fédéral 2024*, 2023, p. 39.

de la Conception générale cyber de l'armée suisse, de la Stratégie de politique extérieure numérique ou de la politique de gestion de risques de la Confédération (II.B à E).

200 Il est possible d'illustrer cette vue d'ensemble des différents instruments politiques en jeu comme suit :

Schéma 5 : les instruments politiques suisses et la cybersécurité



201 Maintenant que le cadre politique est établi, il convient d'analyser les groupes cibles et les principales intervenantes pour la cybersécurité en Suisse. L'examen des compétences des diverses autorités et organisations intervenant dans les processus de cybersécurité permet d'amorcer la réflexion sur les personnes, organisations et autorités concernées par la législation et sur les attentes que l'on peut avoir d'une législation de cybersécurité.

Chapitre 3 : les compétences principales en cybersécurité

Préambule au chapitre 3

Les compétences en matière de cybersécurité ont longtemps manqué de clarté et se trouvaient dispersées entre différents instruments réglementaires. L'administration fédérale a tenté, au fil des années, de clarifier la situation et une première centralisation a été opérée dans le cadre de la SNPC 2018-2022. Cette centralisation a encore été réorganisée début 2024. Les principales modifications dans l'organisation de la cybersécurité en Suisse concernent les autorités compétentes pour la cybersécurité et la sécurité de l'information. Le NCSC a été créé en 2020 et la décision a été prise fin 2022 de le transformer en un office fédéral (art. 15a de l'Ordonnance sur l'organisation du Département fédéral de la défense, de la protection de la population et des sports, Org-DDPS)[391]. La création du NCSC, puis sa transformation en OFCS, ont permis la centralisation de nombreuses compétences en termes de cybersécurité, qui sont désormais majoritairement détenues par l'OFCS (I.A). 202

L'OFCS n'est pas l'unique autorité au service de la cybersécurité. Une vue d'ensemble des actrices est nécessaire afin de comprendre la répartition des compétences ainsi que les collaborations en place au sein de cet écosystème. Cette vue d'ensemble ne saurait se limiter au domaine de la cybersécurité, au vu de sa proximité avec les autres domaines de la protection contre les cybermenaces, à savoir la cyberdéfense et la poursuite pénale de la cybercriminalité (I.B, C et D). Les autorités compétentes pour la cybersécurité sont également amenées à collaborer avec des autorités compétentes dans d'autres domaines connexes, à l'instar de la sécurité de l'information ou de la protection des données personnelles (I.E). 203

Les intervenantes disposant de compétences pour la cybersécurité en Suisse ne sont pas uniquement des autorités. En raison du rôle partenarial et subsidiaire de l'État dans le domaine de la cybersécurité, des actrices privées détiennent également des compétences importantes en pratique. L'accent doit avant tout être mis sur les prestataires de gestion de cyberincidents, qui sont les premières intervenantes dans la cybersécurité, en particulier lorsqu'un cyberincident se produit (II.A, B et C). D'autres entités privées sont importantes dans l'écosystème de la cybersécurité, comme les communautés et autres organisations (II.D). 204

391 CF, *CSN*, 2023, p. 9.

I. Les actrices principales de la Confédération

A. Pour la cybersécurité

1. L'évolution en cours

205 L'organisation de la cybersécurité auprès de la Confédération n'a longtemps pas été claire. Certaines compétences étaient attribuées à différentes autorités durant de nombreuses années. C'est en 2019 qu'une centralisation des compétences a débuté par la création du NCSC. Celui-ci abritait jusqu'à fin 2023 différents services visant à assurer les divers aspects de la cybersécurité de façon centralisée au sein de la Confédération.

206 La situation a donc récemment changé, par la transformation du NCSC en OFCS, opérationnel dès janvier 2024[392]. Cette transformation s'accompagne d'un déplacement du NCSC, jusque-là rattaché au Département fédéral des finances (DFF), au sein du DDPS[393]. L'OFCS a repris une partie des compétences du NCSC, mais non l'ensemble de ses compétences. En effet, un service spécialisé de la Confédération pour la sécurité de l'information intégré au SEPOS a été créé en même temps que l'OFCS et ce service spécialisé a hérité des tâches du NCSC en matière d'autoprotection de la Confédération, ce qui implique la reprise de certaines compétences de sécurité de l'information et de sécurité informatique[394].

2. La situation jusqu'à fin décembre 2023

a. Le Centre national pour la cybersécurité et son organisation

(i) Le Centre national pour la cybersécurité

207 Le NCSC a été, entre 2019 et 2023, l'autorité principale pour la cybersécurité en Suisse. Il détenait à ce titre de nombreuses compétences dans le domaine et c'est à lui que revenaient les tâches les plus importantes dans le domaine de la cybersécurité.

208 Concrètement, il élaborait les directives en matière de sécurité informatique, conseillait les unités administratives lors de leur application et vérifiait le niveau de sécurité informatique au sein des départements de l'administration et de la Chancellerie fédérale (ChF)[395]. Ses compétences, prévues à l'origine à l'art. 12 aOPCy, sont maintenant définies aux art. 73*a* ss LSI2 et 15*a* Org-DDPS ; elles seront abordées plus tard au sein de la présente étude[396]. De manière

392 CF, *CSN*, 2023, p. 9.

393 CF, *Le NCSC deviendra un office du DDPS*.

394 *Législation d'exécution relative à la LSI, Explications*, 2023, p. 5.

395 AFF, *Manuel de gestion des risques de la Confédération*, 2021, p. 59.

396 Cf. *infra* N 703 ss.

générale, le NCSC détenait des compétences de sensibilisation, de mise à disposition d'information et d'instructions sur les mesures à prendre contre les cyberrisques ainsi que de réception de signalements sur des vulnérabilités ou incidents et de soutien aux infrastructures critiques (art. 73a LSI2)[397].

(ii) La personne déléguée à la cybersécurité

Florian Schütz était le délégué à la cybersécurité ou le cyberdélégué[398]. Il avait pour mission de diriger le NCSC (art. 11 al. 1 litt. a aOPCy) et était la personne responsable pour les cybermenaces au niveau de la Confédération. Ce délégué coordonnait la protection contre les cyberrisques, assurait la visibilité de l'action de la Confédération dans le secteur et assumait un rôle d'interlocutrice et de représentant de la Confédération (art. 11 al. 1 litt. b et c aOPCy)[399]. Il avait pour mission de publier des rapports annuels sur les différents travaux liés à la SNPC[400]. En charge de la direction du NCSC, il représentait ce dernier dans les états-majors de crise de la Confédération, comme prévu à l'origine par l'art. 11 al. 1 litt. d aOPCy. Florian Schütz avait finalement la compétence d'édicter les directives en matière de sécurité informatique et décidait des dérogations à celles-ci (art. 11 al. 1 litt. e et f aOPCy)[401]. Il est depuis janvier 2024 le directeur de l'OFCS[402]. 209

(iii) L'ancienne MELANI

MELANI était la Centrale d'enregistrement et d'analyse pour la sûreté de l'information[403]. Elle a été mise sur pied en 2003 par le CF dans le cadre d'une stratégie élaborée à l'époque par l'Unité de stratégie informatique de la Confédération (USIC). Elle a été créée par l'Unité de pilotage informatique de la Confédération (UPIC) et le Service de renseignement de la Confédération 210

397 NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures,* 2022, p. 14 ; NCSC, *Rapport sur la sécurité informatique de la Confédération,* 2021, p. 9.

398 DFF, *Erläuterungen zur Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung,* 2020, p. 4 ; CF, *Florian Schütz a été nommé délégué en 2019*.

399 Cff, *Audit de l'efficacité de la lutte contre la cybercriminalité,* 2021, p. 39.

400 Cff, *Audit de l'efficacité de la lutte contre la cybercriminalité,* 2021, p. 17.

401 NCSC, *Rapport sur la sécurité informatique de la Confédération,* 2021, p. 3. Lorsque les dérogations concernent également les directives de la Chancellerie fédérale sur la transformation numérique et la gouvernance de l'informatique, la personne déléguée consulte le secteur TNI avant de prendre de telles décisions, cf. art. 11 al. 1 litt. f aOPCy ; DFF, *Erläuterungen zur Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung,* 2020, p. 5.

402 CF, *Florian Schütz nommé directeur du nouvel Office fédéral de la cybersécurité*.

403 WEBER/WILLI, p. 79.

(SRC) et introduite définitivement en 2007[404]. Après une période d'évaluation, elle a été intégrée au NCSC à la création de ce dernier[405].

211 Au départ, ses tâches principales étaient la collecte et l'analyse d'informations concernant les cybermenaces pesant sur les infrastructures critiques, le soutien de ces dernières en cas d'incident, la coordination sectorielle et intersectorielle en cas de crise et la prévention[406]. MELANI opérait principalement en faveur de son cercle fermé de clientes dans des secteurs critiques[407]. Durant plusieurs années, les compétences de MELANI ne se sont pas étendues, mais elle a fini par s'ouvrir aux entreprises et à la population, soit à un cercle plus étendu pour certaines prestations. Cela n'a pas empêché le renforcement du PPP entre MELANI et son cercle fermé d'infrastructures critiques, notamment pour la plateforme d'échange d'informations[408]. À la suite de la restructuration de l'organisation fédérale de 2019 en matière de cybersécurité, MELANI comptait en son sein GovCERT, l'*Operation Information Center* de MELANI (MELANI OIC), le service *Open source intelligence* (OSINT), le Réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique (NEDIK) et le guichet national. Les tâches de MELANI ont été peu à peu transférées au NCSC qui a remplacé MELANI, notamment avec sa centrale d'enregistrement[409].

(iv) GovCERT

212 L'équipe d'intervention en cas d'urgence informatique GovCERT, rattachée jusqu'à fin 2023 à MELANI, constituait un service spécialisé du NCSC. L'équipe était spécialisée pour la cybersécurité opérationnelle du NCSC. Contrairement à MELANI, elle existe toujours.

213 Concrètement, GovCERT est l'équipe technique et scientifique ou *Computer Emergency Response Team* (CERT) de la Confédération depuis le 1er avril

404 OFPP, *Protection de la population 27,* 2017, p. 10.

405 GCSCC, *Cybersecurity capacity review – Switzerland,* 2020, p. 8.

406 OFPP, *Protection de la population 27,* 2017, p. 11 s. ; Motion 10.4020 déposée le 16 décembre 2010 par Ida Glanzmann-Hunkeler « Melani pour tous ».

407 GCSCC, *Cybersecurity capacity review – Switzerland,* 2020, p. 27 ; RNS, *Recommandations de mise en œuvre des organisations cantonales pour la cybersécurité,* 2021, p. 14.

408 CF, *Plan de mise en œuvre de la SNPC 2018-2022,* 2019, p. 39 ss ; NCSC, Évaluation de l'efficacité de la stratégie nationale de protection de la Suisse contre les cyberrisques pour les années 2018 à 2022, 2022, p. 24. Il existe, parmi les canaux techniques, MELANI-NET, qui sert justement de plateforme d'échange d'informations entre la Confédération et les infrastructures critiques et qui fonctionne sur une base volontaire.

409 FF 2023 84, p. 13 et 26 ; NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures,* 2022, p. 23 ; GCSCC, *Cybersecurity capacity review – Switzerland,* 2020, p. 27.

2008[410]. GovCERT a été dès sa création le service national spécialisé pour la gestion technique des cyberincidents, l'analyse des questions techniques, l'évaluation technique des menaces et l'appui technique au guichet unique suisse (art. 12 al. 1 litt. c aOPCy)[411]. Le service intervient principalement comme soutien aux équipes présentes en première ligne pour la gestion de cyberincidents[412]. Il sert en outre de point de contact pour la Suisse, participe à la coordination de la réponse aux incidents sur le plan national comme sur le plan international, ainsi qu'à la protection des réseaux de l'administration fédérale suisse et d'autres systèmes et réseaux critiques[413].

Alors que son équipe était initialement rattachée à l'UPIC, GovCERT a 214
été rattachée au NCSC en 2019 et, partant, au DFF, jusqu'à la transformation en janvier 2024 du NCSC en office et son transfert au sein du DDPS[414]. Les États disposent régulièrement de leur CERT nationale au sein d'une autorité gouvernementale, abritant régulièrement un centre de compétences pour la cybersécurité, comme le NCSC[415]. GovCERT est depuis janvier 2024 gérée par l'OFCS (art. 15*a* al. 2 litt. f Org-DDPS).

Les CERT nationales[416], comme GovCERT, poursuivent un but de sécurité 215
nationale. Elles revêtent quelques caractéristiques particulières. Elles doivent par exemple être reconnus comme des CERT nationales par leur gouvernement, pour constituer le point de contact notamment sur le plan international. Elles doivent en outre procéder à tout le moins à des opérations de gestion de cyberincidents pour les systèmes informatiques d'importance nationale et détiennent des compétences de sensibilisation aux cybermenaces. De manière générale, elles cherchent à sauvegarder des intérêts tels que la sécurité

410 MELANI, *Rapport semestriel 2007/2,* 2008, p. 11.

411 MEYER/MÉTILLE, *Computer security incident response teams : are they really regulated ? The Swiss example*, 2022, p. 43. L'art. 7 P-OCyS prévoit que l'équipe d'intervention assume des tâches de gestion des incidents techniques, d'analyse de questions techniques ainsi que d'identification et d'évaluation des cybermenaces.

412 Par exemple, au sein de l'administration fédérale, la surveillance des réseaux relève en partie de la responsabilité de l'équipe d'intervention en cas d'urgence informatique de l'OFIT, cf. NCSC, *Rapport sur la sécurité informatique de la Confédération,* 2021, p. 5.

413 GCSP, *Guide to Developing a National Cybersecurity Strategy,* 2021, p. 39 ; ITU, ***Guide pour l'élaboration d'une stratégie nationale de cybersécurité,*** 2018, p. 40 s ; MEYER/MÉTILLE, *Computer security incident response teams : are they really regulated ? The Swiss example,* 2022, p. 43 ; MORGUS et al., *National CSIRT and Their Role in Computer Security Incident Response,* 2015, p. 8 ; WEST-BROWN et al., p. 62.

414 Art. 17 al. 1 litt. i aOIAF ; UPIC, *Plan de mise en œuvre de la SNPC,* 2013, p. 16 et 20.

415 MORGUS et al., *National CSIRT and Their Role in Computer Security Incident Response,* 2015, p. 9 s.

416 GCSCC, *CSIRT – An Overview,* 2014, p. 7 ; DSOUZA, p. 209 ; MORGUS et al., *National CSIRT and Their Role in Computer Security Incident Response,* 2015, p. 8.

nationale et économique, la sauvegarde des opérations du gouvernement et le bon fonctionnement des infrastructures critiques[417].

216 En plus d'être une CERT nationale, GovCERT a la particularité d'être une CERT gouvernementale. À ce titre, elle constitue l'équipe technique de gestion de cyberincidents pour l'administration fédérale[418]. Par ailleurs, GovCERT est également une CERT coordonnée ou *coordinating CERT*. Cela signifique qu'elle occupe donc une place importante dans la coordination de la gestion de cyberincidents. En effet, elle sert, avec le NCSC (et maintenant l'OFCS) qui l'héberge, de centre de coordination visant à diriger les efforts menés dans le but de gérer un cyberincident tous niveaux confondus, en fournissant des conseils et recommandations ainsi qu'en formant et documentant grâce à son expertise[419]. Les CERT peuvent avoir un cercle de clientes plus ou moins étendu, mais elles fournissent souvent des prestations à un cercle distribué de bénéficiaires[420]. Elles accompagnent les centres et les prestataires de gestion de cyberincidents locales, sectorielles ou internes aux organisations dans leur circonscription et offrent des services présentant une plus-value ; en revanche, elles ne fournissent pas les mêmes prestations que celles-ci[421].

(v) Les autres services du NCSC

217 Le NCSC était composé d'autres services, tantôt rattachés au DFF, tantôt au DFJP ou au DDPS, du moins depuis 2019. Le NEDIK, rattaché au DFJP et aux cantons, sera analysé ci-dessous dans le cadre des autorités compétentes dans la lutte contre la cybercriminalité[422]. MELANI OIC et le service OSINT seront abordés dans le cadre des compétences de cyberdéfense[423].

218 Le guichet unique suisse du NCSC est aussi rattaché au DFF. Il a pour but de centraliser les signalements concernant les cyberincidents, cybermenaces et cyberattaques émanant tant de l'administration fédérale, que

417 ENISA, *National/governmental CERT,* 2014, p. 2 ; GFCE, *GFCE Global Good Practices – National Computer Security Incident Response Teams (CSIRT),* 2017, p. 5 s. ; MEYER/MÉTILLE, *Computer security incident response teams : are they really regulated ? The Swiss example,* 2022, p. 43.

418 MEYER/MÉTILLE, *Computer security incident response teams : are they really regulated ? The Swiss example,* 2022, p. 43 ; MORGUS et al., *National CSIRT and Their Role in Computer Security Incident Response,* 2015, p. 11.

419 KILLCRECE et al., Organisational Models of CSIRT, 2003, p. 116 ; MEYER/MÉTILLE, *Computer security incident response teams : are they really regulated ? The Swiss example,* 2022, p. 43.

420 KILLCRECE et al., *Organisational Models for CSIRT,* 2003, p. 113 s.

421 KILLCRECE et al., *Organisation Models for CSIRT,* 2003, p. 116.

422 Cf. *infra* N 239.

423 Cf. *infra* N 250 s.

des infrastructures critiques, des milieux économiques et de la population (art. 73*a* al. 2 litt. d, 73*b* al. 1 et 74*a* al. 1 LSI2)[424].

b. Les départements, la chancellerie et les unités administratives

La protection contre les cybermenaces est naturellement liée à la transformation numérique. Les départements fédéraux et la ChF sont responsables de cette transformation dans leurs domaines de compétences respectifs et règlent la gouvernance informatique dans ces domaines (art. 3 OTNI). 219

Tout comme l'ensemble des autorités et organisations de la Confédération, les départements, la ChF et les unités administratives sont responsables de l'organisation, de la mise en œuvre et du contrôle de la sécurité de l'information, et de la sécurité des moyens informatiques qu'elles exploitent pour elles-mêmes ou sur mandat d'une autre autorité ou organisation (art. 19 al. 1 LSI)[425]. En tant qu'organisations au sens de l'art. 2 al. 2 LSI, elles sont responsables, doivent détenir des compétences et sont soumises à différentes obligations dans le contexte de la sécurité de l'information et de la sécurité informatique en vertu des art. 6 ss LSI et 5 ss OSI. 220

c. D'autres autorités impliquées

L'aOPCy prévoyait, à son entrée en vigueur en 2020, un Groupe Cyber. Ce groupe était composé du délégué à la cybersécurité représentant le DFF et présidant le groupe, d'une représentante du DDPS, d'une autre du DFJP ainsi que d'une représentante des cantons désignée par la conférence des gouvernements cantonaux, ce groupe évalue les menaces et les dispositifs de sécurité et surveille la gestion des graves cyberincidents (art. 8 aOPCy)[426]. La participation des représentantes des trois domaines de la cybersécurité (DFF), de la poursuite pénale (DFJP) et de la cyberdéfense (DDPS) était nécessaire, puisque le Groupe avait pour mission importante d'évaluer les cyberrisques et leur évolution au sein des trois domaines[427]. En outre, les trois domaines de la protection contre les cybermenaces étant dépendants les uns des autres, il était nécessaire de les inclure dans une collaboration étroite[428]. Le Groupe 221

424 FF 2023 84, p. 13 et 26. Une fois les divers signalements réceptionnés, le NCSC est compétent pour les traiter et pour leur donner la suite appropriée.

425 FF 2017 2765, p. 2840.

426 DFF, *Erläuterungen zur Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung*, 2020, p. 3.

427 Art. 8 al. 5 aOPCy ; CF, *Rapport « La politique de sécurité de la Suisse »*, 2021, p. 35. Par exemple, les découvertes méthodologiques et techniques sur des modèles d'attaques doivent être partagées ; DFF, *Erläuterungen zur Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung*, 2020, pp. 3, 4.

428 DDPS, *Stratégie Cyber VBS*, 2021, p. 17.

Cyber évaluait également continuellement les dispositifs en place dans les trois domaines et demandait au CF de prendre les mesures qui s'imposaient[429]. Il accompagnait en outre la gestion interdépartementale des incidents et informait le Groupe Sécurité (GS) de la Confédération des incidents ainsi que des développements relatifs à la politique extérieure et de sécurité, afin de maintenir une cohérence (art. 8 al. 4 litt. c, d aOPCy).

222 Le Comité de pilotage était responsable sous le régime de l'aOPCy du contrôle et de la mise en œuvre de la CSN[430]. Mis en place par le CF, il était composé notamment du délégué à la cybersécurité, de représentantes des cantons, des milieux économiques, de chaque département et des hautes écoles. Cette composition visait à assurer une implication de toutes les actrices concernées[431]. Parmi ses compétences, le comité de pilotage veillait à la cohérence de la mise en œuvre de la SNPC par le biais d'un contrôle de gestion stratégique et pouvait proposer des mesures d'urgence en cas de besoin. Il assurait le développement de la stratégie conjointement au Groupe Cyber, informait régulièrement le CF et les cantons de l'avancement et veillait à l'adoption d'une approche coordonnée entre les secteurs ainsi qu'à l'imbrication de la CSN avec les autres stratégies nationales, à l'instar de la Stratégie PIC et de la politique de gestion des risques de la Confédération (art. 9 al. 4 aOPCy)[432].

223 Le comité pour la sécurité informatique était composé d'une représentante du NCSC, des déléguées à la sécurité informatique des départements et de la Chancellerie fédérale ainsi que de la déléguée à la sécurité informatique des services standards TIC. Il constituait « l'organe consultatif du NCSC pour les questions de sécurité informatique dans l'administration fédérale » (art. 10 aOPCy).

224 La loi ne fait plus mention de ces autorités et attribue certaines compétences similaires au nouvel OFCS. Il est donc difficile de savoir ce qu'il est advenu début 2024 du Groupe Cyber, du comité de pilotage et du comité pour la sécurité informatique, mais il n'est pas exclu que ces différentes entités existent encore sans être expressément prévues par la loi. Le cadre légal devrait être plus clair quant à leurs compétences si elles existent encore[433].

429 Cff, *Audit de l'efficacité de la lutte contre la cybercriminalité*, 2021, p. 39 ; DFF, *Erläuterungen zur Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung*, 2020, p. 4.

430 CF, *CSN*, 2023, p. 35.

431 CF, *CSN*, 2023, p. 10 ; DDPS, *Stratégie Cyber VBS*, 2021, p. 17 ; DFF, *Erläuterungen zur Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung*, 2020, p. 4.

432 Cf. CF, *CSN*, 2023, p. 10. Ses tâches devraient être à nouveau prévues dans l'OCyS, cf. art. 5 P-OCyS.

433 Il n'est pas exclu que l'OSI prévoie dans sa version révisée ces différentes autorités si elles existent encore.

3. La situation depuis janvier 2024

a. La création de l'Office fédéral de la cybersécurité

Le nouvel office pour la cybersécurité, opérationnel à partir du 1er janvier 2024[434], est le résultat d'une transformation du NCSC. L'art. 15*a* al. 1 Org-DDPS prévoit par ailleurs que l'OFCS est le NCSC. Il reste le centre fédéral de compétences en matière de cybersécurité[435]. Il continue à détenir certaines compétences du NCSC ainsi que des différents services de ce dernier[436]. Officiellement, son mandat est toujours le même, à savoir la protection de la Suisse face aux cybermenaces[437]. 225

La mission de l'OFCS repose sur les quatre piliers stratégiques suivants : la vulgarisation des cybermenaces, la mise à disposition de moyens empêchant les cyberattaques, la réduction des dommages dus aux cyberincidents et l'augmentation de la sécurité des produits et prestations numériques. Premièrement, la vulgarisation des cybermenaces doit d'une part permettre un dialogue entre le monde politique, l'économie et la société au sujet de la cybersécurité, et d'autre part responsabiliser les différents groupes concernés. Deuxièmement, l'OFCS alerte au sujet des cyberattaques, fournit différentes informations ainsi que des instruments pour éviter ces attaques. Troisièmement, l'office soutient les organisations et les personnes touchées par des cyberincidents pour limiter les dommages ainsi que les risques d'extension de la menace à d'autres victimes. Quatrièmement, l'augmentation de la sécurité des produits et des prestations numériques passe par l'incitation des prestataires de services informatiques à être transparentes et à proposer des produits et services sûres à des prix abordables[438]. 226

En tant qu'autorité principale pour la cybersécurité, l'OFCS coordonne les travaux de cybersécurité, élabore la cyberstratégie suisse pour le CF et coordonne sa mise en œuvre (art. 15*a* al. 2 litt. g Org-DDPS). Il est compétent pour réaliser des analyses techniques des cybermenaces et pour les évaluer ainsi que pour identifier et éliminer les vulnérabilités pour protéger le pays (art. 73*a* al. 1 LSI2 et 15*a* al. 2 litt. b Org-DDPS). Il conserve la tâche de réceptionner les cybermenaces signalées auparavant au NCSC et en vertu de la nouvelle obligation de signaler les cyberattaques (art. 73*a* al. 1 lit. d et 73*b* al. 1 LSI2 et 227

434 OFCS, *Rapport semestriel 2023/II*, 2024, p. 4 s.

435 SG-DDPS, *Législation d'exécution relative à la LSI, Explications*, 2023, p. 25.

436 DDPS, *Änderung der Organisationsverordnung für das VBS: Staatssekretariat für Sicherheitspolitik und Bundesamt für Cybersicherheit*, 2023, p. 3.

437 OFCS, *Rapport semestriel 2023/II*, 2024

438 OFCS, *Rapport semestriel 2023/II*, 2024, p. 5 ss ; OFCS, *Stratégie de l'OFCS*, 2023, p. 4 ss.

15*a* al. 2 litt. c Org-DDPS)[439]. C'est également à l'OFCS que revient la tâche de publier des informations sur les cyberincidents pour la protection de la Suisse contre les cybermenaces et d'alerter les autorités, les organisations et la population sur les cybermenaces immédiates ou les cyberattaques en cours (art. 73*a* al. 2 lit. b et c LSI2, art. 15*a* al. 2 litt. d et e Org-DDPS). Finalement, l'OFCS soutient les infrastructures critiques (art. 73*a* al. 2 litt. e et 74 LSI2, art. 15*a* al. 2 litt. f Org-DDPS) ; il exploite GovCERT pour cela (art. 15*a* al. 2 litt. f Org-DDPS). L'office fédéral devrait également continuer de conseiller et soutenir la Confédération dans les questions de cybersécurité, ainsi que d'émettre des directives techniques[440].

228 L'OFCS détient également certaines compétences pour la sécurité de l'information au sein de la Confédération. Le nouvel art. 43 OSI établit une liste de compétences pour le nouvel OFCS en relation avec la sécurité de l'information au sein de la Confédération[441]. L'office conseille l'administration fédérale, l'armée et les organes de sécurité des art. 81 à 83 LSI pour la sécurité technique de l'information (art. 43 al. 1 litt. a OSI). Il peut également effectuer des recherches de menaces et de vulnérabilités techniques sur Internet ou, avec l'accord des responsables de la sécurité de l'information et des fournisseuses de prestations, dans l'infrastructure informatique de l'administration fédérale. Cette recherche sert à évaluer et à améliorer la situation en matière de sécurité technique de l'information de la Confédération (art. 43 al. 1 litt. c OSI)[442]. Il conserve la compétence du NCSC d'élaborer des directives à l'attention de la Confédération jusqu'à 2025 (art. 51 al. 6 OSI qui renvoie notamment à l'art. 27 al. 7 ou à l'art. 29 al. 1 OSI)[443]. Son rôle et ses compétences seront approfondies plus tard[444].

229 L'ancien délégué du NCSC Florian Schütz est maintenant directeur de l'OFCS. Il est directement subordonné à la cheffe du DDPS. Il maintient son

439 DDPS, *Änderung der Organisationsverordnung für das VBS: Staatssekretariat für Sicherheitspolitik und Bundesamt für Cybersicherheit*, 2023, p. 5 s.

440 SG-DDPS, *Législation d'exécution relative à la LSI, Explications*, 2023, p. 5. Pour un exemple de directive, cf. NCSC, *Si001*, 2022.

441 La Confédération est l'une des « clientes » de l'OFCS, cf. SG-DDPS, *Législation d'exécution relative à la LSI, Explications*, 2023, p. 25.

442 Cette tâche peut être déléguée à des personnes tierces, notamment par des programmes de primes aux bogues, cf. SGDDPS, *Législation d'exécution relative à la LSI, Explications*, 2023, p. 25.

443 SG-DDPS, *Législation d'exécution relative à la LSI, Explications*, 2023, p. 20. À partir de 2025, c'est le service spécialisé de la Confédération pour la sécurité de l'information qui reprendra ces tâches (art. 51 al. 6 OSI et les dispositions auxquelles il renvoie), cf. *infra* N 781.

444 Cf. *infra* N 703 ss.

rôle d'interlocuteur des milieux politiques, des médias et de la population pour toute question de cybersécurité. Il est toujours responsable de la mise en œuvre coordonnée de la CSN[445].

b. L'organisation au sein du Conseil fédéral

Le CF est à la tête de la cybersécurité et des domaines connexes. Dans le contexte de la protection de la Suisse contre les cybermenaces et compte tenu du nombre important d'intervenantes dans le domaine et de l'évolution rapide des cybermenaces, le CF doit disposer d'informations sur la mise en œuvre de la stratégie nationale et sur les dispositions en vigueur pour pouvoir les adapter si nécessaire[446]. Il détient qui plus est des compétences législatives et réglementaires, qu'il utilise particulièrement en adoptant des actes d'exécution de la LSI. 230

Le CF a renoncé à la création de la Délégation pour la cybersécurité (Délégation Cyber) et a attribué en 2023 les affaires de cybersécurité touchant à la politique de sécurité à la Délégation du CF pour la sécurité (Délséc)[447]. La Délséc a comme tâches l'évaluation de la situation dans le domaine de la sécurité, la coordination des affaires interdépartementales de politique de sécurité, l'attribution des missions au GS et la préparation des affaires de politique de sécurité en vue des décisions du CF (art. 1.2 des Directives sur l'organisation de la conduite de la politique de sécurité du CF)[448]. Les questions politiques liées à la protection contre les cybermenaces tombent maintenant dans ces compétences. Le GS est chargé, sur un plan politique, de présenter et évaluer la situation ainsi que d'anticiper les défis dans le domaine de la sécurité. Il coordonne les affaires au niveau opérationnel et à celui de la politique de sécurité (art. 2.2 al. 1 et 2 des Directives sur l'organisation de la conduite de la politique de sécurité du CF)[449]. 231

4. Un résumé des changements pour la cybersécurité

Le NCSC, transformé en OFCS, comptait différents services, dont certains sortent de l'objet de la présente étude[450]. Le NCSC était rattaché au DFF, et ses différents services étaient administrativement rattachés tantôt au DFF, tantôt 232

445 OFCS, *Le directeur de l'Office fédéral de la cybersécurité*.

446 DFF, *Erläuterungen zur Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung,* 2020, p. 3.

447 DDPS, ***Stratégie Cyber VBS,*** 2021, p. 18 ; CF, *Politique de sécurité et cyberrisques : le Conseil fédéral renforce la coordination interdépartementale*.

448 CF, *Délégation du Conseil fédéral pour la sécurité,* 2023, p. 1 ; FF 2023 241, p. 1s.

449 FF 2023 241, p. 3.

450 Il en va de la sorte pour les pools d'expertes ou de la cyberdiplomatie.

au Département fédéral de justice et police (DFJP) ou au DDPS. MELANI avait été intégrée au NCSC à sa création en 2019 et les services qui la composait étaient GovCERT, le point de contact ou guichet unique du NCSC, MELANI OIC, OSINT et NEDIK.

233 En janvier 2024 et au plus haut niveau hiérarchique, le CF a renoncé à la création de la Délégation pour la cybersécurité (Délégation cyber du CF). Il a attribué les affaires touchant à la politique de sécurité à la Délséc. La loi ne fait ensuite plus mention du comité de pilotage ou du Groupe Cyber[451]. L'ancien délégué à la cybersécurité, à la tête du NCSC, est maintenant le directeur de l'OFCS.

234 Depuis janvier 2024, la transformation du NCSC en OFCS a entraîné plusieurs conséquences en termes de cybersécurité. MELANI OIC, OSINT et le NEDIK ne font plus partie de l'office. Il a en revanche conservé le point de contact ou guichet central, le service de gestion des vulnérabilités et GovCERT. De nouveaux services ont également vu le jour en termes de prévention et d'analyse, ainsi qu'en termes de planification et de contrôle.

Schéma 6 : l'autorité principale pour la cybersécurité de 2019 à décembre 2023[452]

Jusqu'à décembre 2023

Délégation cyber du Conseil fédéral		
Groupe Cyber	Délégué à la cybersécurité	Comité de pilotage

Centre national pour la cybersécurité (NCSC)			
Direction			
MELANI	Pool d'expertes	Autoprotection	Cyberdiplomatie
Point de contact	Pool central	Gestion des vulnérabilités	Bureau cyber
GovCERT	Experts d'offices spécialisés		
MELANI OIC	…	IKT-SEC	
OSINT			
NEDIK			

451 Néanmoins, les art. 3 ss P-OCyS devraient réintégrer le comité de pilotage de la CSN.

452 Schéma basé sur les archives de l'OFCS et sur l'organisation de la Confédération pour les cyberrisques, cf. notamment CF, *Plan de mise en œuvre de la SNPC 2018-2022*, 2019, p. 6.

Schéma 7 : l'autorité principale pour la cybersécurité à partir de janvier 2024[453]

Depuis janvier 2024	~~Délégation cyber du Conseil fédéral~~ → Délégation du CF pour la sécurité

Office fédéral de la cybersécurité (OFCS)			
Direction			
Cybersécurité opérationnelle	**GovCERT**	Analyse et prévention	Planification et contrôle
Point de contact	**GovCERT**	Gouvernance et conformité	Développement d'affaires
		Technologie et ingénierie de sécurité	
Gestion des vulnérabilités		Analyse	Ressources
Services plateforme		Sensibilisation	Gestion de l'information et secrétariat

B. La poursuite pénale de la cybercriminalité

1. Le département fédéral compétent

La poursuite pénale de la cybercriminalité constitue le second domaine de la protection contre les cyberrisques. Elle réunit les autorités de poursuite pénale des cantons et de la Confédération actives dans la lutte contre la cybercriminalité, sous le couvert, au niveau fédéral, du DFJP[454]. 235

2. Les autorités de poursuite pénale

Les autorités de poursuite pénale, plus précisément les forces de police et les ministères publics, constituent l'autorité principalement compétente pour la lutte contre la criminalité, pour la prévention des dangers et pour la mise en pratique de mesures par l'usage direct de la contrainte. La poursuite pénale de la cybercriminalité incombe souvent aux autorités de poursuite pénale cantonales, conjointement aux forces de police communales[455]. Néanmoins, certains cas relèvent de la compétence fédérale, à savoir celle du Ministère 236

453 Schéma basé sur l'organigramme transmis par l'OFCS.

454 DDPS, *Stratégie Cyber VBS*, 2021, p. 18.

455 CF, *Rapport « La politique de sécurité de la Suisse »*, 2021, p. 29 ; CR Cst.-BLEICKER, art. 57 N 21.

public de la Confédération (MPC) et de l'Office fédéral de la police (fedpol) (art. 23 s. CPP). Tel est le cas pour la lutte contre la grande criminalité, plus précisément le terrorisme, l'extrémisme violent, la criminalité organisée ou transnationale[456]. En outre, fedpol constitue le point de contact international en plus d'être l'office central[457]. Il détient à ce titre d'autres compétences dans ce cadre[458].

3. D'autres entités compétentes

237 Le domaine de la lutte contre la criminalité existe en Suisse depuis longtemps, mais d'autres entités sont pourvues de compétences se recoupant avec la cybercriminalité. Le domaine de direction « Entraide judiciaire internationale », autorité centrale pour l'entraide judiciaire internationale en matière pénale, intégrée à l'Office fédéral de la Justice (OFJ), a reçu en 2021 plus de requêtes étrangères qu'auparavant dans un contexte de poursuite pénale de la cybercriminalité[459].

238 D'autres entités ont été mises en place plus récemment afin de répondre plus adéquatement à la menace relative à la cybercriminalité. Le *Cyberboard* est l'organe de coordination des représentantes de prévention et des autorités de poursuite pénale cantonales et fédérales actives pour les questions de cybercriminalité[460]. Le *Cyberboard* contient aujourd'hui deux modules. Tout d'abord, il y a le Cyber-STRAT, organe stratégique de la plateforme, qui regroupe les directions des actrices actives dans la lutte contre la cybercriminalité. À ce titre, il réunit notamment des représentantes du NCSC, de fedpol, de la Conférence des procureures suisses, du MPC et du NEDIK. Le second module du *Cyberboard* est le Cyber-CASE, organe opérationnel réunissant régulièrement les procureures et enquêtrices cantonales et fédérales ainsi que des représentantes du NCSC afin de coordonner des procédures et échanger des informations et expérience dans le domaine[461]. Le *Cyberboard* élabore une vue

456 CF, *Rapport « La politique de sécurité de la Suisse »,* 2021, p. 29 s. ; RNS, *Recommandations de mise en œuvre des organisations cantonales pour la cybersécurité,* 2021, p. 15.

457 CF, *Rapport « La politique de sécurité de la Suisse »,* 2021, p. 30 ; DDPS, *Stratégie Cyber VBS,* 2021, p. 18 ; RNS, *Recommandations de mise en œuvre des organisations cantonales pour la cybersécurité,* 2021, p. 15.

458 Cff, *Audit de l'efficacité de la lutte contre la cybercriminalité,* 2021, p. 5 et 30.

459 OFJ, *Rapport d'activité 2021,* 2022, p. 11.

460 Il collaborait avec le Groupe Cyber dans le cadre de la poursuite pénale, cf. CF, *Rapport « La politique de sécurité de la Suisse »,* 2021, p. 36 ; Cff, *Audit de l'efficacité de la lutte contre la cybercriminalité,* 2021, p. 39 . Pour une vue d'ensemble des autorités compétentes, voir GCSCC, *Cybersecurity capacity review – Switzerland,* 2020, p. 16.

461 GCSCC, *Cybersecurity capacity review – Switzerland,* 2020, p. 61 s. ; RNS, *Recommandations de mise en œuvre des organisations cantonales pour la cybersécurité,* 2021, p. 28 ; NICOLET/PEISSARD, p. 173.

d'ensemble judiciaire des infractions et participe, par le biais de NEDIK, à la présentation de l'évolution de la cybercriminalité et de ses conséquences[462].

239 Le NEDIK est un regroupement des forces de police qui lutte contre la cybercriminalité de manière concertée[463]. Il assure notamment le transfert de connaissance, l'établissement d'un aperçu national des cas et la classification des cas présentant un caractère intercantonal[464]. Dans ce cadre, la Confédération, par son représentant fedpol, collabore étroitement avec les cantons par la CCPS[465]. Le réseau national de soutien aux enquêtes dans la lutte contre la cybercriminalité est composé des corps de police qui observent, collectent des informations et mènent des enquêtes préliminaires sur les infractions commises sur Internet et sur le *darknet,* en application de la loi sur la police[466]. Le NEDIK a aussi une mission importante de coordination de la collaboration pour la lutte contre la criminalité informatique, au niveau national comme international, ainsi qu'une mission de prévention en collaboration avec la Prévention suisse de la Criminalité (PSC) et le NCSC[467]. Le NEDIK était jusqu'à décembre 2023 hébergé par le NCSC mais rattaché à l'organisation intercantonale. Il ne fait plus partie de l'OFCS mais existe encore, vraisemblablement comme organisation intercantonale. La CSN de 2023 lui confie par ailleurs des responsabilités[468].

240 D'autres services, unités et entités disposent de compétences dans la lutte contre la cybercriminalité, à l'instar du *Cyber Competence Center* (RC3) régional qui contribue avec le NEDIK à renforcer la collaboration entre les polices cantonales[469], du Service national de coordination de la lutte contre la criminalité sur Internet (SCOCI) qui coordonne les tâches relevant de la surveillance Internet pour mieux lutter contre la cybercriminalité, ou du service de surveillance de la correspondance par poste et télécommunication (SCPT), dont l'activité sera abordée lors de l'analyse des règles applicables à

462 CF, *Plan de mise en œuvre de la SNPC 2018-2022,* 2019, p. 51.

463 OFCS, *Rapport semestriel 2023/II,* 2024, p. 14.

464 CF, *Rapport sur l'avancement des travaux concernant la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022,* 2021, p. 6.

465 CF, *Plan de mise en œuvre de la SNPC 2018-2022,* 2019, p. 52.

466 PSC, *INFO 2/2021,* 2021, p. 10 et 12 ; CR Cst.-BLEICKER, art. 57 N 22 ; TEICHMANN/GERBER, *La qualification pénale des attaques DDoS en droit suisse,* 2021, N 9.

467 CF, *CSN,* 2023, p. 29 ; CF, *Rapport sur l'avancement des travaux concernant la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022,* 2021, p. 6 ; PSC, *INFO 2/2021,* 2021, p. 11 s.

468 Par exemple dans l'attribution des cyberattaques ou dans la collaboration entre les autorités de poursuite pénale, cf. CF, *CSN,* 2023, p. 25 et 29.

469 CF, *CSN,* 2023, p. 29.

la poursuite de la criminalité dans le cyberespace[470]. De la même manière que pour la cybersécurité, nous sommes face à un nombre important de structures étatiques impliquées dans la lutte contre la cybercriminalité[471].

C. La cyberdéfense

1. Le département fédéral compétent

241 Pour la cyberdéfense, dernière composante des mesures de protection contre les cyberrisques, le DDPS détient les compétences originaires[472]. Ces compétences sont partagées en quatre secteurs : la lutte contre le renseignement prohibé, la lutte contre le terrorisme, la protection des infrastructures critiques et la défense militaire[473]. À noter que les compétences du DDPS, comme celles du SRC et de l'armée sont subsidiaires lorsqu'il en va du soutien apporté aux infrastructures critiques[474].

242 Le DDPS occupe un rôle toujours plus important dans la protection de la Suisse contre les cybermenaces. Le Secrétariat général du DDPS (SG-DDPS) détenait jusqu'à fin 2023 une partie importante des compétences nouvellement attribuées au service spécialisé de la Confédération pour la sécurité de l'information au sens de l'art. 83 LSI et des dispositions correspondantes dans l'OSI[475]. Les secrétariats du GS et de la Délégation Cyber sont assurés par le DDPS (art. 1.3 al. 1 2.3 al. 1 des Directives sur l'organisation de la conduite de la politique de sécurité du Conseil fédéral), qui constitue donc le département abritant les compétences principales en matière politique pour la protection de la Suisse contre les cybermenaces.

243 Outre ces compétences concernant spécifiquement la cyberdéfense, le DDPS est, comme toute autre unité de l'administration fédérale, responsable de sa protection et de sa défense. En outre, il est intéressant de soulever que le département héberge aujourd'hui également des autorités civiles, soit des autorités autres que l'armée compétente pour la défense du pays[476].

470 Cf. *infra* N 586 s.

471 Pour une représentation de ces actrices, voir CF, *Poursuites pénales en matière de cybercriminalité*, 2024, p. 9 ss.

472 Pour une liste des autorités compétentes, cf. GCSCC, *Cybersecurity capacity review – Switzerland*, 2020, p. 16.

473 DDPS, *PACD*, 2017, p. 6 s. ; DDPS, *Stratégie Cyber VBS*, 2021, p. 18.

474 DDPS, *Stratégie Cyber VBS*, 2021, p. 2 et 25 ss.

475 SG-DDPS, *Législation d'exécution relative à la LSI, Explications*, 2023, p. 10.

476 Comme auparavant MELANI OIC et désormais l'OFCS ; DDPS, *Stratégie Cyber VBS*, 2021, p. 27 ; DDPS, *PACD*, 2017, p. 8 et 14 ss.

2. Le service du renseignement

Le SRC a pour mission principale de rechercher et de traiter des informations pour déceler et prévenir des menaces pour la sûreté intérieure ou extérieure liées au terrorisme, à l'extrémisme violent, à l'espionnage, la prolifération d'armes de destruction massive et aux cyberattaques ciblant les infrastructures critiques[477]. Il détecte, observe, collecte et évalue des événements importants, à l'instar des cybermenaces, assure la capacité d'action de la Suisse et sauvegarde également d'autres intérêts importants (art. 6 al. 1 LRens). Le SRC est l'une des autorités concernées par la SNPC, avec son unité Cyber SRC[478]. C'est typiquement à cette unité d'organisation qu'incombent certaines tâches dévolues au SRC en lien avec les cyberrisques[479]. 244

L'une des tâches principales du SRC est l'attribution d'attaques à leurs auteures[480]. À cette fin, il obtient des informations, provenant de sources publiques ou non, analyse de manière approfondie les acteurs de l'environnement, utilise les instruments techniques à sa disposition et surveille les télécommunications[481]. 245

Lorsque le SRC agit pour soutenir les infrastructures critiques dans le cyberespace, c'est son unité cyber qui est visée. Elle collecte des informations au sujet de certaines cyberattaques[482]. Ses compétences risquent de se croiser avec celles de l'OFCS et de GovCERT, mais le SRC intervient de façon subsidiaire et est en principe spécialisé en ce qui concerne l'espionnage et les attaques impliquant des actrices étatiques[483]. Le plan d'action de cyberdéfense du DDPS, repris ensuite par la cyberstratégie du DDPS, prévoit qu'il peut agir en collaboration avec l'armée dans le cadre de la prévention auprès des infrastructures critiques, en vue de les aider à pourvoir à leur protection. Au-delà de cette compétence de prévention, le SRC peut prêter une assistance réactive aux infrastructures critiques en cas de cyberattaque, au besoin avec 246

477 CF, *Rapport « La politique de sécurité de la Suisse »*, 2021, p. 29.

478 CF, *Rapport « La politique de sécurité de la Suisse »*, 2021, p. 31 ; CR Cst.-BLEICKER, art. 57 N 20.

479 UPIC, *Rapport « évaluation de l'efficacité de la stratégie nationale de protection contre les cyberrisques (SNPC) »*, 2016, p. 41.

480 CF, *CSN*, 2023, p. 25.

481 Parfois en collaboration avec le BAC, DDPS, *Stratégie Cyber VBS*, 2021, p. 35.

482 OBERHOLZER, *Bericht der Administrativuntersuchung – Auszug aus den Empfehlungen und der rechtlichen Beurteilung des Schlussberichts*, 2022, p. 3.

483 OBERHOLZER, *Bericht der Administrativuntersuchung – Zusammenfassung der wesentlichen Erkenntnisse*, 2022, p. 2.

des contre-mesures offensives, à condition d'avoir obtenu les autorisations pour ce faire (art. 26 al. 1 litt. d ch. 2 LRens)[484].

3. L'armée et le commandement Cyber

247 L'armée défend les intérêts du pays. Elle participe à la maîtrise des menaces dont l'intensité et l'ampleur mettent en danger l'intégrité territoriale du pays, l'exercice du pouvoir étatique ou l'ensemble de la population[485]. Alors qu'elle doit principalement être apte à affronter une attaque armée, elle apporte avec le SRC un soutien pour la protection et la défense des autorités civiles dans la maîtrise de situations de crises au sens large ainsi que des infrastructures critiques[486].

248 Le développement de sa résilience est recherché, avec un accent sur l'appui subsidiaire qu'elle peut fournir[487]. Le commandement Cyber (anciennement Base d'aide au commandement, BAC)[488] est rattaché au Groupement Défense et cherche à anticiper les risques pour la défense du pays dans le cyberespace. Il mène également des actions ciblées dans le cyberespace pour affaiblir la capacité de conduite d'adversaires[489].

249 Le commandement Cyber fournit aussi des prestations dans le domaine des TIC au DDPS. C'est à lui que revient la compétence d'exploiter les services et applications TIC du DDPS[490]. Il organise les capacités militaires principales pour disposer d'une vue d'ensemble de la situation en ce qui concerne la cyberdéfense, les prestations informatiques, l'aide au commandement, la cryptologie, la guerre électronique[491]. À ce titre, sa compétence principale est le soutien en cas de cyberattaques, en temps normal comme en temps de crise ou de conflit. Ses compétences d'action dans le cyberespace sont fondées sur l'art. 4 al. 2 OCMil.

484 DDPS, *Stratégie Cyber VBS,* 2021, p. 27 ; DDPS, *PACD,* 2017, p. 15 ; SRC, *Le SRC,* 2013, p. 5 et 17. En 2021, aucune mesure n'a été autorisée et avalisée en ce qui concerne des attaques visant des infrastructures critiques, SRC, *La sécurité de la Suisse*, 2022, p. 86.

485 CF, *Rapport « La politique de sécurité de la Suisse »,* 2021, p. 29.

486 CF, *Rapport « La politique de sécurité de la Suisse »,* 2021, p. 29 ; DDPS, *Stratégie Cyber VBS,* 2021, p. 27 ; DDPS, *PACD,* 2017, p. 8 et 15 ss.

487 CF, *Rapport « La politique de sécurité de la Suisse »,* 2021, p. 34.

488 DDPS, *Stratégie Cyber VBS,* 2021, p. 32 ; ChF, *Rapport « Suisse 2035, les grands défis de demain en 20 questions »,* 2022, p. 110.

489 CF, *Capacité de défense et coopération*, 2024, p. 8.

490 Cff, *Audit de l'impact de l'intégration de l'exploitation de la BAC dans l'OFIT en termes de fiabilité*, 2023, p. 17.

491 FF 2021 2198, p. 18.

4. Les autres entités compétentes

L'existence de MELANI OIC était établie jusqu'à la transformation du NCSC en OFCS. Elle occupait un rôle de coordinatrice opérationnelle entre les actrices fédérales du domaine de la cybersécurité et les infrastructures critiques. Elle était rattachée au SRC mais faisait administrativement partie des unités du NCSC. MELANI OIC servait à l'analyse des menaces, aux échanges d'informations parmi plusieurs centaines d'infrastructures critiques (y compris l'armée et les fournisseuses de prestations de l'administration fédérale) et à l'appui opérationnel et analytique en cas de cyberincident, à condition qu'un incident ne puisse pas être résolu dans le cadre de gestion courante des incidents ou qu'il s'agisse d'un incident menaçant également d'autres organisations[492]. Il est probable que la structure existe encore, bien que la LSI et son ordonnance n'en disent rien. 250

La première étape de recherches, dans un cadre de renseignement, consiste en la recherche d'informations provenant de sources non classifiées et accessibles au public. La recherche, la sélection et le traitement de telles informations étaient jusqu'à fin 2023 effectués dans le cadre d'OSINT, faisant alors partie du NCSC. Les sources les plus utilisées sont souvent Internet, les publications ou médias ainsi que les banques de données accessibles[493]. À noter que la Suisse prévoyait déjà en 2019 un renforcement des capacités d'OSINT[494]. La Stratégie Cyber du DDPS prévoit toujours un renforcement du domaine OSINT, sans précision quant aux autorités et services concernés[495]. 251

Parmi les autorités dont on peut trouver des traces depuis la nouvelle CSN, le *Cyber-Defence Campus* d'armasuisse (CYD Campus) détient tout d'abord des compétences importantes pour la protection contre les vulnérabilités. Il collabore avec les hautes écoles et les milieux économiques pour l'innovation et pour la mise en place de monitorage de vulnérabilités présentes dans les technologies de cybersécurité, en particulier pour le DDPS[496]. Il devrait également participer aux analyses de risques inhérents aux produits TIC lors des 252

492 DDPS, *PACD,* 2017, p. 11 ; SRC, *Le SRC,* 2013, p. 17 ; RNS, *Recommandations de mise en œuvre des organisations cantonales pour la cybersécurité,* 2021, p. 15. À l'avenir, l'unité sera amenée à développer encore davantage ses capacités de soutien aux infrastructures critiques, cf. DDPS, *Stratégie Cyber VBS,* 2021, p. 33.

493 SRC, *Le SRC,* 2013, p. 25.

494 CF, *Plan de mise en œuvre de la SNPC 2018-2022,* 2019, p. 21 et 77.

495 DDPS, *Stratégie Cyber VBS,* 2021, p. 20.

496 CF, *CSN,* 2023, p. 14 et 17 ss ; DDPS, *Stratégie Cyber VBS,* 2021, p. 20 et 33 ss.

préparatifs en vue d'un achat et de l'acquisition de tels produits lorsqu'ils sont critiques pour la sécurité de la Confédération[497].

D. Les autorités compétentes issues d'autres domaines

1. Le SEPOS

253 Le SEPOS a été créé en janvier 2024. Il a pour missions de veiller à ce que la Confédération dispose des bases conceptuelles pour mener une politique de sécurité cohérente, de garantir une politique de sécurité globale sur le plan stratégique et de veiller à la sécurité de l'information pour la Confédération (art. 7 al. 1 Org-DDPS). Il compte en son sein notamment le nouveau service spécialisé de la Confédération pour la sécurité de l'information (art. 7 al. 2 litt. e ch. 1 Org-DDPS). Ce service spécialisé reprend les tâches du NCSC et du SG-DDPS pour ce qui est de l'autoprotection de la Confédération en matière de sécurité de l'information[498]. Cette autorité détient principalement des compétences liées à la sécurité de l'information pour l'administration fédérale et l'armée, dont l'élaboration de stratégies, la participation à la formation ou la représentation de la Suisse sur le plan international pour la sécurité de l'information de la Confédération (art. 42 OSI)[499]. Il reprendra la compétence d'élaborer des directives pour la sécurité de l'information et la sécurité des moyens informatiques pour la Confédération dès 2025 (art. 51 al. 6 OSI et les dispositions auxquelles il renvoie).

254 Le service spécialisé de la Confédération pour la sécurité de l'information devra collaborer étroitement avec l'OFCS pour les questions ayant trait à la cybersécurité, surtout lorsque l'administration fédérale est concernée. Par exemple, l'OFCS et le service spécialisé de la Confédération pour la sécurité de l'information vont coopérer dans la gestion de cyberincidents impactant la Confédération (art. 12 OSI)[500].

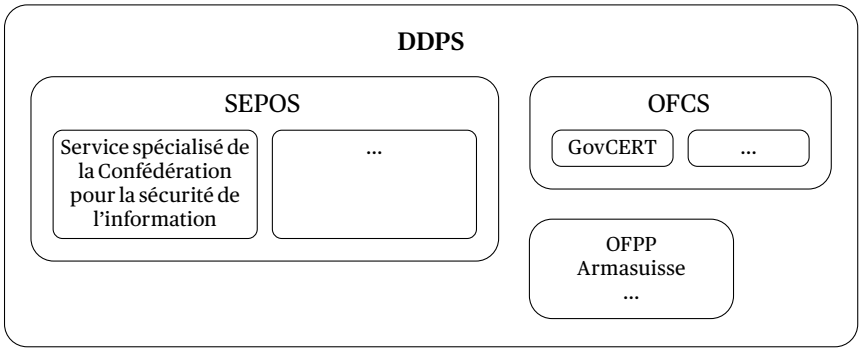
497 CF, *CSN*, 2023, p. 18 ; CF, *Rapport « Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense »*, 2021, p. 19.

498 SG-DDPS, *Législation d'exécution relative à la LSI, Explications,* 2023, p. 5.

499 Le service spécialisé de la Confédération pour la sécurité de l'information dispose d'autres compétences dispersées dans l'OSI, cf. SG-DDPS, SG-DDPS, *Législation d'exécution relative à la LSI, Explications,* 2023, p. 24.

500 Pour plus d'informations sur cet enchevêtrement de compétences, cf. *infra* N 781 ss. Pour des perspectives d'avenir sur la question, cf. *infra* N 1419 ss.

Schéma 8 : l'organisation du DDPS pour la cybersécurité et la sécurité de l'information dès 2024[501]



2. Le secteur TNI

Le secteur Transformation numérique et gouvernance de l'informatique (TNI) de la ChF a été créé en 2020, lors de la réorganisation par le Conseil fédéral du domaine[502]. L'OTNI, qui a remplacé l'Ordonnance sur l'informatique dans l'administration fédérale (OIAF), prévoit son organisation et ses compétences (art. 4 OTNI). C'est effectivement cette ordonnance qui sert de base légale pour l'organisation interdépartementale du secteur TNI, qui règle la collaboration entre les institutions de la Confédération en vue d'assurer une numérisation efficace axée sur les besoins de l'économie et des citoyennes. 255

Le secteur TNI de la ChF dispose de compétences pour le numérique et l'informatique au sein de la Confédération. Il veille, par une coordination interdépartementale, à ce que les processus d'affaires, les modèles de données, les applications et les technologies soient définies et mises en œuvre de façon cohérente et efficace par l'administration fédérale[503]. Il définit et gère des instruments pour aider à la gouvernance de l'informatique et à la coordination de la transformation numérique et gère, entre autres, des projets ou programmes relevant de son domaine de compétences (art. 4 OTNI). Il est 256

501 Le DDPS compte naturellement d'autres offices et autorités que le SEPOS et l'OFCS. Qui plus est, d'autres entités que le service spécialisé de la Confédération pour la sécurité de l'information sont rattachées au SEPOS, mais ce service est l'autorité qui nous intéresse principalement dans le contexte de la cybersécurité.

502 Il constitue le centre de compétence pour les questions de numérisation en instruisant, lançant ses projets ou en soutenant ceux des départements et des offices. Il assure également une vue d'ensemble supradépartementale sur les différents projets, les ressources et les prestations administratives de la TNI au sein de l'administration fédérale, cf. AFF, *Manuel de gestion des risques de la Confédération,* 2021, p. 59.

503 SG-DDPS, *Législation d'exécution relative à la LSI, Explications,* 2023, p. 24 s.

également responsable de développer, coordonner et surveiller la Stratégie Suisse numérique et de communiquer sur cette dernière[504]. L'OTNI ne précise pas si l'intervention du secteur TNI se limite à des recommandations et à un travail de coordination ou s'il peut imposer ses choix aux départements ; la formulation de l'ordonnance laisse à penser qu'il se limite à apporter un soutien et à collaborer avec les départements.

257 À noter que le secteur TNI collabore activement avec les autres intervenantes étatiques, notamment avec l'OFCS en ce qui concerne les aspects sécuritaires[505].

3. La Préposée fédérale à la protection des données et à la transparence

258 La Préposée fédérale à la protection des données et à la transparence (PFPDT) est l'autorité indépendante d'application de la Loi fédérale sur la protection des données (LPD) et de la Loi fédérale sur le principe de transparence dans l'administration (LTrans)[506]. Les organes fédéraux et les responsables du traitement et sous-traitantes privées sont soumises à sa surveillance pour leurs traitements de données personnelles[507].

259 Lorsque l'on parle de cybermenaces, la sécurité de données personnelles est régulièrement en jeu. Partant, il faut prendre en considération les différentes autorités impliquées dans les processus. Lors de la survenance d'un cyberincident compromettant des données personnelles et comme nous le verrons plus en détail, la PFPDT est amenée à collaborer avec l'OFCS dans le cadre de l'obligation d'annonce de violations de la sécurité des données[508].

4. D'autres autorités

260 D'autres autorités fédérales, cantonales, communales, intercantonales et intercommunales ou des personnes privées exerçant des tâches publiques sont amenées à œuvrer de près ou de loin pour la protection de la Suisse contre les cybermenaces[509].

504 ChF, *Stratégie Suisse numérique 2023*, 2022, p. 4.

505 ChF, *Transformation numérique et gouvernance de l'informatique (TNI) : le Conseil fédéral confirme la nouvelle organisation*.

506 Il est également l'autorité de surveillance pour la transparence de la Confédération (art. 18 s. LTrans).

507 FF 2017 6565, p. 6638.

508 NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures*, 2022, p. 27 s.

509 Par exemple, le RNS assume un rôle partenarial par le biais de sa déléguée pour coordonner la mise en œuvre des mesures de la CSN entre la Confédération et les cantons ;

L'OFPP contribue à protéger la population globalement. La protection de la population passe par la maîtrise, avec le concours de ses partenaires, d'événements de grande portée, à l'instar de catastrophes ou de situations d'urgence (art. 14 al. 1 Org-DDPS). L'OFPP détient une série de compétences dans ce contexte (art. 14 al. 2 Org-DDPS). Parmi ces compétences, l'office élabore les bases pour la protection des infrastructures critiques (art. 14 al. 2 litt. a in fine Org-DDPS). À ce titre, l'OFPP est l'autorité chargée de nombreuses compétences de soutien pour les infrastructures critiques en Suisse. Cet office est compétent pour l'élaboration de la Stratégie de protection des infrastructures critiques (Stratégie PIC), qui est le document identifiant les infrastructures critiques. L'OFPP tient l'inventaire des infrastructures critiques[510]. L'OFPP collabore notamment avec l'OFAE pour favoriser la résilience des infrastructures critiques au moyen de mesures ciblées[511]. L'OFAE, rattaché au Département fédéral de l'économie, de la formation et de la recherche (DEFR), a notamment comme compétence de diminuer les risques de perturbation de l'approvisionnement en services et en biens d'importance vitale par le biais d'une préparation adéquate et d'une organisation opérationnelle constante de l'économie privée, de la Confédération et des cantons (art. 9 al. 2 litt. a Org DEFR). L'OFAE a typiquement édicté une norme minimale pour améliorer la résilience informatique pour les organisations actives dans l'approvisionnement économique du pays[512]. 261

L'OFIT, administrativement rattaché au Département fédéral des finances (DFF), représente l'une des fournisseuses internes de prestations informatiques de l'administration fédérale. Il fonde son activité sur les art. 16 ss Org DFF et sur l'OTNI pour exister[513]. Il développe et exploite des systèmes et des applications pour sa clientèle, ainsi que des centres de compétences y afférents (art. 17 litt. a à c Org DFF). L'OFIT assure l'interopérabilité technique de la bureautique pour toute l'administration fédérale, collabore avec les organisations actives dans la fourniture de services informatiques ou encore représente la Confédération au sein de ces organisations (art. 17 litt. f à i Org DFF). 262

le RNS a élaboré des recommandations pour la cybersécurité au sein des cantons, cf. CF, *CSN*, 2023, p. 10 ; RNS, *Recommandations de mise en œuvre des organisations cantonales pour la cybersécurité*, 2021, p. 15.

510 FF 2023 1659, p. 3 et 14.

511 RNS, *Recommandations de mise en œuvre des organisations cantonales pour la cybersécurité*, 2021, p. 14.

512 RNS, *Recommandations de mise en œuvre des organisations cantonales pour la cybersécurité*, 2021, p. 14 ; OFAE, *Norme minimale pour améliorer la résilience informatique*, 2023.

513 Les art. 8 ss OTNI mentionnent les fournisseuses internes et externes de prestations informatiques de la Confédération.

L'OFIT est compétent à ce titre notamment pour l'exploitation des services et applications TIC non critiques du DDPS[514]. L'exploitation des systèmes informatiques et le contrôle de la mise en œuvre des projets numériques par l'OFIT constituent des prestations principalement réactives, sur demande des clientes de l'OFIT[515]. Ses prestations peuvent être tournées vers l'administration fédérale (par exemple vers un département ou vers une application interdépartementale) comme vers d'autres services fédéraux ainsi qu'à des organisations tierces aux conditions de la législation sur les finances de la Confédération (art. 18 al. 4 Org DFF). Ses prestations sont facturées à la clientèle (art. 18 Org DFF).

263 Il existe notamment, pour certains secteurs critiques, des autorités de surveillance ou autres entités auxquelles les organisations doivent annoncer les cas de cyberattaques. À titre d'exemple, l'on peut typiquement citer l'Autorité fédérale de surveillance des marchés financiers (FINMA), les organes d'alerte cantonaux ou la Centrale nationale d'alarme (CENAL)[516]. Parmi ces autres entités disposant de certaines compétences, l'on peut également citer le réseau national de sécurité (RNS). Il unifie et coordonne les prestations fournies par l'ensemble des intervenantes pour la sécurité sur le plan national et sur le plan régional[517].

E. Une synthèse

264 Les compétences en matière de cybersécurité de la Confédération sont dispersées mais une évolution majeure a eu lieu ces dernières années. C'est peu avant 2020 que la première autorité principale pour la cybersécurité a été créée : le NCSC. Il comptait en son sein notamment MELANI, la centrale d'enregistrement et d'analyse pour la sûreté de l'information, ainsi que GovCERT, le service national spécialisé dans la gestion technique d'incidents. D'autres compétences étaient attribuées de façon éparse. Au-delà des départements, de la ChF et des unités administratives qui étaient déjà responsables de leur cybersécurité, le groupe cyber avait principalement la mission de coordonner les domaines de la cybersécurité, de la poursuite pénale de la cybercriminalité

514 Cff, *Audit de l'impact de l'intégration de l'exploitation de la BAC dans l'OFIT en termes de fiabilité*, 2023, p. 15.

515 Sa clientèle souhaiterait que l'office occupe un rôle plus proactif en relation avec la numérisation, par exemple par le biais de conseils et d'informations sur des solutions innovantes. Ce souhait devrait conduire à certaines évolutions au sein de l'OFIT et dans les prestations qu'il offre, cf. OFCOM, *Des prestations convaincantes*, « Eisbrecher ».

516 Au sujet de la FINMA, cf. art. 29 al. 2 LFINMA ; FINMA, Circulaire 2018/3, p. 4. Concernant la CENAL et les organes d'alerte cantonaux, voir art. 9 s., 16 LPPCi et 6 ss, 17 ss, 25 s. OProP.

517 CR Cst.-BLEICKER, art. 57 N 50.

et de la cyberdéfense. Le comité de pilotage contrôlait la mise en œuvre de la CSN et le comité de sécurité informatique était l'organe consultatif du NCSC pour la sécurité informatique de l'administration fédérale.

En janvier 2024, le NCSC a été transformé en OFCS. L'OFCS reprend la majeure partie des tâches du NCSC pour la cybersécurité. Florian Schütz, anciennement délégué du NCSC, est maintenant directeur de l'OFCS. L'office fédéral héberge toujours, entre autres, le guichet unique et GovCERT. Les dispositions de l'aOPCy sur le groupe cyber, le comité de pilotage ou le comité de sécurité informatique ont été abrogées, ce qui a pour conséquence que la situation concernant ces autorités n'est plus aussi claire. En revanche, la Délséc est depuis 2023 compétente pour la gestion politique de la sécurité en Suisse. 265

D'autres autorités sont naturellement compétentes dans les autres domaines de la protection contre les cybermenaces. Le département compétent pour la lutte contre la cybercriminalité est le DFJP. Les autorités de poursuite pénale et les tribunaux sont les autorités principales pour la poursuite pénale de la cybercriminalité. D'autres entités existent pour coordonner et optimiser la coopération entre les intervenantes compétentes, à l'instar du *Cyberboard* ou du NEDIK. 266

La cyberdéfense est sous la responsabilité du DDPS (comme la cybersécurité depuis janvier 2024). Le domaine de la cyberdéfense compte des autorités comme le SRC ou l'armée. Le SRC recherche et traite des informations pour déceler et prévenir des menaces importantes pour la sûreté intérieure ou extérieure. Il attribue des attaques à leurs auteures et soutient les infrastructures critiques. L'armée apporte un appui subsidiaire aux infrastructures critiques et doit disposer des compétences pour maîtriser des crises dans des contextes armés. La protection contre les cybermenaces se basant sur la collaboration entre différentes entités, elle compte encore d'autres autorités à l'instar du CYD-Campus pour l'innovation et la protection contre les vulnérabilités. 267

Finalement, le domaine de la cybersécurité est proche d'autres domaines qui supposent d'autres compétences. Il se rapproche de la sécurité de l'information, qui appelle les compétences du nouveau SEPOS et du nouveau service spécialisé de la Confédération pour la sécurité de l'information. Le secteur TNI est compétent pour la coordination du numérique et de l'informatique au sein de l'administration fédérale ou la PFPDT pour la sécurité et la protection des données personnelles. Ces autorités collaborent avec l'OFCS, de la même manière que d'autres autorités, parfois sectorielles, apportant un soutien aux infrastructures critiques. 268

II. Les actrices privées

A. Une contextualisation de la gestion de cyberincidents

269 Nous avons pu constater la multitude d'intervenantes étatiques dans la cybersécurité et, plus largement, la protection contre les cybermenaces. Dans le secteur privé, la diversité d'intervenantes est encore plus importante. Il existe certains rôles privés majeurs dans la cybersécurité ou dans la gestion de cyberincidents. Les compétences en découlant peuvent être intégrées aux organisations responsables de leur cybersécurité ou externalisées.

270 Alors que les compétences sont fortement étatiques en ce qui concerne la défense ou la lutte contre la criminalité, tel n'est pas le cas de la cybersécurité. Elle repose sur la responsabilité propre de tout individu et de toute organisation. Chacune est responsable de sa propre cybersécurité et les autorités n'apportent en principe qu'un soutien subsidiaire et partenarial dans ce domaine[518].

271 Dans la mesure où chaque organisation est responsable de sa propre cybersécurité, il va de soi que l'ensemble de la population, des infrastructures critiques et des autres entreprises détient des compétences importantes dans ce contexte[519]. La responsabilité pour assurer sa propre cybersécurité est générale et dépend de chaque organisation. Cela étant, un type d'intervenante détient des compétences capitales pour la cybersécurité : les prestataires de services de gestion de cyberincidents. Elles font parfois partie des organisations (étatiques ou privées) dont elles protègent les systèmes informatiques et les informations. Dans ce cas, ce sont les organisations au sein desquelles elles sont intégrées qui ont une personnalité juridique. Ces prestataires peuvent également être externes et offrir leurs prestations à un cercle plus ou moins étendu de clientes. Dans ce cas de figure, les prestataires jouissent d'une propre personnalité juridique et elles peuvent être tant des personnes physiques que des personnes morales qui traitent avec une clientèle externe. La présente étude cherchant à comprendre le cadre légal circonscrivant l'activité de celles-ci, un accent sera mis sur ces intervenantes, en gardant à l'esprit qu'il existe naturellement d'autres organisations privées impliquées dans la protection contre les cybermenaces disposant des compétences complémentaires et distinctes[520].

518 FF 2017 2765, p. 2870 ; CF, *Rapport « La politique de sécurité de la Suisse »*, 2021, p. 26.

519 Cf. *supra* N 73 ss.

520 Certaines actrices privées sont par exemple actives dans la recherche, dans l'innovation ou encore dans la sensibilisation à large échelle, ce qui sort du cadre de la présente étude.

B. Les organisations compétentes dans la gestion technique des cyberincidents

1. Une multitude de structures et de pratiques

En pratique, toujours plus d'organisations disposent en leur sein de compétences propre de cybersécurité[521]. L'institution et l'exploitation d'une organisation chargée de la gestion de cyberincidents est une priorité en matière de cybersécurité[522]. Ces collaboratrices détiennent des compétences plus ou moins étendues selon les ressources et les besoins de l'organisation au sein de laquelle elles œuvrent. Ces personnes se trouvent en principe en première ligne de la gestion de cyberincidents et elles peuvent disposer de compétences préventives, détectives et réactives. Ces structures permettent une meilleure gestion des cyberincidents, ainsi qu'une organisation interne plus claire caractérisée par des tâches attribuées à des personnes ou des services spécifiques. Les processus de cybersécurité au sein des organisations s'en trouvent également améliorés. Les politiques de cybersécurité peuvent être mieux suivies et les échanges ainsi que la coopération entre les différents services d'une organisation sont généralement aussi facilités. 272

Il se peut que ces compétences soient externalisées auprès de prestataires externes, ce qui peut être préférable en fonction des besoins, des infrastructures et systèmes informatiques à protéger ainsi que des ressources d'une organisation (l'on parle parfois à ce sujet d'*Incident Response Providers* ou de CSIRT commerciales, même si ces organisations ne s'identifient pas toujours à ces terminologies)[523]. Dans ce cas, la prestataire de gestion de cyberincidents sert une clientèle ou une *constituency*[524]. 273

Certaines organisations comptent des collaboratrices internes tout en externalisant une partie des compétences en matière de cybersécurité. Un tel fonctionnement hybride est souvent préféré[525]. Ce partage des tâches permet de combiner la connaissance des infrastructures informatiques dont dispose des collaboratrices internes à l'expertise et aux ressources supplémentaires 274

521 GCSCC, *CSIRT – An Overview,* 2014, p. 7.

522 CF, *CSN,* 2023, p. 23.

523 AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung,* 2018, p. 30 ; GCSCC, *CSIRT – An Overview,* 2014, p. 8 ; DSOUZA, p. 211 et 217 ; KILLCRECE et al., *Organisational Models for CSIRT,* 2003, p. 12 ; MEYER/MÉTILLE, *Computer security incident response teams : are they really regulated ? The Swiss example,* 2022, p. 42 ; SURY, *Digital in Law,* 2021, p. 114.

524 GÖBEL, p. 168 ; WEST-BROWN et al., p. 11.

525 NIST, *Computer Security Incident Handling Guide,* 2012, p. 14 ; AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung,* 2018, p. 24 ; WEST-BROWN et al., p. 28.

d'une personne physique ou morale externe, tout ceci dans un esprit de coopération et de sécurité participative qui correspond à la conception aujourd'hui prisée. Dans tous les cas, l'organisation doit effectuer une analyse rigoureuse afin de déterminer la meilleure solution compte tenu de ses besoins, de ses ressources, de sa mission et ainsi de suite[526].

275 Sur le plan terminologique, l'on peut trouver des équipes informatiques *(IT teams),* des centres des opérations de sécurité (*Security Operation Centers,* SOC), des équipes d'intervention en cas d'incident lié à la sécurité informatique (*Computer Security Incident Response Teams,* CSIRT ou parfois appelées CSIRT organisationnelles[527]), des équipes d'intervention en cas d'incident relatif à la sécurité des produits (*Product Security Incident Response Teams,* PSIRT) ou encore des *IT vendors*. De plus en plus d'organisations se dotent de *Cyber Fusion Centers,* regroupant les compétences de SOC, CSIRT et *Red Teams* et *Blue Teams*. Le nom et la structure de la prestataire de gestion de cyberincidents peuvent donc varier et certaines organisations disposent de plusieurs services compétents pour différents aspects de la cybersécurité, en employant par exemple un SOC et une CSIRT[528].

276 Ces prestataires collaborent activement sur le plan national comme sur le plan international en vue d'établir une bonne vision des cybermenaces et de gérer efficacement les cyberincidents, ce qui est prévu par la SNPC 2018-2022 et la CSN de 2023[529]. En outre, certaines plateformes regroupent les CSIRT et autres organisations similaires pour privilégier un échange d'informations, notamment techniques, le plus efficient possible[530].

2. Le Security Operation Center

277 Le SOC est le centre opérationnel de commandement pour la protection et la réaction aux cyberincidents au sein d'une entreprise. En d'autres termes, il est le point central pour les opérations de sécurité et la protection des réseaux informatiques d'une organisation[531]. Il peut être mis en place et géré

526 NIST, *Computer Security Incident Handling Guide,* 2012, p. 19 ; WEST-BROWN et al., p. 28.

527 DSOUZA, p. 211.

528 AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung,* 2018, p. 24 ; CF, *CSN,* 2023, p. 24 ; ENISA, *How to set up CSIRT and SOC,* 2020, p. 7 ; DIOGENES/OZKAYA, p. 31 ; JOHANSEN, p. 28 ss, en particulier p. 30 ; MEYER/MÉTILLE, *Computer security incident response teams : are they really regulated ? The Swiss example,* 2022, p. 42. Certaines compétences sont même attribuées à d'autres actrices, à l'instar de compagnies d'assurance, cf. ENISA, *Cyber Insurance : Recent Advances, Good Practices and Challenges,* 2016, p. 14 ss.

529 CF, *CSN,* 2023, p. 24 ; CF, *Plan de mise en œuvre de la SNPC 2018-2022,* 2019, p. 43.

530 FIRST, *CSIRT – Services Framework,* 2019, p. 4 ; SKOPIK/SETTANNI/FIEDLER, p. 170 s.

531 NIST, 800-53, rev. 5, IR-4, p. 155.

de plusieurs manières. Il peut être établi à l'interne d'une organisation ou constituer un service externe auprès duquel l'organisation confère différentes compétences[532]. Le SOC prend en charge tant l'exploitation de l'infrastructure informatique en termes de serveurs, de centre de données et de réseaux, que les processus de sécurité et de gestion de cyberincidents. Dans ce cadre, il surveille les infrastructures informatiques en vue de détecter à un stade précoce les cyberincidents[533].

Le SOC met en œuvre des contrôles de gestion, techniques et opérationnels pour pouvoir surveiller, analyser, corréler les données relatives aux menaces et répondre aux événements[534]. Contrairement à la CSIRT, il est souvent le premier à détecter des événements et des incidents ou à recevoir des rapports d'incidents, qu'il transmettra à celui-là en cas de besoin[535]. 278

Pour remplir sa mission, le SOC doit être apte à adapter rapidement les mesures qu'il entreprend à l'état des menaces en se basant sur des analyses de sécurité et sur divers scénarii. En outre, il augmente sa capacité à réagir en se basant sur les succès de la protection offerte et sur la visibilité de la situation des menaces. Il prépare des rapports de sécurité afin de réagir toujours plus efficacement aux attaques subies[536]. Ses prestations concrètes dépendent de l'activité, des infrastructures, des besoins, des ressources et des processus de l'organisation qui bénéficie de ses compétences[537]. 279

3. Le Computer Security Incident Response Team

La CSIRT ou *incident response team*[538] est une équipe d'intervention d'urgence en informatique qui cherche à gérer et à répondre aux cyberincidents[539]. L'on 280

532 NIST, 800-53, rev. 5, IR-4, p. 156 ; AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung*, 2018, p. 24.

533 AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung,* 2018, p. 24 ; NIST, 800-53, rev. 5, IR-4, p. 155 ; SWISSCOM, *Security Operation Center,* 2020, p. 3 et 5 ; SALAMON, p. 121 ; VON OW, p. 87.

534 NIST, 800-53, rev. 5, IR-4, p. 156.

535 AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung,* 2018, p. 26 ; ENISA, *How to set up CSIRT and SOC,* 2020, p. 7 ; OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »,* 2021, p. 133 et 160 ; SWISSCOM, *Security Operation Center,* 2020, p. 3 ; JOHANSEN, p. 30.

536 SWISSCOM, *Security Operation Center,* 2020, p. 5.

537 AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung,* 2018, p. 24.

538 C. 34 Directive SRI ; ISO/IEC 27035-1 : 2016, p. 2 ; ISO/IEC 27035-2 : 2016, p. 2 ; ENISA, *How to set up CSIRT and SOC,* 2020, p. 6 ; ENISA, *Good Practice Guide for Incident Management,* 2010, p. 12 ; OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »,* 2021, p. 133 ; DIOGENES / OZKAYA, p. 31.

539 Voir notamment ISO/IEC 27019 : 2017, p. 2 ; ENISA, *How to set up CSIRT and SOC,* 2020, p. 6 ; GCSCC, *CSIRT – An Overview,* 2014, p. 6 ; ALBERTS et al., p. 1 s. ; SALAMON, p. 128 s.

utilise parfois le synonyme de *Computer Emergency Response Team* (CERT), qui reflète aujourd'hui davantage une marque déposée (qui sert en particulier pour les CERT nationales ou gouvernementales)[540]. Comme nous l'avons vu, la prestataire de gestion de cyberincidents de la Confédération est GovCERT.

281 Comme GovCERT, la mission des autres CSIRT est principalement l'assistance technique dans la gestion de cyberincidents, en vue de les détecter et de les maîtriser. La différence principale est que GovCERT intervient en seconde ligne, typiquement lors d'incidents d'importante envergure[541].

282 L'activité des CSIRT s'articule autour des compétences techniques, de la confiance et de la coopération[542]. L'organisation et les compétences concrètes varient d'une CSIRT à un autre. Néanmoins, l'on peut à ce stade poser quelques généralités sur celles-ci. Une CSIRT traite généralement les cyberincidents. Elle investigue pour tenter de régler ces derniers, de réduire les dommages en résultant, ce tout en cherchant à développer une réponse systématique et coordonnée aux cyberincidents et en tirer des leçons[543]. Plus précisément, cette équipe d'expertes dispose de qualifications en termes d'analyse, d'élaboration et déploiement de mesures défensives et d'atténuation ainsi que de préservation de preuves notamment, tout cela en temps réel[544]. La mission de la CSIRT s'articule autour de trois points centraux : la prévention, la détection et la réaction aux incidents informatiques et réseau[545].

540 ENISA, *Good Practice Guide for Incident Management,* 2010, p. 12 ; GCSCC, *CSIRT – An Overview,* 2014, p. 6 ; GHERNAOUTI, *Cybercriminalité,* 2023, p. 173 ; voir notamment SALAMON, p. 129. La marque déposée appartient au CERT/CC du *Software Engineering Institute de la Carnegie Mellon University,* compétent pour coordonner des actions de gestion de vulnérabilités et incidents et partageant des *best practices,* mais la marque n'est pas déposée en Suisse, raison pour laquelle les CSIRT situées sur territoire helvétiques peuvent l'utiliser, cf. IPI, Base de données, Marque, Titre : « CERT » ; SOFTWARE ENGINEERING INSTITUTE, *Authorized Users of the CERT Mark*.

541 GovCERT intervient en qualité de soutien aux équipes de gestion de cyberincidents. Par exemple, au sein de l'administration fédérale, la surveillance des réseaux relève souvent de la responsabilité de l'équipe d'intervention en cas d'urgence informatique de l'OFIT, qui est le CSIRT de l'OFIT, cf. NCSC, *Rapport sur la sécurité informatique de la Confédération*, 2021, p. 5.

542 Voir par exemple GCSCC, *CSIRT – An Overview*, 2014, p. 8.

543 KILLCRECE et al., *State of Practice of CSIRT,* 2003, p. 51. Une équipe peut typiquement mieux se préparer pour les attaques à venir ainsi que construire une meilleure protection par l'utilisation d'informations relatives à des incidents, cf. VAN DER KLEIJ/KLEINHUIS/YOUNG, p. 2.

544 NIST, 800-53, rev. 5, IR-4, p. 155.

545 OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »,* 2021, p. 133 ; MEYER/MÉTILLE, *Computer security incident response teams : are they legally regulated ? The Swiss example,* 2022, p. 44 ; NIST, *Computer Security Incident Handling Guide,* 2012, p. 65 ; SWISSPOWER, *Swisspower Cybersecurity*. À noter qu'il détient parfois un pouvoir décisionnel, mais pas systématiquement, cf. GCSCC, *CSIRT – An Overview,* 2014, p. 9 ; WEST-BROWN et al., p. 15 s.

4. Les Cyber Fusion Centers, Red Teams et autres structures

Les *Cyber Fusion Centers,* toujours plus utilisés en pratique, ont pour mission 283
de regrouper le SOC et la CSIRT afin d'offrir les prestations en principe fournies par ces équipes-ci, à savoir la prévention, mais surtout la détection et la réaction aux cyberincidents[546]. La pratique des *Cyber Fusion Centers* compte aussi régulièrement un aspect de *threat hunting* ou, du moins, de collecte de renseignements.

Les *Red Teams* sont des équipes destinées à fournir des services de protec- 284
tion active ou, du moins, proactive. Elles simulent typiquement des attaques sur les infrastructures de ses clientes ou de l'organisation de laquelle elles font partie, afin d'une part d'optimiser la protection contre de réelles attaques et, d'autre part, de collecter des renseignements à des fins d'investigation. Les *Blue Teams* sont confrontées aux attaques simulées des *Red Teams* et tentent d'y répondre. Ces processus servent notamment à comprendre le comportement d'une actrice malveillante, collecter des informations de renseignement, créer de meilleurs plans de réponse et mieux réagir à des attaques futures[547]. Des *Purple Teams* peuvent être intégrées pour soutenir ces processus[548]. Leurs prestations semblent donc en pratique limitées en comparaison à celles de CSIRT ou *Cyber Fusion Centers*.

Il existe encore d'autres types de prestataires de gestion de cyberinci- 285
dents, souvent dotées de compétences plus spécifiques comme les PSIRTs. Certaines structures sont dotées de compétences connexes à l'instar des fabricantes de produits informatiques *(IT vendors* ou *vendor teams)* qui disposent de compétences de coordination dans le cadre de la gestion de vulnérabilités[549].

5. Le rôle de la responsable de la sécurité des systèmes d'information

La responsable de la sécurité des systèmes d'information (RSSI) définit et 286
développe la politique de sécurité de l'information de son organisation[550]. Elle dirige les opérations relatives à la sécurité des systèmes d'information.

546 JOHANSEN, p. 31 s. ; VON OW, p. 87. La fournisseuse de prestations du DDPS dispose notamment d'un *Cyber Fusion Center,* cf. NCSC, *Rapport sur la sécurité informatique de la Confédération,* 2021, p. 5.

547 À ce sujet, voir notamment DIOGENES/OZKAYA, p. 19 s.

548 HOSSAM M., *Red team, blue team & purple team : Quelles sont les différences ?*.

549 Au sujet des PSIRTs, voir notamment ENISA, *PSIRT Expertise and Capabilities Development – Health and Energy PSIRT study and recommendations,* juin 2021 ; FIRST, *Cadre de service de l'Équipe d'intervention en cas d'incident relatif à la sécurité des produits (PSIRT),* version 1.1, 2020. Pour les *vendor teams,* voir par exemple GCSCC, *CSIRT – An Overview,* 2014, p. 8 ; DSOUZA, p. 211.

550 ORACLE, *Qu'est-ce qu'un RSSI et quel est son rôle ?*.

Lorsqu'elle existe au sein d'une organisation, c'est souvent à elle qu'incombe la responsabilité globale de la sécurité informatique et de la sécurité des systèmes de contrôle des processus et des réseaux[551]. Elle est régulièrement amenée à travailler de façon indépendante au sein des organisations qui l'emploient. Spécialisée dans les aspects sécuritaires de la stratégie d'entreprise, elle peut aussi, parfois, revêtir des compétences opérationnelles[552]. Elle nécessite d'être appuyée dans ses tâches par des SOC et des CSIRT afin de garantir au mieux un niveau de sécurité suffisant[553].

C. Les compétences des prestataires de gestion de cyberincidents

1. Des remarques introductives

287 Avant d'analyser les compétences principales possibles des prestataires de gestion de cyberincidents, il convient de rappeler qu'elles offrent des prestations diverses et variées[554]. Chaque organisation est libre d'aménager sa structure comme elle le souhaite. Que les prestataires de gestion de cyberincidents soient internes ou externes à l'organisation, la liberté contractuelle prévaut et la profession n'est pas réglementée[555]. Les prestations offertes par la prestataire de gestion de cyberincidents et les expertes dépendent notamment de l'organisation pour laquelle elles opèrent, des besoins de cette dernière, de sa nature, de son domaine d'activité ainsi que d'autres paramètres[556]. Ces prestations varient également selon la structure de la prestataire de gestion de cyberincidents (selon qu'elle est interne, externe et selon les tâches qu'on lui attribue concrètement).

288 Compte tenu de ce qui précède, les compétences analysées ci-dessous se rapportent aux compétences générales qu'une prestataire de gestion de

551 AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung,* 2018, p. 10 ; HOOPER /MCKISSACK, p. 585 ss ; LUSSAN Pierre-Louis, *4 étapes clés pour développer une forte culture de sécurité en entreprise,* Les Echos, Paris 23 juillet 2018. Pour plus de détails sur ses possibles compétences, voir ISACA, COBIT 5, p. 169 s.

552 HOOPER/MCKISSAK, p. 587 s.

553 SWISSCOM, *Security Operation Center,* 2020, p. 2. Pour plus d'informations au sujet des fonctions de la CISO, qui est régulièrement l'une des personnes à qui la RSSI rend compte ou qui est parfois utilisée comme traduction pour la notion de RSSI, cf. HOOPER/MCKISSACK, p. 587 s.

554 Sur les compétences typiques d'un CSIRT, cf. ENISA, *How to set up CSIRT and SOC,* 2020, p. 7 ; KILLCRECE et al., *Organisational Models for CSIRT,* 2003, p. 11 ; WEST-BROWN et al., p. 22.

555 SURY, *Digital in Law,* 2021, p. 62.

556 CF, *CSN,* 2023, p. 24 ; ENISA, *Good Practice Guide for Incident Management,* 2010, p. 14 ; WEST-BROWN et al., p. 19.

cyberincidents est susceptible de se voir attribuer en pratique. Cette analyse se focalise sur les compétences de gestion de cyberincidents[557], mais nous verrons que d'autres compétences parallèles peuvent être attribuées aux prestataires de gestion de cyberincidents[558].

289 Le catalogue présenté ci-dessous se réfère notamment aux normes suisses (souvent sectorielles) ainsi qu'aux normes internationalement reconnues. La plupart de ces recommandations mettent un accent sur les mêmes principes et fonctions, se reprennent parmi et ne sont pas directement contraignantes en Suisse[559]. Pour des raisons de cohérence, l'analyse de la présente étude se limite surtout aux normes principalement prises en compte en Suisse pour la gestion d'incidents et, plus spécifiquement, aux compétences des CSIRT.

290 Les prestations concrètes effectuées dans le cadre de la gestion d'incident peuvent être divisées selon différentes catégorisations[560]. La présente étude répartit les compétences selon le type de service entre la gestion de cyberincidents, la gestion de vulnérabilité, la gestion de la qualité de la sécurité et les compétences liées à la collecte et à l'exploitation de renseignements. La gestion de cyberincidents sera divisée chronologiquement, en distinguant entre les services proactifs, détectifs, réactifs et post-cyberincident[561]. Seront ensuite brièvement abordées les compétences additionnelles dont une prestataire de gestion de cyberincidents peut disposer en pratique, à savoir dans le cadre de la gestion de vulnérabilités, de la gestion de la qualité de la sécurité ou de la collecte et de l'exploitation de renseignements ou de CTI.

557 La gestion de cyberincidents constitue effectivement le centre de leurs prestations ; il est par ailleurs nécessaire d'offrir des prestations de gestion de cyberincidents pour être considéré comme un CSIRT, cf. ENISA, *How to set up CSIRT and SOC,* 2020, p. 6 ; WEST-BROWN et al., p. 23.

558 Cf. *infra* N 328 ss.

559 Cf. par exemple les normes sur lesquelles se base la norme minimale TIC de l'OFAE (et les normes sectorielles en découlant), cf. OFAE, *Norme minimale pour améliorer la résilience informatique,* 2023, p. 4 s. Pour un exemple de norme sectorielle et la mention faite des normes internationales pertinentes, cf. AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung,* 2018, p. 127 ss.

560 Voir les similitudes et différences entre par exemple NIST, 800-53, rev. 5 ; ENISA, *How to set up CSIRT and SOC,* 2020, p. 20 et FIRST, CSIRT – *Services Framework*, 2019, p. 8 et WEST-BROWN et al., p. 25. Pour une comparaison entre les cadres NIST et SANS, cf. ISA CYBERSECURITY, *Comparing NIST & SANS Incident Frameworks*, 3 février 2021 (consulté le 20.3.2024).

561 Les étapes chronologiques se fondent sur les compétences de gestion de cyberincidents analysées au début de cette étude, cf. *supra* N 90.

Schéma 9 : exemples de catégorisations des compétences de CSIRT

Reactive Services	Proactive Services	Security Quality Management Services

– Alerts and Warnings
– Incident Handling
  – Incident analysis
  – Incident response on site
  – Incident response support
  – Incident response coordination
– Vulnerability Handling
  – Vulnerability analysis
  – Vulnerability response
  – Vulnerability response coordination
– Artifact Handling
  – Artifact analysis
  – Artifact response
  – Artifact response coordination
	– Announcements
	– Technology Watch
	– Security Audit or Assessments
	– Configuration & Maintenance of Security Tools, Applications, & Infrastructures
	– Development of Security Tools
	– Intrusion Detection Services
	– Security-Related Information Dissemination
		– Risk Analysis
		– Business Continuity & Disaster Recovery Planning
		– Security Consulting
		– Awareness Building
		– Education/Training
		– Product Evaluation or Certification

Tiré de West-Brown et al., p. 25

Information Security Incident Management	Vulnerability Management	Situational Awareness	Knowledge Transfer	Information Security Event Management
– Information Security Incident Report Acceptance – Information Security Incident Analysis – Artifact and Forensic Evidence Analysis – Mitigation and recovery – Information Security Incident Coordination – Crisis management Support	– Vulnerability Discovery/ Research – Vulnerability Report intake – Vulnerability Analysis – Vulnerability Coordination – Vulnerability Disclosure – Vulnerability Response	– Data Acquisition – Analysis and Synthesis – Communication	– Awareness Building – Training and Education – Exercises – Technical and Policy Advisory	– Monitoring and Detection – Event Analysis

Tiré de ENISA, How to set up CSIRT and SOC 2020, p. 7

Reactive Services	Proactive Services	Artifact Handling	Security Quality Management
– Alerts and Warnings – Incident Handling – Incident Analysis – Incident Analysis – Incident Response Support – Incident Response Coordination – Incident Response on Site – Vulnerability Handling – Vulnerability Analysis – Vulnerability Response – Vulnerability Response Coordination	– Announcements – Technology Watch – Security Audits or Assessments – Configuration and Maintenance of Security – Development of Security Tools – Intrusion Detection Services – Security Related Information – Dissemination	– Artifact Analysis – Artifact Response – Artifact Response Coordination	– Risk analysis – Business Continuity and Disaster Recovery – Security Consulting – Awareness Building – Education/Training – Product Evaluation or Certification

Tiré de GCSCC, CSIRTs - An Overview 2014, p. 7

2. La planification et la préparation

Pour comprendre comment la gestion d'incident se déroule, il est nécessaire d'aborder les prestations de prévention et de préparation qu'une prestataire de gestion de cyberincidents est susceptible de fournir. Ces moyens cherchent à réduire la probabilité que des cyberincidents se produisent, à les anticiper et à y réagir au mieux[562]. 291

Le personnel compétent et les ressources organisationnelles et matérielles exploitables doivent être déterminées et identifiées[563]. À ce titre, les compétences d'une prestataire de gestion de cyberincidents doivent être prévues et son organisation doit être établie afin qu'elle soit apte à évoluer dans un environnement dynamique[564]. L'organisation souhaitant bénéficier des services d'une prestataire de gestion de cyberincidents doit avoir examiné les services qu'elle nécessite, en sus de la fonction principale de réaction aux incidents[565]. 292

Une fois mise sur pied, la prestataire de gestion de cyberincidents peut encourager la prise de conscience en matière de cybersécurité par la prévention d'événements futurs sur la base de réactions passées[566]. Elle peut être tenue de procéder à des audits ou des évaluations des infrastructures de ses clientes[567]. La prévention peut également passer par l'optimisation de l'infrastructure de sécurité, le conseil et l'échange d'informations, qui permettent de prévenir les cyberincidents[568]. La prestataire de gestion de cyberincidents 293

562 AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung*, 2018, p. 26 s. ; KILLCRECE et al., *Organisational Models for CSIRT*, 2003, p. 14 ; KILLCRECE et al., *State of Practice of CSIRT*, 2003, p. 65 ; MORGUS et al., *CSIRT Basics for Policy-Makers*, 2015, p. 14 s. ; WEST-BROWN et al., p. 24.

563 Cf. *supra* N 94 ; GILLIÉRON Philippe, *L'établissement d'un plan de réponse en cas de faille de sécurité* ; JOHANSEN, p. 8 s.

564 ISO/IEC 27035-2 : 2016, p. 4 ; NIST, 800-53, rev. 5, AU-1, p. 65 ; NIST, 800-53, rev. 5, IR-8, p. 158 s. ; art. 4.2.1 ISO/EIC 27000 : 2018 ; ISO/IEC 27001 : 2013, A.16.1.1 ; ISO/IEC DIS 27002 : 2021, A.5.24 ; BSI-Standard 100-4, p. 24 ; ISACA, COBIT 5, p. 65 ; ENISA, *Good Practice Guide for Incident Management*, 2010, p. 19 s. ; ENISA, *How to set up CSIRT and SOC*, 2020, p. 15 ; KILLCRECE et al., *State of Practice of CSIRT*, 2003, p. 85 s. ; VON OW, p. 87 ; WEST-BROWN et al., p. 41 et 50. Il doit en outre bénéficier des ressources nécessaires et de mécanismes de soutien, voir ISO/IEC 270351 : 2016, p. 9.

565 NIST, *Computer Security Incident Handling Guide*, 2012, p. 18 ss.

566 KILLCRECE et al., *State of Practice of CSIRT*, 2003. p. 12. Elle favorise en même temps l'échange d'informations à l'interne, NIST, 800-53, rev. 5, IR-4, p. 155.

567 NIST, *Computer Security Incident Handling Guide*, 2012, p. 24 ; AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung*, 2018, p. 28 ; WEST-BROWN et al., p. 30.

568 AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung*, 2018, p. 27 ; SALAMON, p. 129. Elle peut typiquement être amenée à procéder à des annonces, comme la transmission de ses coordonnées aux clientes ou le partage de

peut prévenir la diffusion de logiciels malveillants et sécuriser les hôtes et le réseau afin d'éviter tout accès non autorisé. Elle peut aussi développer des outils et applications de sécurité[569].

3. De la prévention à la détection de cyberincidents

294 Il est nécessaire de mettre en place les mesures pour détecter le plus tôt possible des événements anormaux, raison pour laquelle une prestataire de gestion de cyberincidents peut être amenée à mettre à disposition de sa clientèle des services de détection de cyberincidents[570]. Afin d'aider sa cliente ou son organisation à détecter des cyberincidents, la prestataire de gestion de cyberincidents fournit et exploite parfois des outils techniques de détection, à l'instar d'IDPS ou encore de SIEM[571].

295 Un cyberincident peut avoir différentes origines. Il peut se manifester sous la forme d'un code malicieux se propageant depuis une clé USB externe, depuis Internet ou encore depuis un courriel. Il peut survenir par l'activité non autorisée d'une collaboratrice, être constitutif d'une attaque DoS ou DDoS contre le serveur d'une organisation, d'hameçonnage ou, encore souvent, d'une autre manipulation humaine non autorisée[572]. Alors que certains cyberincidents sont faciles à détecter, à l'instar d'un défacement de site Internet, d'autres sont plus délicats et nécessitent l'utilisation de logiciels et autres outils informatiques[573]. Il existe différents processus de surveillance, de contrôles, d'audits, d'évaluations et de corrélations d'informations permettant de connaître le fonctionnement normal des infrastructures informatiques, des comptes ou des logiciels[574]. Une vue d'ensemble appropriée des fonctionnements en

documentation relative aux meilleures pratiques, cf. AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung,* 2018, p. 28 s., ou aux nouveaux outils d'intrusion, cf. WEST-BROWN et al., p. 29.

569 AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung,* 2018, p. 28 s. ; ENISA, *How to set up CSIRT and SOC,* 2020, p. 7 ; KILLCRECE et al., *Organisational Models for CSIRT,* 2003 p. 21 ; NIST, *Computer Security Incident Handling Guide,* 2012, p. 24 ; WEST-BROWN et al., p. 31.

570 OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »,* 2021, p. 168 ; FIRST, *CSIRT – Services Framework,* 2019, p. 9 ; LUNDELL, p. 7 ; WEST-BROWN et al., p. 31. Les responsables du traitement et les sous-traitantes sont par ailleurs obligées de mettre en place des mesures de détection rapide lorsque des données personnelles sont compromises (art. 3 al. 3 litt. c OPDo), cf. OFJ, *Rapport explicatif OPDo,* 2022, p. 19.

571 NIST, *Computer Security Incident Handling Guide,* 2012, p. 14 ; LUNDELL, p. 7.

572 NIST, *Computer Security Incident Handling Guide,* 2012, p. 25 s.

573 Sur l'obligation de détection active d'incidents, voir art. 4.2.1 ISO/EIC 27000 : 2018, p. 12.

574 NIST, 800-53, rev. 5, AU-6, p. 70 ; en matière de surveillance et d'autres moyens de détection, voir notamment COBIT 5, DSS01.03. DSS05.07 ; ISO/IEC 27035-1 : 2016, p. 9 ; ISO/IEC 27035-2 : 2016, p. 22 ; OFAE, *Norme minimale pour améliorer la résilience infor-*

temps normal permet de percevoir plus aisément un fonctionnement anormal et ainsi détecter un événement anormal[575]. Les prestataires de gestion de cyberincidents peuvent être les personnes responsables de donner suite aux alertes lancées par les systèmes de *monitoring* ou de surveillance. En parallèle, les cyberincidents peuvent aussi être identifiés par des collaboratrices ou des usagères de l'organisation, à la suite de quoi les informations relatives à l'incident sont transmises à la prestataire de gestion de cyberincidents[576].

4. La réaction

a. La réception comme déclencheur

Une fois que la prestataire de gestion de cyberincidents prend connaissance d'un événement revêtant les caractéristiques d'un cyberincident, elle doit prendre les mesures réactives qui s'imposent pour restaurer une situation sûre, conformément à ses fonctions principales[577]. Chronologiquement, la prestataire compétente réceptionne les différents cyberincidents, effectue un tri, les analyse et y répond[578]. 296

La prestataire de gestion de cyberincidents trie, catégorise et hiérarchise des rapports d'incidents et les autres demandes qu'elle réceptionne[579]. Cette étape permet d'assurer une compréhension initiale de la situation ainsi qu'une estimation de l'impact de l'incident. Par ce biais, toutes les informations (vérifiées) passent à la prestataire de gestion de cyberincidents par un point de contact, ce qui permet une redistribution appropriée des fonctions de gestion de cyberincidents[580]. C'est lors de cette étape qu'un ordre de priorité 297

matique, 2023, DE.CM, p. 28 ; NIST, *Computer Security Incident Handling Guide,* 2012, p. 29 s. et 43 ; WEBER/WILLI, p. 35. Plus spécifiquement sur la surveillance d'accès physiques ou de biens, voir NIST, 80053, rev. 5, PE-3, p. 181 s., PE-3, p. 184 s. et PE-20, p. 192.

575 L'on peut par exemple faire du profilage de réseaux et systèmes, qui permettra d'identifier plus rapidement des changements au niveau des caractéristiques de ces derniers ou disposer de mécanismes automatisés de notifications et alertes pour détecter des potentielles fuites de données, cf. NIST, 800-53, rev. 5, AU-13, p. 79 ; NIST, *Computer Security Incident Handling Guide,* 2012, p. 29 et 43.

576 FIRST, CSIRT – *Services Framework,* 2019, p. 10.

577 ENISA, *Good Practice Guide for Incident Management,* 2010, p. 53. Pour rappel, elles doivent naturellement être basées sur un plan de réponse préétabli, cf. GILLIÉRON Philippe, *L'établissement d'un plan de réponse en cas de faille de sécurité* ; AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung,* 2018, p. 26 s.

578 Pour un résumé, voir notamment MORGUS et al., *CSIRT Basics for Policy-Makers,* 2015, p. 14 ; SALAMON, p. 129. Au sujet de la réception d'un incident par la prestataire de gestion de cyberincidents, voir notamment FIRST, *CSIRT – Services Framework,* 2019, p. 12 ss.

579 KILLCRECE et al., *Organisation Models for CSIRT,* 2003, p. 16.

580 ENISA, *Good Practice Guide for Incident Management,* 2010, p. 45. L'impact est typiquement différent si, par exemple, le site affecté était visé ou s'il fait l'objet de dommages collatéraux, cf. FIRST, *CSIRT – Services Framework,* 2019, p. 14.

va être fixé, en vertu notamment de l'impact fonctionnel du cyberincident sur le(s) système(s) informatique(s), de l'impact sur les informations, des dommages potentiels ainsi que des ressources nécessaires pour le traiter[581]. Il est possible que le tri ne soit pas effectué par la même entité physique ou géographique selon l'organisation de la prestataire de gestion de cyberincidents ou de l'organisation au sein de laquelle elle œuvre[582].

298 La prestataire de gestion de cyberincidents alerte en principe les personnes responsables des sites affectés par un cyberincident dont elle prend connaissance[583]. Elle peut ensuite procéder à l'analyse de cyberincidents, à la suite de laquelle elle prend les mesures qui s'imposent pour répondre à cet incident. Si l'incident est important au point d'être qualifié de crise, il est probable que la prestataire de gestion de cyberincidents transmette le dossier à une équipe spécifique de gestion de crises, qu'elle peut par la suite soutenir dans ses missions[584]. Dans le cadre de la réponse au cyberincident, la prestataire de gestion de cyberincidents prend parfois des mesures sur site[585], et coordonne la gestion de cyberincidents en plus d'y contribuer. Ces mesures peuvent être prises en temps réel ou nécessiter un certain temps d'investigation[586].

299 Il est important que la réponse se déroule selon un plan et un processus établis à l'avance[587]. Seront donc approfondies dans cette partie principalement

581 COBIT 5, DSS02.02 ; ISO/IEC 27035-3 : 2020, p. 14 s. ; ENISA, *Good Practice Guide for Incident Management,* 2010, p. 47 s. ; NIST, *Computer Security Incident Handling Guide,* 2012, p. 43 ; FIRST, *CSIRT – Services Framework*, 2019, p. 11 ; WEST-BROWN et al., p. 68. Au sujet des critères de l'établissement de priorités, voir KILLCRECE et al., *State of Practice of CSIRT,* 2003 p. 95 ; WEST-BROWN et al., p. 124 ss. À titre d'exemple, un incident à l'origine d'un impact fonctionnel élevé et dont la récupération requiert peu d'efforts et de ressources constitue un scénario requérant une action immédiate, cf. NIST, *Computer Security Incident Handling Guide,* 2012, p. 32.

582 Par exemple, dans le cas d'une prestataire de gestion de cyberincidents interne centralisée c'est cette dernière qui procède au tri, alors que si son équipe est interne mais distribuée, ce sont ses membres présents sur chaque site qui procèdent au tri initial selon le site affecté. Le tri peut même être fait par une autre entité entretenant des relations avec la prestataire de gestion de cyberincidents, cf. KILLCRECE et al., *Organisational Models for CSIRT,* 2003, p. 35 s., 61 et 79 s.

583 OFAE, *Norme minimale pour améliorer la résilience informatique,* 2023, DE.DP-4, p. 29.

584 BSI-Standard 100-4, p. 65 ; ISO/IEC 27035-1 : 2016, p. 11 ; ISO/IEC 27035-2 : 2016, p. 11. Elle peut tout de même être amenée à apporter un soutien à l'équipe de crise, cf. FIRST, *CSIRT – Services Framework*, 2019, p. 12 et 28 ss.

585 La différence étant qu'à distance, la prestataire de gestion de cyberincidents a moins d'interactions directes avec les systèmes concernés, cf. AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung,* 2018, p. 28. Concernant les interventions sur site, voir notamment WEST-BROWN et al., p. 27.

586 ISO/IEC 27035-1 : 2016, p. 11.

587 ISO/IEC 27001 : 2013, A.16.1.5 ; ISO/IEC DIS 27002 : 2021, A.5.26 ; NEDIK, *Cyberattaque – que faire ?,* 2020, p. 1 ; OFAE, *Norme minimale pour améliorer la résilience informatique,*

les fonctions d'analyse et les mesures de soutien à la réponse aux cyberincidents, ces compétences constituant les fonctions principales des prestataires de gestion de cyberincidents.

b. L'analyse

(i) Des généralités

Il existe différents niveaux et différentes prestations d'analyse. De manière générale, l'analyse consiste en une évaluation et une corrélation de toutes les informations à disposition sur un événement, un incident, un artéfact ou une vulnérabilité[588]. L'analyse peut donc prendre place dès la détection d'un événement[589]. Elle peut avoir lieu après réception d'un rapport d'incident avant la phase de réaction proprement dite. Elle peut également se dérouler dans ce cadre réactif pour comprendre et réduire la portée d'un cyberincident ou être menée durant l'investigation pour comprendre l'origine de l'incident, ou encore pour définir les stratégies et les mesures à prendre pour l'éradiquer[590]. Il est intéressant d'analyser aussi certains comportements suspects ou anormaux ou encore des codes malicieux afin de comprendre les tactiques, caractéristiques, processus d'une attaquante[591]. L'analyse demeure en tout cas, de manière générale, une phase cruciale pour déterminer les bonnes mesures à adopter[592]. 300

(ii) L'analyse de cyberincidents

Une fois un cyberincident réceptionné, accepté et trié par la prestataire de gestion de cyberincidents, cette dernière l'examine[593]. L'analyse d'un cyberincident peut être définie comme une évaluation de toutes les informations 301

2023, RS.RP-1, p. 30 ; OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »,* 2021, p. 154 et 162 ; CHRISTEN/KNIEPS, p. 8.

588 L'analyse consiste en la corrélation de différentes informations, à l'instar d'activités, de tendances ou de signatures, cf. AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung,* 2018, p. 27 ; WEST-BROWN et al., p. 26.

589 Il faut en effet d'abord s'assurer que l'événement détecté est bel et bien constitutif d'un cyberincident. Cette tâche ne revient pas forcément à la prestataire de gestion de cyberincidents, qui est davantage susceptible de recevoir un rapport indiquant que l'événement constitue un incident ou une fausse alarme, cf. ISO/IEC 27035-1 : 2016, p. 10 ; FIRST, *CSIRT – Services Framework,* 2019, p. 11 ; SALAMON, p. 124 s.

590 Voir par exemple ENISA, *Good Practice Guide for Incident Management,* 2010, p. 34 ; FIRST, *CSIRT – Services Framework,* 2019, p. 22. Il convient par ailleurs de pister les informations durant l'entier du cycle de vie d'un incident, cf. WEST-BROWN et al., p. 91.

591 NIST, 800-53, rev. 5, IR-4, p. 155.

592 ENISA, *Good Practice Guide for Incident Management,* 2010, p. 51.

593 Au sujet de la réception d'un cyberincident par une CSIRT, voir notamment ISO/IEC 27035-3 : 2020, p. 12 ; FIRST, *CSIRT – Services Framework,* 2019, p. 12 ss.

disponibles sur l'incident. Les objectifs de cette analyse sont la détermination des causes et de l'étendue de l'incident, l'identification des réponses appropriées et l'utilisation des résultats obtenus. L'utilisation des résultats sert à fournir une analyse la plus précise possible le concernant et une appréciation des tendances et des menaces ainsi qu'à améliorer constamment la sécurité de l'organisation[594]. Cette analyse est nécessaire afin d'enclencher la bonne réaction, dans la mesure où les indicateurs d'incidents sont très nombreux dans le quotidien d'infrastructures informatiques et qu'ils ne peuvent pas garantir une fiabilité totale[595].

302 L'analyse peut être menée plus ou moins en profondeur[596]. Elle porte sur l'hôte ou les hôtes compromises ou affectées, la mémoire, le trafic réseau, les fichiers de journalisation *(log files),* les connexions réseau ou les processus logiciels[597]. L'analyse peut consister en l'examen de codes malicieux et de l'environnement d'un logiciel en vue de fournir un soutien technique, des solutions ou une assistance sur site[598]. Les capacités concrètes d'analyse varient d'une prestataire de gestion de cyberincidents à une autre[599].

303 L'analyse peut porter plus précisément sur les artéfacts, à savoir sur des objets permettant de comprendre la nature, les mécanismes, les versions et l'utilisation des traces laissées par la personne à l'origine de l'intrusion (à

594 COBIT 5, DSS02.04, DSS02.07 ; ISO/IEC 27035-3 : 2020, p. 17 ; OFAE, *Norme minimale pour améliorer la résilience informatique,* 2023, DE-AE.2, DE-AE-4, RS.AN-2, p. 27 et 32 ; OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »,* 2021, p. 27 et 154 ; GILLIÉRON Philippe, *L'établissement d'un plan de réponse en cas de faille de sécurité* ; SALAMON, p. 131 ; WEST-BROWN et al., p. 26. Concernant l'utilisation des résultats d'analyses en vue de dresser une vue d'ensemble, voir WEST-BROWN et al., p. 80 s.

595 Des alertes peuvent en effet être enclenchées sans cyberincident, cf. NIST, *Computer Security Incident Handling Guide,* 2012, p. 28. À noter que des mécanismes automatisés peuvent être utilisés au titre de système de gestion des incidents ou encore en tant qu'outils permettant la prise en charge de la collecte de données de réponse en direct, la saisie de paquets ou l'analyse forensique, NIST, 800-53, rev. 5, IR-4, p. 152.

596 La profondeur de l'analyse dépend de facteurs tels que la mission et les capacités de la prestataire de gestion de cyberincidents, la gravité du cyberincident ou encore des risques de réitération d'une cyberattaque, cf. WEST-BROWN et al., p. 82.

597 KILLCRECE et al., *State of Practice of CSIRT,* 2003, p. 98. L'analyse de fichiers journaux a pour but de connaître qui s'est connecté d'où, selon quel type de connexion et de comprendre l'origine de l'erreur qui s'est produite. Les objets de cette analyse sont principalement l'horodatage, l'origine des accès et l'authentification de ceux-ci, cf. WEST-BROWN et al., p. 84 s.

598 ISO/IEC 27035-3 : 2020, p. 16 ss ; WEST-BROWN et al., p. 76 et 82.

599 À titre d'exemple, certaines équipes n'ayant que quelques années d'informations enregistrées disposent de possibilités limitées d'analyse de tendances passées, cf. DSOUZA, p. 216.

l'instar de codes sources ou scripts d'exploitation)[600]. Les personnes compétentes tentent par cette analyse de reconstituer les agissements de la personne s'étant introduite indûment, de déterminer la vulnérabilité potentiellement exploitée, d'évaluer les dommages, de développer des solutions permettant d'atténuer les artéfacts et de fournir les informations pertinentes aux cibles et aux personnes concernées[601]. L'analyse d'artéfacts n'étant pas suffisante, l'analyse de l'environnement logiciel doit être effectuée également[602]. Ces analyses servent de base pour fournir des conseils à la victime par la révélation des vulnérabilités connues dans un logiciel (environnement) spécifique. Le problème est ensuite transféré au service de traitement des vulnérabilités si une vulnérabilité inconnue vient à être détectée[603].

Les analyses de cyberincidents peuvent se faire selon une approche 304
forensique, permettant d'une part de comprendre et de reconstruire le déroulement d'un cyberincident et d'autre part de déterminer les vecteurs d'attaque[604]. L'analyse forensique cherche à conserver la continuité de la preuve ; les moyens de preuves numériques doivent être préservés pour le cas où ils pourraient être requis dans le cadre d'une procédure subséquente[605]. L'analyse forensique peut porter sur un réseau ou sur une machine spécifique[606]. Cette analyse est conduite par des procédés forensiques dont l'utilisation permet de collecter des moyens de preuve digitaux fiables et exploitables servant à prouver la culpabilité d'actrices malveillantes ou la conformité à certaines obligations incombant aux organisations visées par des attaques

600 FIRST, *CSIRT – Services Framework*, 2019, p. 18 ; OAS, *Best Practices National CSIRT,* p. 42 ; KILLCRECE et al., *Organisational Models for CSIRT,* 2003, p. 19 : WEST-BROWN et al., p. 29 et 85. L'artéfact peut être, dans ce contexte, un dossier ou un objet impliqué dans une cyberattaque trouvé sur un système informatique, WEST-BROWN et al., p. 28. À noter que la gestion des artéfacts peut être considérée comme une tâche à part de la réponse aux incidents, cf. OAS, *Best Practices National CSIRT,* p. 42.

601 FIRST, *CSIRT – Services Framework*, 2019, p. 19.

602 WEST-BROWN et al., p. 88.

603 WEST-BROWN et al., p. 89.

604 À ce sujet voir : ENISA, *Electronic evidence*, 2015, p. 18 ; KILLCRECE et al., *Organisational Models CSIRT,* 2003, p. 17 ; KILLCRECE et al., *State of Practice of CSIRT,* 2003, p. 98. Il faut que la documentation de ces éléments soit conciliable avec une déposition devant la justice si besoin, WEST-BROWN et al., p. 26. À noter que, comme pour l'analyse d'artéfacts, certaines considèrent qu'il s'agit d'une compétence additionnelle, cf. ENISA, *Good Practice Guide for Incident Management,* 2010, p. 102.

605 ISO/IEC 27035-1 : 2016, p. 11. Il faut pouvoir démontrer que les moyens de preuve ont été collectés et conservées conformément aux règles de l'art.

606 Les analyses forensiques peuvent porter sur un réseau ou sur une machine spécifique, mais il semble moins onéreux et plus facile de procéder à des analyses forensiques du réseau, cf. ENISA, *Good Practice Guide for Incident Management,* 2010, p. 102.

notamment[607]. Ces compétences ne sont pas toujours attribuées à la prestataire de gestion de cyberincidents, mais peuvent incomber à un service ou une équipe distincte et spécialisée dans le domaine forensique, à l'instar d'une première intervenante ou d'une spécialiste de la preuve numérique (respectivement *Digital Evidence First Responser* et *Digital Evidence Specialist*). Dans ce cas, la prestataire de gestion de cyberincidents a comme mission principale d'utiliser, dans sa réponse à un incident, des mécanismes d'authentification des traces collectées pour permettre à l'équipe forensique de gagner du temps[608]. Ce type de mesures et d'approches soulève des questions découlant de la sauvegarde des moyens de preuve, qu'il s'agisse de proportionnalité dans la conservation de données notamment personnelles ou encore de coûts[609].

305 Il peut être intéressant de procéder durant une investigation à une analyse supplémentaire : l'analyse interincidents, à savoir l'établissement d'une connexion entre plusieurs incidents par la recherche de similitudes. Les analyses interincidents visent à trouver des origines communes ou reliées entre différents incidents[610].

c. La circonscription, l'éradication et la restauration

(i) La circonscription des cyberincidents

306 Il faut, pour résoudre l'incident à court terme d'abord, atténuer au maximum les impacts négatifs de ce dernier et remédier à la situation en restaurant un état sûr pour les systèmes affectés, tout cela le plus rapidement possible[611]. Après avoir obtenu une meilleure compréhension d'un cyberincident et de

607 ENISA, *Good Practice Guide for Incident Management*, 2010, p. 102 ; MARCELLA/MENENDEZ, p. 14 s. ; MITROPOULOS/PATSOS/DOULIGERIS, p. 364 ss. Il n'existe aujourd'hui pas d'unanimité entre les termes de *Cyber Forensics, e-discovery, digital forensics, computer forensics* et ainsi de suite. Néanmoins, ces notions s'orientent toutes vers le même domaine qui est celui de la recherche, de la collecte ou de l'extraction, de la préservation, de l'analyse et de l'utilisation de données à des fins légales, cf. MARCELLA/MENENDENZ, p. 4 s., 268 et références citées. Sur le plan international, voir notamment les normes ISO applicables au traitement des moyens de preuve électroniques, cf. ISO/IEC 27035-1 : 2016, p. 13 ss pour les différents standards ISO en la matière.

608 ISO/IEC 27037 : 2012, p. 13.

609 Les analyses forensiques peuvent porter sur un réseau ou sur une machine spécifique, mais il semblerait moins onéreux et plus facile de procéder à des analyses forensiques du réseau, cf. ENISA, *Good Practice Guide for Incident Management*, 2010, p. 102. Au sujet de la proportionnalité dans la collecte et la conservation de données personnelles, cf. *infra* N 917 ss.

610 ISO/IEC 27035-3 : 2020, p. 19 s. ; FIRST, *CSIRT – Services Framework*, 2019, p. 11 et 17 s. ; WEST-BROWN et al., p. 80.

611 ISO/IEC 27035-3 : 2020, p. 21 ; OFAE, *Norme minimale pour améliorer la résilience informatique*, 2023, RS.MI-1, RS.MI-2, p. 33 ; KRAL, p. 6. Le même objectif est prévu implicitement à l'art. 3 al. 3 litt. c OPDo lorsque des données personnelles sont impactées, cf. OFJ, *Rapport explicatif OPDo*, 2022, p. 19.

son étendue, la prestataire de gestion de cyberincidents doit éviter que les conséquences d'un cyberincident ne s'étendent et ne fassent davantage de victimes ou de dégâts. Pour ce faire, il faut trouver une stratégie et l'adapter à chaque cas d'espèce[612]. La stratégie de confinement de l'incident ou d'une infection par un logiciel malveillant transmis par courriel peut par exemple être différente de celle pour l'attaque DDoS d'un réseau[613]. Plusieurs stratégies sont envisageables et le choix doit porter sur la plus efficace pour gérer le cyberincident spécifique[614].

Le confinement est souvent cherché par la prestataire compétente pour réduire l'impact d'un cyberincident[615]. Il peut se faire selon plusieurs stratégies physiques et virtuelles. Il peut se faire par le biais notamment de l'isolement, du blocage ou de la déconnexion d'un système contaminé du reste du réseau (si les systèmes affectés peuvent être isolés des systèmes « sains »), par son arrêt, par une modification du routage ou par la mise en place des verrouillages d'urgence sur des pare-feux[616]. La prestataire doit surveiller des activités suspicieuses, identifier les annonces à faire et suivre des lignes directrices visant les échanges internes d'informations et les communications externes[617]. Le service compétent assiste et guide l'entité affectée par un cyberincident par assistance téléphonique, par courriel ou sur site[618]. En plus de cette assistance, il est possible que la prestataire apporte un soutien plus actif encore par le biais de manipulations informatiques permettant, outre la collecte d'informations, la suppression de la menace. 307

Des mesures comme le confinement de l'incident, ou, par exemple, d'un logiciel malveillant, risquent de soulever des questions importantes en pratique concernant la collecte de preuves. Un confinement peut effectivement 308

612 FIRST, *CSIRT – Services Framework*, 2019, p. 22.

613 GILLIÉRON Philippe, *L'établissement d'un plan de réponse en cas de faille de sécurité*.

614 NIST, 800-61, rev. 2, p. 35.

615 ISO/IEC DIS 27002 : 2021, p. 45 ; FIRST, *CSIRT – Services Framework*, 2019, p. 23 s. ; LUNDELL, p. 8.

616 ISO/IEC 27035-3 : 2020, p. 21 s. ; OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »*, 2021, p. 169 ; GILLIÉRON Philippe, *L'établissement d'un plan de réponse en cas de faille de sécurité* ; GÖBEL, p. 169 ; MITROPOULOS/PATSOS/DOULIGERIS, p. 360 ; SALAMON, p. 131 ; KRAL, p. 6. Le but du confinement est d'empêcher une intruse d'accéder ou exfiltrer d'autres données, de détruire des preuves ou encore d'utiliser le système affecté pour étendre une cyberattaque et pour, finalement, permettre un retour au fonctionnement normal des opérations, cf. ISO/IEC 270353 : 2020, p. 21 ; KRAL, p. 6.

617 NIST, *Computer Security Incident Handling Guide*, 2012, p. 8.

618 AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung*, 2018, p. 28 ; KILLCRECE et al., *State of Practice of CSIRT*, 2003, p. 98 ; LUNDELL, p. 8 ; WEST-BROWN et al., p. 27.

causer dans le système confiné la perte ou la destruction potentielles d'informations susceptibles d'être nécessaires dans une investigation subséquente[619]. La prestataire de gestion de cyberincidents procède par conséquent régulièrement à une sauvegarde du système affecté, notamment pour collecter des moyens de preuve et analyser les informations relatives à l'état de la machine infectée[620]. Une attention particulière doit en revanche être portée à l'utilisation de techniques de surveillance, car elles peuvent permettre aux personnes à l'origine d'attaques de persévérer dans celles-ci et, partant, de causer de plus amples dommages[621]. Les stratégies pour les différents cyberincidents et les preuves collectées par leur biais doivent être documentées et différenciées selon le cyberincident, en se basant sur des critères, à l'instar du vol ou non de ressources, de la disponibilité des services, du temps et des moyens nécessaires à la mise en œuvre de la stratégie et ainsi de suite[622]. Les personnes ayant travaillé sur l'incident, les heures auxquelles les mesures ont été mises en place, les données d'identification nécessaires doivent également être recueillies et stockées de manière sécurisée.

(ii) L'éradication

309 Après avoir contenu ou confiné un incident, la prestataire de gestion de cyberincidents doit tenter d'éradiquer, à savoir éliminer définitivement les composants du cyberincident, à l'instar des logiciels malveillants ou des comptes d'utilisatrices infectés. Il en va de même pour les artéfacts trouvés sur un système[623]. Ceci peut par exemple se faire par le reformatage d'un disque dur ou par une destruction physique[624]. C'est pourquoi il est nécessaire de connaître au mieux les machines infectées en dépit de la difficulté pratique que cette connaissance implique. Il faut que l'arrêt d'un système soit approuvé par les services compétents[625]. L'on peut analyser les systèmes précédemment affectés à l'aide d'un logiciel pour s'assurer que toute trace d'un logiciel malveillant latent est effectivement supprimée[626].

619 ISO/IEC 27035-3 : 2020, p. 22.

620 KRAL, p. 7.

621 NIST, *Computer Security Incident Handling Guide*, 2012, p. 36.

622 NIST, *Computer Security Incident Handling Guide*, 2012, p. 35 ; FIRST, CSIRT – *Services Framework*, 2019, p. 24.

623 ISO/IEC 27035-3 : 2020, p. 22 ; LUNDELL, p. 9 ; WEST-BROWN et al., p. 29.

624 ISO/IEC 27035-3 : 2020, p. 22 ; MITROPOULOS/PATSOS/DOULIGERIS, p. 361.

625 De même si la prestataire de gestion de cyberincidents décide de laisser un système affecté continuer d'opérer, cf. ISO/IEC 27035-2 : 2016, p. 13.

626 KRAL, p. 8.

À noter qu'il est parfois possible d'éradiquer l'incident durant la phase de restauration. Il n'est par ailleurs pas systématiquement nécessaire de l'éradiquer[627]. En outre, le risque de perte de données ou la destruction de supports demeure, de la même façon que lors du confinement d'un incident[628]. 310

(iii) La restauration

Une fois le cyberincident maîtrisé, il s'agit de voir si le système peut être restauré et nettoyé ou désinfecté[629]. Le retour à un fonctionnement normal des systèmes ou leur récupération se fait à l'issue des phases précédemment décrites et a lieu si l'on répond positivement à la question de savoir si le système peut être restauré et nettoyé par des mesures permettant d'éviter un incident futur[630]. Le rétablissement doit se faire selon un plan de récupération préétabli par l'organisation en fonction notamment de ses missions et de ses priorités. Cette phase peut impliquer la désactivation des capacités utilisées pour répondre à un cyberincident, le rétablissement des activités de surveillance continue ou encore l'évaluation des capacités du système restauré[631]. L'on parle aussi typiquement de l'arrêt du système ou de sa dégradation ordonnée, d'un retour au mode manuel, de la récupération de données effacées ou encore de l'activation d'une technologie alternative permettant au système de fonctionner différemment[632]. Il peut également s'agir de la restauration de systèmes à partir de sauvegardes propres, de la reconstruction d'un système à partir de zéro, du renforcement de la sécurité et de la modification des mots de passe, du remplacement de fichiers affectés par des versions propres, de la mise en place de correctifs et ainsi de suite[633]. Il est essentiel de tester, surveiller et valider les systèmes rétablis pour vérifier qu'ils ne puissent pas être 311

627 NIST, *Computer Security Incident Handling Guide*, 2012, p. 37.

628 ISO/IEC 27035-3 : 2020, p. 23.

629 COBIT 5, DSS02.05 ; GILLIÉRON Philippe, *L'établissement d'un plan de réponse en cas de faille de sécurité* ; SALAMON, p. 131. Lorsque des données personnelles sont concernées, l'art. 3 al. 2 litt. d OPDo dispose que la disponibilité et l'accès aux données doit au surplus être restauré aussi rapidement que possible, cf. OFJ, *Rapport explicatif OPDo*, 2022, p. 19.

630 OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »*, 2021, p. 154 ; GILLIÉRON Philippe, *L'établissement d'un plan de réponse en cas de faille de sécurité*.

631 NIST, 800-53, rev. 5, CP-10, p. 128 ; OFAE, *Norme minimale pour améliorer la résilience informatique*, 2023, RC.RP-1, p. 35.

632 NIST, 800-53, rev. 5, IR-4, p. 153 ; MITROPOULOS/PASTOS/DOULIGERIS, p. 361 ; WEBER/WILLI, p. 36.

633 ISO/IEC 27035-3 : 2020, p. 23 ; NIST, *Computer Security Incident Handling Guide*, 2012, p. 37 ; OFJ, *Rapport explicatif OPDo*, 2022 D, p. 19 ; SALAMON, p. 131.

compromis d'une autre manière[634]. La récupération peut poser des problèmes, en lien par exemple avec la connectivité du réseau ou encore si la sauvegarde n'est pas complète et que des données viennent à être perdues[635].

312 Ces processus doivent être opérés dans une approche progressive avec des phases hiérarchisées. Dans cet ordre d'idée, lors d'un incident à large échelle, il faut débuter l'éradication et le rétablissement de la situation par les mesures visant la sécurité à court terme, puis s'occuper de la sécurité à long terme[636]. Il est important de savoir si les solutions envisagées sont durables ou s'il est nécessaire de prendre davantage de mesures à long terme[637].

d. La question de l'attribution

313 Parallèlement à la réponse à un incident et dans le cas d'attaques sophistiquées, il peut être intéressant de chercher à déterminer l'organisation à l'origine d'une attaque[638]. L'attribution permet de mieux comprendre tant les motivations des délinquantes que leurs modes opératoires[639]. Bien que cette démarche semble concerner de prime abord principalement les autorités de poursuite pénale, elle peut également servir à la prestataire de gestion d'incidents ainsi qu'à la cible de l'attaque. La recherche de cette information peut être légitime dans des cas sophistiqués, à l'instar d'attaques organisées ou de tentatives d'espionnage : dans ces cas, si la cible se limite à supprimer le logiciel malveillant, la personne à l'origine de l'attaque initiale pourrait simplement changer de mode opératoire avant de réattaquer. Une démarche d'identification permettrait de comprendre précisément ce qui est recherché par la personne à l'origine de l'intrusion, de mieux sécuriser les systèmes informatiques ainsi que les informations[640]. Cette démarche peut également permettre des échanges d'informations visant à aider d'autres organisations pour identifier plus facilement l'intruse et contrecarrer des attaques.

634 KRAL, p. 8.

635 ISO/IEC 27035-3 : 2020, p. 23. La norme ISO/IEC 27019 : 2017, prévoit des normes pour le domaine de l'énergie, anticipe par ailleurs l'incompatibilité qui peut exister entre la restauration de systèmes en temps voulu et la collecte de preuves ; partant, elle prévoit que l'exploitante définit les situations et les systèmes pour lesquels la collecte de preuves est possible, cf. ISO/IEC 27019 : 2017, p. 29.

636 NIST, *Computer Security Incident Handling Guide*, 2012, p. 37.

637 Il faut surveiller et tester les systèmes restaurés pour s'assurer qu'il n'y a plus de risque qu'un incident semblable se produise, cf. GILLIÉRON Philippe, *L'établissement d'un plan de réponse en cas de faille de sécurité*.

638 CF, *CSN*, 2023, p. 25.

639 SRC, *Compétences du SRC en matière d'attribution des cyberattaques*, 2020, p. 6.

640 SRC, *Compétences du SRC en matière d'attribution des cyberattaques*, 2020, p. 6.

Cela étant, les ressources des prestataires de gestion de cyberincidents doivent être privilégiées pour investiguer et contenir un cyberincident avant de consacrer du temps à attribuer l'origine d'une attaque, pratique qui peut facilement rester sans succès. En outre, l'attribution peut soulever des questions de légalité et elle fait l'objet des compétences de certaines autorités, raison pour laquelle ces autorités, dont les autorités de poursuite pénale et les services de renseignement, doivent demeurer compétentes pour l'attribution des cyberattaques[641]. Il est toujours possible de transmettre les informations collectées dans le cadre de la gestion du cyberincident à une organisation tierce compétente pour ces questions d'attribution et disposant de plus larges bases de données[642]. 314

e. Les activités post-incident

La prestataire de gestion de cyberincidents clôt un incident une fois qu'aucune partie prenante n'identifie ou ne signale d'informations supplémentaires le concernant à l'équipe d'expertes et que cette dernière a pris les mesures qui s'imposaient vis-à-vis des différentes personnes concernées[643]. D'un point de vue technique, il n'est pas exclu que la prestataire de gestion de cyberincidents procède à davantage d'investigations ou d'analyses après le rétablissement d'une situation sûre, par exemple si elle trouve une nouvelle source intéressante d'informations[644]. 315

Une fois un incident clos et archivé, il est primordial d'en tirer des enseignements afin d'améliorer la résilience future des systèmes informatiques utilisés[645]. L'on apprend et partage des informations sur le déroulement de l'incident *(Who, What, Where, Why and How*[646]*)*, sur les mesures qui auraient été nécessaires plus tôt dans la réaction, sur les comportements qui auraient 316

641 CF, *CSN*, 2023, p. 25 ; SRC, *Compétences du SRC en matière d'attribution des cyberattaques*, 2020, p. 6 s.

642 NIST, *Computer Security Incident Handling Guide*, 2012, p. 37.

643 COBIT 5, DSS02.06. À noter qu'il faut que les personnes impliquées soient informées de la clôture de cyberincident. En outre, il est possible qu'un site demeure actif sur la résolution d'un incident malgré la clôture de celui-ci par la prestataire de gestion de cyberincidents si, par exemple, elle essaie encore de récupérer le système par la suite, ou encore si une procédure judiciaire s'ensuit, WEST-BROWN et al., p. 77 s.

644 ISO/IEC 27035-1 : 2016, p. 11 ; ISO/IEC 27035-2 : 2016, p. 11.

645 ISO/IEC 27001 : 2013, A.16.1.6 ; ISO/IEC DIS 27002 : 2021, A.5.27 ; OFAE, *Norme minimale pour améliorer la résilience informatique*, 2023, RS.IM-1, p. 34 ; OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »*, 2021, p. 169. Pour des exemples de leçons à tirer pour différentes personnes concernées par un cyberincident, cf. ENISA, *Good Practice Guide for Incident Management*, 2010, p. 56.

646 JOHANSEN, p. 316 ; KRAL, p. 9.

dû être adoptés ou devraient être omis ou modifiés à l'avenir[647]. Cette phase comprend également la collecte et la documentation d'informations relatives à l'incident pour améliorer le contrôle de gestion de risques, évaluer le succès de la prestataire de gestion de cyberincidents, remplir certaines obligations, éviter qu'un incident similaire se produise et améliorer le plan de continuité, l'entraînement et les procédures[648]. Par exemple, si en observant les statistiques, la prestataire de gestion de cyberincidents observe une montée du nombre de cas d'hameçonnage, elle peut se concentrer sur les différentes techniques actuelles et former davantage les personnes potentiellement visées[649].

317 La prestataire de gestion d'incidents transmet les différentes informations susmentionnées par la remise d'un ou plusieurs rapport(s) à sa cliente[650]. Le rapport peut consister en un résumé des événements, en une description de l'origine de l'incident ainsi qu'en des recommandations pour remédier à la situation et empêcher la survenance d'un incident similaire. Le résumé permet à l'organisation cliente de comprendre l'ampleur de l'incident et de s'assurer que les mesures juridiques et de communication adéquates sont prises et envisagées. Les expertes transmettent le plus souvent un rapport d'incident prévoyant d'une part une vue d'ensemble plus détaillée sur la base de la documentation des différents événements et des mesures prises et, d'autre part, des enseignements et recommandations[651]. Elles peuvent également fournir sur la base de leur intervention un rapport forensique, plus complexe techniquement, qui peut ensuite être utilisé lorsqu'une attaque a été attribuée à une personne ou si l'incident est susceptible d'entraîner des conséquences juridiques[652].

647 COBIT 5, BAI01.13 ; ISO/IEC 27035-2 :2016, p. 11 ; NIST, *Computer Security Incident Handling Guide*, 2012, p. 38 et 44 ; LUNDELL, p. 11.

648 COBIT 5, BAI01.13 ; ISO/IEC 27035-1 : 2016, p. 12 ; NIST, 800-53, rev. 5, CP-2, p. 116 ss et IR-4, p. 152 ; OFAE, *Norme minimale pour améliorer la résilience informatique,* 2023, RS.IM-2, p. 34 ; ENISA, *How to set up CSIRT and SOC,* 2020, p. 22. À noter qu'il est essentiel de ne collecter que les données utiles, et non toutes les données en raison de leur disponibilité, cf. NIST, *Computer Security Incident Handling Guide,* 2012, p. 39 s. ; GILLIÉRON Philippe, *L'établissement d'un plan de réponse en cas de faille de sécurité* ; KRAL, p. 9 ; LUNDELL, p. 10. Pour plus d'informations au sujet des enseignements tirés, voir ISO/IEC 27035-2 : 2016, p. 27 ss.

649 ENISA, *Good Practice Guide for Incident Management,* 2010, p. 64.

650 NIST, *Computer Security Incident Handling Guide*, 2012, p. 39 ; JOHANSEN, p. 318.

651 LUNDELL, p. 11.

652 JOHANSEN, p. 324 ss.

5. Tout au long du processus

a. Un point de contact

(i) Les communications hors cyberincident

La prestataire de gestion de cyberincidents peut effectuer plusieurs types de communications et d'annonces dans le cadre de ses activités. Ces échanges peuvent être formels ou informels[653]. En amont d'un éventuel cyberincident, la prestataire de gestion de cyberincidents peut déjà être amenée à échanger des informations avec les entités qu'elle soutient, ce conformément à un plan de communication qui peut être établi à l'avance[654]. 318

Elle peut par exemple informer les différents services concernés des tendances ou des cybermenaces en cours[655]. Elle peut même avoir une tâche plus large de publication de contenus en la matière, permettant une information plus complète, ou, dans le cadre d'une potentielle activité de conseil, établir des lignes directrices, des meilleures pratiques ou des procédures techniques[656]. 319

(ii) Les échanges dans le cadre de la gestion de cyberincidents

Lorsqu'elle traite un cyberincident, la prestataire compétente peut être amenée à annoncer celui-ci à diverses personnes et pour de multiples raisons. Les diverses annonces peuvent être faites à l'interne comme à l'externe, pendant ou après la réaction à un tel événement[657]. 320

Sur le plan interne d'abord, la prestataire de gestion de cyberincidents peut avoir à communiquer une alerte, à savoir une information aux utilisatrices de l'activité visée par l'événement dommageable[658]. Elle peut aussi avoir à rendre des feedbacks, directement liés ou non à des incidents spécifiques, 321

653 Qui devront toutes être entreprises de manière sûre, cf. KILLCRECE et al., *State of Practice of CSIRT,* 2003, p. 105 ; WESTBROWN et al., p. 109 s. et 133. Au sujet de l'importance de l'établissement de mécanismes de partage d'informations, cf. notamment GCSP, *Guide to Developing a National Cybersecurity Strategy,* 2021, p. 40 ; UIT, *Guide pour l'élaboration d'une stratégie nationale de cybersécurité,* 2018, p. 41.

654 ISO/IEC 27035-1 : 2016, p. 11.

655 AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung,* 2018, p. 28.

656 Pour la fonction d'annonce, voir WEST-BROWN ET al., p. 68. Pour le conseil politique ou technique, voir FIRST, *CSIRT – Services Framework,* 2019, p. 54 ss.

657 ISO/IEC DIS 27002 : 2021, p. 45. Concernant la nécessité de coopérer au sein d'une organisation pour coordonner la capacité de répondre aux incidents, NIST, 800-53, rev. 5, IR-4, p. 154.

658 AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung,* 2018, p. 27 ; KILLCRECE et al., *Organisational Models for CSIRT,* 2003, p. 16 ; KILLCRECE et al., *State of Practice of CSIRT,* 2003, p. 98 ; WEST-BROWN et al., p. 25 et 94.

pour répondre aux requêtes de différentes interlocutrices, ainsi que des informations finales par suite de la clôture de l'incident[659]. Lors de la survenance d'un incident, la prestataire de gestion de cyberincidents peut être amenée à rendre compte de l'incident conformément aux voies hiérarchiques appropriées[660]. Il peut s'agir par là d'un signalement à la CISO, à la directrice des systèmes d'information (*Chief Information Officer,* CIO) ou à une autre supérieure[661]. En parallèle, les ressources humaines de l'organisation pourraient avoir à être informées de violations dans certaines circonstances, par exemple lorsque les collaboratrices sont affectées par une cyberattaque[662]. Tel peut être le cas notamment lors d'attaques d'hameçonnage ou de harcèlement par courriels. Finalement, il est souvent opportun d'informer le département juridique de l'organisation, dès lors qu'un cyberincident entraîne des conséquences juridiques, par exemple dans le cas où des données personnelles seraient concernées par l'incident ou lorsque des obligations légales pourraient être violées[663]. Dans l'autre sens, la prestataire de gestion de cyberincidents doit pouvoir accéder aux informations de l'organisation cliente lorsqu'elles sont nécessaires à son activité.

322 La prestataire de gestion de cyberincidents est susceptible de détenir des compétences de coordination dans le cadre de la communication[664]. La coordination sert à faciliter les transferts d'informations au sujet des cyberincidents entre la victime du cyberincident, les autres sites impliqués, les ressources humaines, le département juridique ou le département de relations publiques ainsi que les autorités d'application de la loi ou les services de télécommunication[665].

323 La prestataire de gestion de cyberincidents peut également être amenée à partager certaines informations à l'externe, bien que ces compétences soient

659 OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »,* 2021, p. 111 ; WESTBROWN et al., p. 68 et 100 s. La prestataire de gestion de cyberincidents doit se demander à la clôture de l'incident si elle doit informer particulièrement la victime de l'attaque, une autorité ou un partenaire, cf. ENISA, *Good Practice Guide for Incident Management,* 2010, p. 54.

660 ISO/IEC 27001 : 2013, A.16.1.2 ; NIST, 800-61, rev. 2, p. 34 ; OFAE, *Norme minimale pour améliorer la résilience informatique,* 2023, RC.CO-3, p. 36.

661 GILLIÉRON Philippe, *L'établissement d'un plan de réponse en cas de faille de sécurité* ; KILLCRECE et al., *State of Practice of CSIRT,* 2003, p. 107.

662 GILLIÉRON Philippe, *L'établissement d'un plan de réponse en cas de faille de sécurité*.

663 MEYER/MÉTILLE, *Computer security incident response teams : are they legally regulated ? The Swiss example,* 2022, p. 47.

664 Pour plus d'informations sur les fonctions de coordination, voir FIRST, *CSIRT – Services Framework,* 2019, p. 28 ss ; WEST-BROWN et al., p. 27 et 62.

665 WEST-BROWN et al., p. 27.

régulièrement attribuées à d'autres services[666]. Les communications peuvent être obligatoires ou facultatives[667]. Les communications obligatoires répondent à une obligation légale de fournir une information. Les prestataires de gestion de cyberincidents peuvent y être confrontées principalement lorsqu'une autorité de poursuite pénale requiert la transmission de moyens de preuve collectés durant la gestion d'un incident présentant une composante pénale. Il peut aller de la sorte également lorsqu'une infrastructure critique est visée par une cyberattaque devant être signalée sur la base des art. 74*a* ss LSI2[668]. La première situation renvoie à l'administration des preuves en procédure pénale et implique pour la prestataire de gestion de cyberincidents d'être attentive, lors de la documentation de son activité, au fait que son rapport est susceptible d'être exploité dans le cadre d'une procédure pénale. La seconde situation est susceptible de lui demander une attention plus particulière.

D'autres annonces doivent potentiellement être faites, à l'instar d'an- 324
nonces à la PFPDT et aux personnes concernées en cas de violation de la sécurité des données (art. 24 LPD), ou à d'autres autorités de surveillance[669]. Cela étant, il n'est pas certain que ces obligations incombent au sein d'une organisation à ses collaboratrices compétences pour la gestion de cyberincidents, encore moins à la partenaire contractuelle pour les incidents dans la sphère de sa cliente.

Pour ce qui est des communications facultatives, la prestataire de gestion 325
de cyberincidents peut annoncer, sur une base volontaire, toute cybermenace à l'OFCS qui peut fournir une recommandation quant aux mesures à prendre (art. 73b al. 1 LSI)[670]. Les expertes peuvent également échanger facultativement avec d'autres entités, à l'instar de partenaires, pour améliorer la gestion de cyberincidents. Dans certains cas, la communication d'informations, par exemple à une fournisseuse de services de télécommunication, peut avoir un

666 ISO/IEC 27035-1 : 2016, p. 11. Elle peut par exemple revenir à la RSSI, à la CISO, à un service de communication, au service juridique etc., ISO/IEC 27035-3 : 2020, p. 25 s.

667 MEYER/MÉTILLE, *Computer security incident response teams : are they legally regulated ? The Swiss example,* 2022, p. 47.

668 ISO/IEC 27035-1 : 2016, p. 11 ; ISO/IEC 27035-3 : 2020, p. 25 ; KILLCRECE et al., *State of Practice of CSIRT,* 2003, p. 107 ; WEST-BROWN et al., p. 117 s. Sur cette obligation, cf. *infra* N 521 ss.

669 Comme l'obligation de signaler les cyberattaques à la FINMA en vertu de l'art. 29 al. 2 LFINMA, cf. *infra* chapitre 4.I.C.5.c ; FINMA, *Communication FINMA sur la surveillance 05/2020 – Obligation de signaler les cyberattaques selon l'art. 29 al. 2 LFINMA*, 2020 ; NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques,* 2022, p. 18.

670 NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques*, 2022, p. 14.

impact positif[671]. Dans d'autres cas de figure, la transmission d'informations sur un événement détecté est bénéfique, par exemple dans la situation où l'événement a été identifié également au sein d'une organisation partenaire[672]. En outre, la prestataire de gestion de cyberincidents échange tout particulièrement des organisations détenant des compétences similaires, sur le plan national et sur le plan international[673]. Il est en effet possible de mettre au courant d'autres professionnelles, par exemple en prenant part aux échanges de données au sein du *Forum of Incident Response and Security Teams* (FIRST). De telles communautés et réseaux permettent les échanges d'informations et de bonnes pratiques. Ces communautés sont essentielles dans le fonctionnement d'une CSIRT ou d'une autre équipe de gestion de cyberincidents[674]. Finalement, les expertes en cybersécurité peuvent être amenées à échanger avec les médias, bien que la compétence de communication publique en cas de cyberincident leur incombe rarement. Une limite claire sur les compétences et sur ce qui peut être dit ou non doit être tracée au sein des organisations et un point de contact doit être créé pour échanger avec les médias[675].

b. La documentation

326 La documentation des mesures prises en vue de répondre à un cyberincident n'est pas légalement imposée en Suisse, à moins que des données personnelles soient affectées par l'incident (art. 15 al. 4 OPDo)[676]. Néanmoins, des recommandations internationalement reconnues font état de la nécessité, en accord avec la pratique, de documenter toutes les informations relatives à un incident[677]. Selon ces pratiques, il convient de documenter les questions « qui, quoi, où, pourquoi et comment » *(« Who, What, Where, Why and How »)*[678]. Il est important d'horodater les mesures prises depuis la détection d'un incident[679],

671 ISO/IEC 27035-1 : 2016, p. 11.

672 NIST, *Computer Security Incident Handling Guide*, 2012, p. 45.

673 ISO/IEC 27035-1 : 2016, p. 11 ; KILLCRECE et al., *Sate of Practice of CSIRT*, 2003, p. 107 ; NIST, *Computer Security Incident Handling Guide*, 2012, p. 47 ; OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »*, 2021, p. 160.

674 Cf. *infra* N 341 ss ; SALAMON, p. 130.

675 WEST-BROWN et al., p. 118 s. et 148 s.

676 OFJ, *Rapport explicatif OPDo*, 2022, p. 32.

677 La documentation est utile même en dehors de tout incident, voir par exemple NIST, 800-53, rev. 5, SA-5 pour la documentation du système ; AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung*, 2018, p. 104 pour la documentation des cybermenaces ; FIRST, *CSIRT – Services Framework*, 2019, p. 32 pour la documentation de vulnérabilités.

678 JOHANSEN, p. 316 ; KRAL, p. 5.

679 BSI-Standard 100-4, p. 74 s. ; NIST, 800-53, rev. 5, IR-5.

d'y faire figurer « le statut de l'incident, son résumé, les indicateurs, les incidents corollaires, les actions prises par les différents membres de l'équipe, l'analyse de l'impact lié à l'incident, les coordonnées des différentes parties impliquées, la liste des preuves réunies durant l'analyse de l'incident et les prochaines étapes »[680]. En effet, la documentation des événements, conversations et changements au sein des fichiers permet de traiter des problèmes plus efficacement, systématiquement et avec un plus bas taux d'erreur.

La prestataire de gestion de cyberincidents doit garder à l'esprit les différentes destinataires de sa documentation ; il peut s'agir du service juridique, du personnel IT, d'autorités d'application de la loi et ainsi de suite[681]. Elle doit également savoir quel type de rapport elle doit transmettre, principalement à sa cliente[682]. Le résultat de la documentation des informations et l'inventaire dressé sont utilisés tout d'abord pendant la réponse à un incident, mais aussi une fois l'incident clos. La documentation sert à disposer de moyens de preuve, à tirer des enseignements de la gestion d'un incident et à améliorer tout ce processus de sécurité[683]. La prestataire de gestion de cyberincidents peut effectivement par ce biais aider l'organisation lors de la réalisation d'obligations postérieures, lors de la réponse à de futurs incidents qui pourra être améliorée ou accélérée, lors de la prévention ou encore lors du développement d'un plan de continuité, contenant les objectifs et priorités de récupération, continuellement mis à jour[684]. 327

6. Des compétences accessoires

a. La gestion des vulnérabilités

En parallèle de leurs compétences de gestion d'incidents, les prestataires de gestion de cyberincidents peuvent être en mesure d'analyser les vulnérabilités et les risques qu'elles engendrent, afin de les corriger. Ces compétences s'exercent en collaboration avec les clientes, les fabricantes, d'autres spécialistes et d'autres personnes concernées par les vulnérabilités. 328

Lorsque des vulnérabilités sont découvertes ou suspectées et d'une façon similaire à la gestion de cyberincidents, elles doivent être analysées techniquement, afin de déterminer où elles se trouvent, comment elles peuvent être 329

680 NIST, 800-53, rev. 5, IR-5, p. 156 ; NIST, *Computer Security Incident Handling Guide*, 2012, p. 31 ; GILLIÉRON Philippe, *L'établissement d'un plan de réponse en cas de faille de sécurité*.

681 JOHANSEN, p. 319.

682 Sur les rapports, cf. *supra* N 317.

683 NIST, *Computer Security Incident Handling Guide*, 2012, p. 31 et 44 ; KRAL, p. 3. Au sujet des enseignements tirés, cf. *supra* N 316.

684 NIST, 800-53, rev. 5, CM-8, p. 107 s. et CP-2, p. 116 ss ; KRAL, p. 3.

exploitées et comment y remédier[685]. Après l'analyse, une réponse doit être donnée, en développant et en utilisant des correctifs et des solutions de contournement[686]. La réponse couvre aussi la notification de la stratégie aux autres interlocutrices et elle doit être coordonnée, comme la réponse aux incidents[687]. Ces informations sont ensuite partagées avec les clientes et les partenaires[688]. De la même manière que dans le cadre de la gestion des cyberincidents, il faut pouvoir détecter et appréhender les vulnérabilités. Cette tâche peut être attribuée à des prestataires de gestion de cyberincidents, à un autre service de sécurité informatique ou encore à la développeuse du produit informatique concerné[689].

b. La gestion de la qualité de la sécurité

330 La prestataire de gestion de cyberincidents peut également offrir des services de gestion de la qualité de la sécurité, ou *security quality management* pour aider une organisation à améliorer sa sécurité générale[690]. La gestion de la qualité de la sécurité peut englober les compétences d'analyse de risque et de soutien général à un département informatique. Il s'agit d'aider à augmenter la qualité des services préexistants et de diminuer indirectement le nombre d'incidents[691].

331 La prestataire de sécurité informatique constitue l'une des entités ou l'un des services présents en première ligne pour préparer une organisation à affronter des cybermenaces. Partant, elle peut agir au titre de conseillère technique ou politique[692]. En d'autres termes, elle peut être à même de conseiller dans un contexte de gouvernance sur la préparation des stratégies et des plans

685 NIST, 800-53, rev. 5, RA-5, SA-15. Pour quelques moyens de découvrir une vulnérabilité, voir FIRST, *CSIRT – Services Framework*, 2019, p. 32 s. ; pour l'analyse de vulnérabilités, voir notamment FIRST, *CSIRT – Services Framework*, 2019, p. 35 ss ; WEST-BROWN et al., p. 28.

686 FIRST, *CSIRT – Services Framework*, 2019, p. 39 ss.

687 FIRST, *CSIRT – Services Framework*, 2019, p. 37 s. ; KILLCRECE et al., *Organisational Models for CSIRT*, 2003, p. 18 ; WEST-BROWN et al., p. 28.

688 AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung*, 2018, p. 28 ; ISO/IEC 27001 : 2013, A.12.6.1 ; ENISA, *How to set up CSIRT and SOC*, 2020, p. 7.

689 Concernant la fonction de gestion des vulnérabilités de l'*IT vendor*, cf. WEST-BROWN et al., p. 62.

690 AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung*, 2018, p. 27.

691 KILLCRECE et al., *Organisational Models for CSIRT*, 2003, p. 14 s. ; KILLCRECE et al., *State of Practice of CSIRT*, 2003, p. 66.

692 ENISA, *How to set up CSIRT and SOC*, 2020, p. 7 ; FIRST, *CSIRT – Services Framework*, 2019, p. 56 ss ; WEST-BROWN et al., p. 33.

comme des procédures à suivre en cas de soupçon d'incident[693]. C'est également dans le cadre de la gestion de la qualité de la sécurité qu'elle peut être amenée à contribuer à la planification de la continuité des activités et de la reprise après sinistre[694].

Les expertes peuvent également fournir des conseils et former leur circonscription par la sensibilisation, la formation ou l'évaluation et la certification de produits[695]. Elles peuvent finalement contribuer à l'analyse d'une vue d'ensemble des cybermenaces. Les expertes peuvent mettre à disposition des personnes concernées un ensemble d'informations utiles en matière de cybersécurité grâce à la perspective unique qu'elles tirent de leurs expériences[696]. 332

c. Les compétences de renseignement

La prestataire de gestion de cyberincidents est susceptible de collecter des renseignements (ou de la CTI) exploitables stratégiquement, opérationnellement et tactiquement[697]. En outre, la CTI peut être utilisée par la prestataire de gestion de cyberincidents, qui en bénéficie à tout stade de la gestion d'un cyberincident. 333

Pour que la CTI remplisse sa finalité tactique, la prestataire de gestion de cyberincidents collecte des renseignements, notamment sur les traces pertinentes. La collecte doit se faire selon des procédés attestant de l'authenticité des renseignements dans le cadre de ses analyses et elle doit permettre une utilisation postérieure de ces informations. La prestataire de gestion de 334

693 NIST, 800-53, rev. 5, IR-1, p. 149 et IR-5, p. 152 ; FIRST, *CSIRT – Services Framework*, 2019, p. 56 ss ; NIST, *Computer Security Incident Handling Guide*, 2012, p. 44 ; KILLCRECE et al., *State of Practice of CSIRT*, 2003, p. 84.

694 KILLCRECE et al., *State of Practice of CSIRT*, 2003, p. 66. Les compétences de gestion de la qualité de la sécurité sont donc étroitement liées aux compétences préventives de cybersécurité.

695 AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung*, 2018, p. 30 ; ENISA, *How to set up CSIRT and SOC*, 2020, p. 8 ; FIRST, *CSIRT – Services Framework*, 2019, p. 7 et 50 ss ; NIST, *Computer Security Incident Handling Guide*, 2012, p. 24 ; FIRST, CSIRT 2019, p. 52 ss ; LUNDELL, p. 3 s. ; KILLCRECE et al., *Organisational Models for CSIRT*, 2003, p. 24 ; WEST-BROWN et al., p. 33 s. et 173.

696 WEST-BROWN et al., p. 32 s. À titre d'exemples : elle transmet ses coordonnées aux clientes, peut également transmettre de la documentation relative aux meilleures pratiques, cf. AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung*, 2018, p. 28 s. ; FIRST, *CSIRT – Services Framework*, 2019, p. 56 ss. Cette compétence fait plus précisément partie des services de « *situation awareness* », cf. ENISA, *How to set up CSIRT and SOC*, 2020, p. 7 ; FIRST, *CSIRT – Services Framework*, 2019, p. 8 et 42 ss ; WEST-BROWN et al., p. 25. La transmission d'informations peut, selon le contenu, également être considérée comme faisant partie des prestations proactives fournies par la prestataire de gestion de cyberincidents, cf. WEST-BROWN et al., p. 32.

697 Sur la CTI, cf. *supra* N 103 s.

cyberincidents peut également tirer un bénéfice de la CTI. Par exemple elle peut l'utiliser dans la phase de préparation aux cyberincidents, dans l'établissement d'une vue d'ensemble des menaces et des tendances futures, dans le processus de détection d'incidents comme au stade du tri grâce au *threat modelling,* ou dans la phase de réaction et des activités post-incident[698]. Elle devrait par ailleurs se tenir constamment informée en dehors de la survenance d'un incident, afin de maintenir les processus de collecte de renseignements à jour et de pouvoir identifier au mieux les attaques lorsqu'elles sont subies[699].

335 Les informations collectées dans ce contexte ont également un impact à d'autres niveaux, à savoir opérationnel ou stratégique. Les informations transmises par une prestataire de gestion de cyberincidents à ses supérieures devraient effectivement contribuer à appréhender les menaces pesant sur l'organisation et à les mettre à jour[700].

D. Des communautés et les organisations en développement

1. Les communautés

(i) De manière générale

336 Les États doivent encourager les infrastructures critiques à partager leurs connaissances et leurs pratiques en vue d'améliorer leurs capacités à prévenir, détecter les cyberincidents et y réagir[701]. Les échanges d'informations dans le domaine de la protection contre les cybermenaces ont lieu dans différents cercles, pour des questions diverses et ils mêlent le travail de nombreuses autorités et organisations. Ainsi, il faut appréhender cette question à plusieurs niveaux.

337 Toujours plus de plateformes sont créées, exploitées et soutenues afin de pallier un manque d'efficacité et de coopération[702]. Certaines communautés ou centres d'échange et de collaboration existent, sur le plan international comme sur le plan national, voire régional. Certaines communautés sont également propres à des secteurs d'activité. Les ISAC sont par exemple des centres d'échange d'informations qui se développent toujours plus en pratique. En

698 Dans la préparation, cf. ISO/IEC 27035-2 : 2016, p. 24 ; KIME, p. 10 ss. Pour la détection, cf. KIME, pp. 7 s. et 13 s. Au sujet de la *threat modelling* et du tri, cf. ISO/IEC 27031-2 : 2016, p. 16 ; ISO/IEC 27035-3 : 2020, p. 15. Sur l'analyse, cf. ISO/IEC 27035-3 : 2020, p. 16. Sur le confinement, l'éradication et la récupération, cf. KIME, p. 15 s. et pour l'utilisation de la CTI dans les activités post-incidents, cf. KIME, p. 16 s.

699 ISO/IEC 20735-3 : 2020, p. 16.

700 ISO/IEC 27035-2 : 2016, p. 26 ; KIME, p. 8 s. et 17 ss.

701 Le même constat a été formulé au sein de l'UE, cf. c. 120 Directive SRI2.

702 La Confédération soutient la création d'ISAC conformément à sa stratégie, CF, *CSN,* 2023, p. 16.

principe, un ISAC sert de plateforme à une branche ou à un secteur spécifique afin de permettre à un cercle spécifique d'organisations et potentiellement d'autorités ayant des intérêts communs d'échanger des informations entre interlocutrices de confiance[703]. Il peut également avoir une portée plus large. Au vu de leur nécessité en pratique, la CSN prévoit par ailleurs la mise en place d'un ISAC pour la Genève internationale pour favoriser l'échange d'informations et d'expériences entre les organisations internationales[704].

338 Les ISAC peuvent être créés entre organisations privées, publiques ou encore sous la forme de PPP[705]. Il n'existe à l'heure actuelle que peu d'ISAC en Suisse dans le domaine de la cybersécurité. L'art. 74 al. 2 litt. a LSI2 prévoit que l'OFCS met à disposition des infrastructures critiques un système de communication permettant l'échange sécurisé d'informations. Cette disposition sert de fondement légal pour que les relations entre l'OFCS et les infrastructures critiques puissent continuer par le biais du *Cybersecurity hub,* anciennement MELANI (et MELANI-NET)[706]. Ce canal d'information devrait également être utilisé par l'OFCS pour informer les infrastructures critiques de modes opératoires qui ne peuvent pas encore être rendus publics pour des raisons de sécurité[707]. Il est nécessaire de maintenir en Suisse de tels échanges d'informations en toute confiance, en tout cas entre l'OFCS et les infrastructures critiques[708]

339 Au vu de l'importance transfrontière de la cybersécurité, des communautés internationales existent et sont soutenues en Suisse également. La CSN de 2023 met notamment comme priorités la mise en place d'un ISAC pour la Genève internationale et l'encouragement des échanges avec les autorités internationales. La Suisse, désireuse de s'engager dans les règles internationales pour le cyberespace, compte participer activement aux processus de l'ONU, dont le Groupe de travail ouvert (OEWG) et les négociations relatives à une nouvelle Convention sur la cybercriminalité font partie intégrante[709].

340 Les autorités suisses peuvent également rejoindre des ISAC et des réseaux de collaboration, et contracter avec de telles organisations afin de collaborer au mieux à différents échelons et entre différentes actrices[710]. Les prestataires

703 ENISA, *ISAC,* 2018, p. 20 ss ; GHERNAOUTI, *Cybercriminalité,* 2023, p. 173 ss ; VON OW, p. 88.

704 CF, *CSN,* 2023, p. 32.

705 Les ISAC sont en principe plus formels que les autres PPP, cf. ENISA, *ISAC,* 2018, p. 12.

706 Au sujet de MELANI, cf. *supra* N 210 s.

707 FF 2023 84, p. 30.

708 Sur les flux de communications passant par l'OFCS, cf. *infra* N 730 ss.

709 CF, *CSN,* 2023, p. 22 et 32 s.

710 Concernant les réseaux avec lesquels la Suisse pourrait conclure, voir par exemple ce qui est instauré par la Directive SRI2 avec un groupe de coopération, un réseau de CSIRT et EU-CyCLONe (art. 17 Directive SRI2 ; c. 73 Directive SRI2).

de gestion de cyberincidents participent généralement aux efforts de coopération internationale ou opèrent même sous le couvert d'accords transnationaux[711]. Il est important de faire partie d'associations et autres regroupements pour faciliter l'échange d'informations au sujet des menaces, vulnérabilités et incidents et en vue d'augmenter le niveau global de cybersécurité[712].

(ii) Dans la pratique de gestion de cyberincidents

341 Durant plusieurs années, les prestataires de gestion de cyberincidents se liaient par des relations informelles bilatérales, ensuite formalisées. Pour leur permettre de contracter avec plus d'organisations aux compétences similaires et pour augmenter la confiance entre expertes, plusieurs associations et autres organisations ont été développées[713]. Par exemple, l'organisation FIRST a été fondée à la fin du XX^e^ siècle, poursuivant l'objectif d'établir une meilleure communication et une meilleure coordination entre les différentes CSIRT sur le plan international[714]. Les membres peuvent accéder à des outils et des procédés, et peuvent communiquer avec les autres membres en toute confiance pour optimiser les réponses aux incidents[715]. L'association propose un cadre constamment développé pour les services offerts par les CSIRT[716].

342 Certaines communautés sont plus spécialisées, étant donné que des questions similaires se posent pour des expertes dans des domaines comparables. Dans cet ordre d'idées, le groupe des CERT des gouvernements européens (*European Government CERT group,* EGC) est une association informelle des gouvernements européens et dont la Suisse fait également partie par l'inter-

711 MITROPOULOS/PATSOS/DOULIGERIS, p. 353. Voir par exemple le réseau des CSIRT au sein de l'UE, cf. art. 15 Directive SRI2.

712 GCSCC, *CSIRT – An Overview,* 2014, p. 8 ; RASHID/NOOR/ALTMANN, p. 448 s. Dans un sens similaire, SALAMON, p. 130.

713 ENISA, *Baseline Capabilities of National/Governmental CERT, Part 2,* 2010, p. 40 ; GFCE, *GFCE Global Good Practices – National Computer Security Incident Response Teams (CSIRT),* 2017, p. 15. Nous nous limiterons à aborder deux exemples revêtant un intérêt particulier pour la Suisse, mais il convient de noter qu'il en existe d'autres : à ce sujet, voir notamment GCSCC, *CSIRT – An Overview,* 2014, p. 14 s. ; DSOUZA, p. 212 s. ; KILLCRECE et al., *State of Practice of CSIRT,* 2003, p. 119 ss.

714 NIST, *Computer Security Incident Handling Guide,* 2012, p. 12 ; GCSCC, *CSIRT – An Overview,* 2014, p. 13 s. ; KILLCRECE et al., *State of Practice of CSIRT,* 2003, p. 20 et 47 ; WEBER/WILLI, p. 75.

715 ENISA, *Baseline Capabilities of National/Governmental CERT, Part 2,* 2010, p. 38 s. ; ENISA, *Good Practice Guide for Incident Management,* 2010, p. 87 ; DSOUZA, p. 212 ; SKOPIK/SETTANI/FIEDLER, p. 166.

716 ENISA, *How to set up CSIRT and SOC,* 2020, p. 6.

médiaire de GovCERT[717]. Elle a pour but de développer une coopération effective sur la gestion de cyberincidents en Europe. Pour ce faire, les membres de l'ECG développent conjointement des mesures, facilitent le partage d'informations, encouragent la formation de CERT gouvernementaux dans les États membres de l'UE et ainsi de suite[718].

Outre la coopération entre CSIRT et CERT, l'ensemble des intervenantes 343
dans le domaine doivent travailler conjointement sur le plan international. Afin d'illustrer cela, nous pouvons citer comme premier exemple l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), qui est l'entité principale de collaboration européenne. Établie en 2004 par le Parlement européen, ce centre d'expertise soutient les États membres et les institutions de l'UE pour les questions relatives à la sécurité des réseaux et de l'information[719]. L'agence encourage par ailleurs les différents États membres à l'échange d'informations et au partage de procédés pour la réponse aux cyberincidents. Elle soutient par ce biais les organes européens et les États membres de l'UE à trouver des réponses coordonnées aux cybermenaces[720]. Sa documentation est également utilisée comme source de documentation en Suisse[721].

À noter que, dans des domaines connexes comme celui de la lutte contre 344
la cybercriminalité, europol, eurojust ou interpol, collaborent étroitement avec les autorités de poursuite pénale suisses dans la lutte transfrontière contre les actes de criminalité perpétrés dans le cyberespace (notamment art. 350 s. CP)[722]. Certaines autorités étrangères ont également formé des alliances dans le domaine de la défense[723].

717 ENISA, *Baseline Capabilities of National/Governmental CERT, Part 2,* 2010, p. 39 ; OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »,* 2021, p. 54 ; GCSCC, *CSIRT – An Overview,* 2014, p. 13 ; SALAMON, p. 130.

718 ENISA, *Good Practice Guide for Incident Management,* 2010, p. 87 ; GCSCC, *CSIRT – An Overview,* 2014, p. 13.

719 ENISA, *Baseline Capabilities of National/Governmental CERT, Part 2,* 2010, p. 38. ENISA ne dispose pas d'un pouvoir de décision sur les citoyennes, cf. WEBER/WILLI, p. 75.

720 DSOUZA, p. 212 ; SKOPIK/SETTANNI/FIEDLER, p. 157.

721 Cf. par exemple OFAE, *Norme minimale pour améliorer la résilience informatique,* 2023, p. 5.

722 Au sujet d'Eurojust, voir OFJ, *Rapport d'activité 2021,* 2022, p. 15 ss ; OFJ, *Rapport d'activité 2022,* 2023, p. 8.

723 Voir par exemple les *Five Eyes* regroupant les services de renseignement d'Australie, du Canada, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis, qui collaborent et partagent conjointement des informations, cf. notamment UNITED STATES CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY et al., *Cybersecurity Best Practices for Smart Cities,* 19 avril 2023.

2. Une nouvelle entité : l'Institut national de test pour la cybersécurité

345 En Suisse, un nouvel Institut national de test pour la cybersécurité (NTC) a récemment été créé. Le NTC est une association (art. 60 ss du Code civil, CC). Son rôle était initialement perçu par la CSN comme complémentaire aux capacités du CYD Campus pour mener des évaluations indépendantes relatives aux risques de sécurité inhérents aux produits et services informatiques[724]. Il est néanmoins indépendant des autorités de la Confédération[725]. Sur son site Internet, le NTC annonce identifier et tester les vulnérabilités de tels produits en vue de mettre ses résultats à disposition de la population, des pouvoirs publics et des actrices de l'économie[726]. Dans les analyses publiées, il peut être délicat de comprendre exactement quelle est sa mission, à savoir s'il inspecte tout type de produits et services informatiques, s'il analyse uniquement des applications et si son expertise se limite à des aspects techniques. Compte tenu de ce qui précède, l'initiative tendant à l'établissement d'une telle organisation est intéressante pour la Suisse mais l'avenir nous dira ce qu'il adviendra de ce nouvel institut[727].

E. Une synthèse

346 Les intervenantes privées dans la cybersécurité sont nombreuses, d'une façon similaire à ce qui prévaut auprès des autorités compétentes. Les principales intervenantes sont les prestataires de gestion de cyberincidents. Il en existe une grande diversité : elles peuvent être internes aux organisations, externes, et une multitude de structures et de compétences existe.

347 Leurs compétences principales portent sur la gestion de cyberincidents. Elles peuvent disposer de compétences préventives. Ces compétences servent à réduire la probabilité de cyberincidents et à les anticiper. Les prestataires de gestion de cyberincidents peuvent aussi servir dans la détection d'incidents, par exemple en procédant à de la surveillance. Dans tous les cas, elles sont informées lors de la survenance de cyberincidents. À la suite de ces alertes, elles trient puis analysent les incidents et leurs différents composants. Les analyses poursuivent différentes finalités dont celles de comprendre l'étendue

724 CF, *CSN*, 2023, p. 17.

725 Le Conseil des États a par ailleurs enterré une motion visant à ce que la Confédération fournisse un soutien au NTC, Dépêche ATS, *Pas de soutien à l'Institut national de test pour la cybersécurité*.

726 NTC, *Mandat*.

727 MEYER Pauline, *TikTok : une analyse technique helvétique des risques de sécurité*.

de l'incident et de trouver les mesures réactives appropriées. Ces mesures tendent en principe à éviter que l'incident ne se propage, à l'éradiquer et à rétablir une situation sûre. D'autres compétences doivent être exercées tout au long de la gestion de cyberincidents, à l'instar des communications et de la documentation.

Les prestataires de gestion de cyberincidents peuvent détenir d'autres 348
compétences en parallèle de la gestion de cyberincidents. Certaines disposent de compétences dans la gestion de vulnérabilité, dans la gestion de la qualité de la sécurité ou encore dans le renseignement.

Au-delà de ces intervenantes principales, d'autres entités privées inter- 349
viennent activement dans la gestion de cyberincidents et dans la cybersécurité. Par exemple, les communautés et les plateformes d'échange d'informations existent en raison de la place centrale des échanges d'informations sont au centre des pratiques de cybersécurité. D'autres organisations non étatiques servent également de façon plus large à la cybersécurité, à l'instar du nouveau NTC en Suisse.

III. Une conclusion au chapitre 3

La cybersécurité implique l'intervention de nombreuses autorités et organi- 350
sations ainsi que leur étroite collaboration. Elle implique des compétences publiques et des compétences privées. Les compétences étatiques ont fait l'objet d'importants changements ces dernières années (I.A). La création en 2019 du NCSC a marqué un tournant dans l'organisation de la cybersécurité au sein de la Confédération. En janvier 2024, l'autorité principale pour la cybersécurité en Suisse a été transformée en office fédéral et a été déplacée au sein du DDPS.

Les compétences principales pour la cybersécurité sont conservées par 351
l'OFCS, mais sa position a été affaiblie par la création du nouveau service spécialisé de la Confédération pour la sécurité de l'information qui reprend les compétences du NCSC pour l'autoprotection de la Confédération. Le déplacement de l'OFCS au sein du DDPS a fait l'objet de critiques, de la même manière que son affaiblissement au profit du service spécialisé de la Confédération pour la sécurité de l'information, indépendamment du fait que son mandat reste officiellement le même que celui du NCSC.

L'OFCS n'est pas la seule autorité compétente pour des aspects de cyber- 352
sécurité en Suisse. D'autres autorités interviennent dans la protection de la Suisse contre les cybermenaces (I.B et C). En parallèle et au-delà du service spécialisé de la Confédération pour la sécurité de l'information, la connexité

de la cybersécurité à d'autres domaines implique l'intervention d'autres autorités telles que la PFPDT ou des autorités sectorielles, qui collaborent avec l'OFCS (I.D).

353 Certaines intervenantes privées sont également centrales à la cybersécurité. Les prestataires de gestion de cyberincidents sont les intervenantes principales dans la cybersécurité des différentes autorités et organisations. Une diversité de structures est possible mais ces prestataires doivent être présentes et établies bien avant qu'un incident survienne (I.A et B). Leurs compétences servent dans la prévention de cyberincidents, mais aussi dans leur détection et leur réaction (I.C).

354 D'autres intervenantes non étatiques existent et disposent de compétences importantes dans la cybersécurité (I.D). Il en va typiquement de la sorte pour les communautés et les plateformes d'échange d'informations. Elles permettent aux différentes intervenantes de bénéficier d'informations précieuses pour leurs tâches. Des organisations aux compétences diverses commencent à exister. Elles peuvent par exemple être actives dans l'analyse de vulnérabilités dans le partage d'informations avec différents groupes cibles.

355 Les deux premiers chapitres de cette étude ont permis de poser le cadre constitué des notions, des enjeux et des évolutions politiques en lien avec la cybersécurité. Le troisième chapitre a permis de mieux appréhender la multitude d'intervenantes dans la cybersécurité et la gestion de cyberincidents, principalement en Suisse.

356 Maintenant que les rôles des différentes intervenantes sont posés, il faut se pencher sur le cadre légal applicable aux autorités et organisations principales. Les infrastructures critiques ont été définies au chapitre 1[728] et n'ont pas été approfondies dans le cadre des intervenantes spécifiques pour la cybersécurité. En effet, elles sont les bénéficiaires du soutien de l'État et des prestations de gestion de cyberincidents. Elles détiennent néanmoins un rôle important en étant les premières responsables de leur cybersécurité. Il est maintenant nécessaire de voir quelles exigences légales s'appliquent à ces organisations et autorités qui font l'objet de réglementations et qui sont au centre de la présente recherche. Il conviendra également d'analyser le cadre légal applicable aux autres intervenantes principales, à savoir les prestataires de gestion de cyberincidents et l'OFCS, en parcourant également la réglementation des domaines connexes à la cybersécurité pour comprendre la coordination entre les différents instruments réglementaires.

728 Cf. *supra* N 73 ss.

Deuxième partie : un état des lieux du cadre réglementaire suisse

Chapitre 4 : le cadre réglementaire pour la cybersécurité des infrastructures critiques

Préambule au chapitre 4

La réglementation est l'un des leviers d'action pour encadrer la cybersécurité et pour inciter les différents groupes cibles à améliorer leur résilience face aux cybermenaces. La réglementation ne peut pas prévoir des exigences minimales de cybersécurité pour l'ensemble de la société civile, qui est confrontée à des pratiques, des menaces, des enjeux et des connaissances très diverses. En revanche, la nécessité de réglementer la cybersécurité des autorités et des autres infrastructures critiques est reconnue au sein de différents États dont la Suisse[729] (I.A). Le groupe cible des infrastructures critiques fera donc l'objet principal de ce chapitre consacré à l'examen du cadre légal et réglementaire suisse pour la cybersécurité. La réglementation s'entend dans un sens plus large que la législation ; elle comprend la législation adoptée par les pouvoirs législatifs, mais englobe aussi d'autres instruments réglementaires à l'instar du droit souple[730]. 357

L'analyse du cadre réglementaire ne peut pas se faire sans porter une attention particulière aux standards internationaux. En effet, la cybersécurité étant un domaine très technique, les différentes lois, ordonnances et instruments de droit souple suisse s'en inspirent fortement (I.B). 358

Le cadre réglementaire suisse pour la cybersécurité des infrastructures critiques se développe de façon sectorielle, en partenariat avec un État intervenant de façon subsidiaire et prônant l'autoréglementation (I.C). Certaines bases légales et réglementaires s'appliquent peu à peu de façon transversale à un nombre plus important de ces organisations (I.D). 359

Finalement, la cybersécurité faisant partie d'un ensemble de domaines composant la protection contre les cybermenaces, il n'est pas possible de se limiter à ce domaine. Il est nécessaire de parcourir les bases légales principales des domaines connexes que sont la poursuite pénale de la cybercriminalité et la cyberdéfense. Ce bref examen permettra de comprendre les interactions entre ces trois domaines étroitement liés dans le contexte juridique de la cybersécurité auprès des infrastructures critiques (II.). 360

729 CF, *CSN*, 2023, p. 21 ; CF, *Plan de mise en œuvre de la SNPC 2018-2022*, 2019, p. 31 ss ; CF, *SNPC 2018-2022*, 2018, p. 17 s.

730 Cf. *infra* N 366 ss et N 378 ; WISCHMEYER, p. 34 ss.

I. La cybersécurité comme domaine transversal et dispersé

A. La nécessité de légiférer au fil du temps

361 C'est à la suite des évolutions d'abord technologiques puis politiques[731] que la nécessité de légiférer en matière de cybersécurité est devenue claire. La réglementation doit constituer l'un des leviers pour inciter une amélioration de la résilience face aux cybermenaces[732].

362 La législation suisse en matière de cybersécurité se développe de façon dispersée, avec un État prônant l'autoréglementation et insistant sur le rôle subsidiaire et partenarial de l'État, notamment concernant ses compétences de réglementation et de législation[733]. En outre, le fédéralisme implique une cohabitation entre les compétences législatives de la Confédération et celles des cantons. Finalement, il est nécessaire de tenir compte des spécificités sectorielles ainsi que de la difficulté pour les autorités d'appréhender la cybersécurité sur le plan juridique et de s'adapter à la vitesse des évolutions technologiques[734].

363 La Suisse, comme de nombreux autres États, s'est tout de même engagée à mobiliser ses ressources pour améliorer la cybersécurité dans le pays. L'amélioration doit porter sur la cybersécurité des autorités et organisations étatiques, des infrastructures critiques ou encore d'autres entreprises et de la population. Il n'est pas possible à ce jour de concevoir l'adoption d'exigences minimales de cybersécurité applicables à l'ensemble de la société et de la même façon. Les individus n'utilisent pas la technologie de la même façon et avec les mêmes enjeux que des autorités étatiques, ne traitent pas le même genre d'informations, ne fournissent pas les mêmes prestations et les traitements d'informations effectués par des autorités sont, en raison des mandats de ces dernières, susceptibles d'engendrer des risques particuliers s'ils viennent à être compromis. Une approche réglementaire différenciée et fondée sur les

731 Cf. *supra* N 166 ss au sujet des stratégies illustrant l'intérêt porté par les autorités étatiques sur ces questions. Voir en ce moment la Motion 23.002 « Pour une meilleure sécurité des données numériques essentielles de la Suisse », déposée le 12 janvier 2023 par Josef Dittli, qui aspire à une meilleure réglementation pour la sécurité des informations critiques en Suisse.

732 GCSCC, *Cybersecurity capacity review – Switzerland*, 2020, p. 7 ; OFPP, *Protection de la population 27*, 2017, p. 14 s.

733 CF, *CSN*, 2023, p. 12 et 21 ; ChF, *Rapport « Suisse 2035, les grands défis de demain en 20 questions »*, 2022, p. 115 ; GCSCC, *Cybersecurity capacity review – Switzerland*, 2020, p. 13 ; WEBER/WILLI, p. 41.

734 FF 2017 2765, p. 2784 ss ; NICOLET/PEISSARD, p. 165.

risques associés aux activités de certaines organisations est nécessaire[735]. Pour ces raisons, la Suisse a emboîté le pas à ses voisines en limitant sa réflexion à l'introduction de certaines obligations de cybersécurité à un cercle restreint qui est celui des infrastructures critiques[736].

La cybersécurité auprès des infrastructures est réglementée de façon fragmentée en raison des spécificités sectorielles, du souhait partagé d'autoréglementation et de la volonté de l'État de conserver un rôle subsidiaire et partenarial. Certains instruments de droit contraignant et de droit souple ont été adoptés au fil du temps et continuent à être élaborés[737]. Les lacunes sont examinées de façon isolée et leur comblement se fait peu à peu le cas échéant[738]. En parallèle, certaines réglementations transversales sont adoptées et ont vocation à s'appliquer à une diversité d'infrastructures critiques[739]. 364

Pour adopter des réglementations adaptées aux évolutions technologiques ainsi qu'à la dimension transfrontière de la cybersécurité, les autorités de réglementation doivent tenir compte de standards internationaux[740]. Il faut donc disposer d'une vue d'ensemble de ces différents standards dont les instruments suisses s'inspirent. 365

B. La prise en compte de standards internationaux

1. Les références aux standards internationaux

Le cadre réglementaire suisse pour la cybersécurité auprès des infrastructures critiques est construit sur l'autoréglementation. Pour cette raison, il existe de nombreux types de normes applicables[741]. Le cadre réglementaire pour la cybersécurité auprès des infrastructures critiques se compose en Suisse 366

735 WISCHMEYER, p. 163.

736 CF, *CSN*, 2023, p. 21 ; CF, *Plan de mise en œuvre de la SNPC 2018-2022*, 2019, p. 31 ss ; CF, *SNPC 2018-2022*, 2018, p. 17 s. Sur la limitation aux infrastructures critiques pour l'introduction de l'obligation de signaler les cyberattaques, voir CF, *Rapport « Obligation de déclarer les incidents graves affectant la sécurité des infrastructures critiques »,* 2019, p. 7. Sur la notion d'infrastructure critique et sur son rôle, cf. *supra* N 73 ss.

737 Cf. *infra* N 378.

738 CF, *CSN*, 2023, p. 21.

739 Cf. *infra* N 518 ss.

740 Cf. *infra* N 377 ss.

741 SNV, *Le statut juridique des normes*, 2013, p. 1. À titre de comparaison et à toutes fins utiles, l'UE définit la « norme » comme « une spécification technique, approuvée par un organisme reconnu de normalisation, pour application répétée ou continue, dont le respect n'est pas obligatoire et qui relève » des normes internationales, européennes, harmonisées ou nationales, cf. art. 2 ch. 1 Règlement (UE) 1025/2012. La spécificité technique peut concerner les TIC, art. 2 ch. 5 Règlement (UE) 1025/2012.

de lois et d'ordonnances législatives, mais également d'autres instruments réglementaires dont de normes de droit souple. Indépendamment de leur caractère contraignant, ces normes renvoient régulièrement à des standards internationaux. Pour cette raison, il est important de parcourir ces standards et comprendre leur impact dans le cadre réglementaire helvétique.

367 Les standards internationaux constituent des normes, en principe de nature technique, qu'une organisation recommande de suivre dans l'accomplissement d'une tâche[742]. N'étant pas adoptées par une autorité détenant des compétences législatives, ces normes ne sont par essence pas juridiquement contraignantes. Elles peuvent néanmoins produire des effets juridiques dans certaines situations, typiquement si des actes législatifs y renvoient[743].

368 Le cadre légal renvoie effectivement parfois aux normes techniques ou aux standards internationaux, implicitement ou explicitement[744]. Tel est notamment le cas lorsqu'une loi ou une ordonnance prévoit un renvoi « à l'état de la technique » ou plus explicitement aux standards internationaux. Par exemple, l'art. 7 al. 1 LSI impose aux autorités et organisations assujetties d'organiser, de mettre en œuvre et de contrôler la sécurité de l'information « conformément à l'état des connaissances scientifiques et techniques »[745]. Pour un autre exemple, l'art. 23 litt. a de l'Ordonnance sur le dossier électronique du patient (ODEP) renvoie explicitement à une norme de l'Organisation internationale de normalisation (ISO) lorsqu'il en va des exigences applicables au moyen d'identification. L'art. 18 al. 1 de l'Ordonnance zougoise sur l'informatique (*Informatikverordnung*, ITV-ZG) renvoie aux standards reconnus *(« anerkannten Standards »)* pour la protection des moyens informatiques.

742 MONTAVON, p. 23.

743 SNV, *Le statut juridique des normes*, 2013, p. 2 s. Par exemple, les art. 4 de l'Ordonnance sur le courant fort et de l'Ordonnance sur le courant faible prévoient qu'à défaut de prescriptions de l'ordonnance pour la sécurité, l'on s'en tient aux règles techniques acceptées, dont en particulier les normes internationales reconnues des art. 4 al. 2 et, à défaut, aux normes suisses. Dans le sous-secteur des télécommunications, l'OFCOM est habilitée à déclarer obligatoires des normes de sécurité techniques harmonisées au niveau international en vertu de 31 al. 2 litt. b LTC pour l'importation, l'offre, la mise à disposition sur le marché et la mise en service d'installations de télécommunication.

744 Les notions de standard et de normes techniques, qui n'ont à l'origine pas de caractère légal, sont à distinguer de celle de norme de droit et s'utilisent de manière générale dans les domaines techniques et scientifiques. Les standards sont élaborés par des organisations de droit privé non autorisées à légiférer et leur application est volontaire, cf. CF, *Rapport « Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense »*, 2021, p. 4, 7 et 9. Les normes techniques servent à standardiser des états de fait techniques, cf. SNV, *Le statut juridique des normes*, 2013, p. 1 ; FLÜCKIGER, p. 340.

745 Le message précise que les assujetties doivent s'inspirer de la norme DIN ISO/IEC 27001, cf. FF 2017 2765, p. 2829.

Dans un contexte connexe, l'art. 3 de l'Ordonnance sur les accidents majeurs (OPAM) impose à toute détentrice d'une entreprise, d'une voie de communication ou d'une installation de transport par conduites de prendre les mesures propres à diminuer le risque correspondant notamment « à l'état de la technique de sécurité ». Comme exemple de norme de droit souple, la Norme minimale pour améliorer la résilience informatique de l'Office fédéral de l'approvisionnement économique du pays (OFAE) précise les standards internationaux sur lesquelles elle se base ; il en va de même pour les autres manuels et normes plus spécifiques[746]. Il convient maintenant de parcourir quels sont, justement, ces standards internationaux principaux dont certaines infrastructures critiques devraient s'inspirer pour assurer un certain niveau de cyberrésilience[747].

2. Les cadres du NIST

De nombreuses autorités réglementaires et législatives suisses s'inspirent largement des cadres du *National Institute of Standards and Technology* (NIST)[748]. Le NIST est une autorité de normalisation américaine. Il a adopté plusieurs recommandations dans le domaine de la cybersécurité, que ce soit de pour les secteurs critiques ou plus largement pour l'industrie[749]. Les projets sont adoptés conjointement entre les secteurs privé et public aux USA[750]. Ils visent en premier lieu les organisations américaines mais ne s'y limitent pas et peuvent revêtir un intérêt pour d'autres organisations. 369

Le cadre du NIST est largement reconnu dans le monde et est souvent utilisé comme source d'inspiration en Suisse notamment. Il couvre de manière générique tous les types de cyberrisques[751]. Il s'articule autour de trois points : 370

746 OFAE, *Norme minimale pour améliorer la résilience informatique,* 2023, p. 5. Pour un exemple de norme applicable à un secteur de l'approvisionnement, basée sur la norme minimale TIC de l'OFAE, cf. AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung,* 2018, p. 125 ss.

747 L'on peut s'inspirer également des standards cités par le CF pour la sécurité des produits dans le domaine de la cybersécurité, cf. CF, *Rapport « Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense »,* 2021, p. 16 s.

748 Cf. par exemple la révision de l'OApEl ou la Norme minimale pour améliorer la résilience informatique de l'OFAE, sur laquelle se basent les normes pour les différents secteurs de l'approvisionnement.

749 NIST, *Framework for Improving Critical Infrastructure Cybersecurity,* 2018, p. V ; HUSI-STÄMPFLI/MORAND, p. 126 ; SALAMON, p. 108 ; WEBER/WILLI, p. 77.

750 NIST, *Framework for Improving Critical Infrastructure Cybersecurity,* 2018, p. IV.

751 CF, *Rapport « Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense »,* 2021, p. 10 ; RNS, *Recommandations de mise en œuvre des organisations cantonales pour la cybersécurité,* 2021, p. 30 et 37.

the Framework Core, the Framework Tiers et *the Framework Profiles*[752]. Le cadre pour la cybersécurité du NIST est en voie de révision et un *Cybersecurity Framework 2.0* a été mis en consultation publique en 2023 et adopté en 2024[753]. Le *Framework Core* de la première version se concentre sur cinq fonctions simultanées et continues qui sont l'identification, la protection, la détection, la réponse et la récupération[754]. La version 2.0 ajoute une fonction de gouvernance en amont de l'identification[755]. Ce cadre apporte une base de considérations communes à tous les secteurs et les entreprises, ainsi que des recommandations détaillées permettant l'élaboration de profils organisationnels individuels[756]. Le *Framework Profiles* permet de décrire la posture actuelle d'une organisation et celle visée pour sa cybersécurité en fonction de ses résultats par rapport aux fonctions du *Framework Core*[757]. Finalement, le *Framework Tiers* se focalise sur la progression d'une organisation dans sa gestion de la cybersécurité ainsi que sur la visualisation de l'organisation des caractéristiques de sa gestion de la cybersécurité, en vue d'établir des priorités et d'atteindre les objectifs fixés[758]. Le *Framework Tiers* permet d'attribuer des valeurs ou des niveaux à des pratiques, en allant du 1 (partiel) au 4 (dynamique), passant par le 2 (consciente des risques) et le 3 (reproductible). En d'autres termes, il s'agit d'un barème où la valeur 0 implique qu'une mesure n'est pas

752 NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, 2018, p. V ; ce cadre est reconnu également par les industries et les infrastructures critiques suisses, cf. OFAE, *Norme minimale pour améliorer la résilience informatique*, 2023, p. 5, ainsi qu'en Europe, cf. ENISA, *National Capabilities Assessment Framework*, 2020, p. 62.

753 NIST, *The NIST Cybersecurity Framework (CSF) 2.0*, 2024.

754 ENISA, *National Capabilities Assessment Framework*, 2020, p. 62 ; SKOPIK/SETTANI/FIEDLER, p. 164.

755 NIST, *Public Draft : The NIST Cybersecurity Framework 2.0*, 2023, p. 5 ; NIST, *The NIST Cybersecurity Framework (CSF) 2.0*, 2024, p. 3.

756 NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, 2018, p. 3. En d'autres termes, cela revient à établir un profil selon le résultat de l'ajustement d'une entreprise aux fonctions, cf. NIST, *Public Draft : The NIST Cybersecurity Framework 2.0*, 2023, p. 8 ; NIST, *The NIST Cybersecurity Framework (CSF) 2.0*, 2024, p. 1 ; SSIGE, *Norme minimale pour garantir la sécurité des technologies de l'information et de la communication (TIC) requises dans l'approvisionnement en gaz*, 2020, p. 39.

757 NIST, *Public Draft : The NIST Cybersecurity Framework 2.0*, 2023, p. 8 s. ; NIST, *The NIST Cybersecurity Framework (CSF) 2.0*, 2024, p. 6 ; SKOPIK/SETTANI/FIEDLER, p. 164.

758 ENISA, *National Capabilities Assessment Framework*, 2020, p. 62 s. ; NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, 2018, p. 3 s. ; NIST, *Public Draft : The NIST Cybersecurity Framework 2.0*, 2023, p. 13 ; NIST, *The NIST Cybersecurity Framework (CSF) 2.0*, 2024, p. 7 s. À noter qu'outre les cadres qu'il a adoptés, le NIST a élaboré d'autres documents, à l'instar des lignes directrices concernant plus spécifiquement la gestion de cyberincidents, établissant les compétences et processus d'une équipe de réponse aux incidents, qui servent parfois également de lignes directrices pour différents milieux en Suisse.

mise en œuvre par une organisation, la valeur 1 équivaut à la mise en œuvre partielle sans définition complète de la mesure ou validation de celle-ci, et la valeur 2 signifie la mise en œuvre partielle d'une mesure entièrement définie et acceptée. La valeur 3 revient à la mise en œuvre entière ou presque de façon définitive ou statique, et la valeur 4 équivaut à la mise en œuvre dynamique d'une mesure, son contrôle et son amélioration permanente[759].

3. Les normes ISO

L'ISO est une association de droit suisse composée d'organismes nationaux de normalisation. Elle est régulièrement amenée à travailler conjointement avec la Commission internationale électrotechnique (IEC)[760]. L'ISO a notamment publié la « Suite ISO 2700x », qui est composée de différentes normes se complétant dans le cadre de la sécurité informatique et qui est souvent considérée comme faisant partie des standards les plus pertinents en pratique[761]. Parmi ces standards figure la norme ISO 27001, la plus connue, qui prévoit l'établissement et l'exploitation d'un système de gestion de sécurité de l'information (SGSI, aussi appelé système de management de l'information, SMSI), servant à l'élaboration auprès des organisations d'un cadre de référence pour gérer la sécurité de l'information et l'intégrer aux systèmes existants[762]. Les normes de cette suite, en particulier ISO 27001 et 27002, sont pertinentes pour toute organisation ; elles peuvent donc s'appliquer aux organismes publics comme aux organisations des milieux économiques ou à but lucratif[763]. 371

Des normes concernent des aspects plus concrets de la cybersécurité, comme la norme ISO/IEC 27032 pour la sécurité sur Internet ou la famille ISO/IEC 27035 pour la gestion d'incidents de sécurité de l'information, qui s'applique en sus des normes de base ISO/IEC 27001 et ISO/IEC 27002[764]. D'autres 372

759 NIST, *Public Draft : The NIST Cybersecurity Framework 2.0,* 2023, p. 26 ss ; NIST, *The NIST Cybersecurity Framework (CSF) 2.0,* 2024, p. 8 ; OFAE, *Norme minimale pour améliorer la résilience informatique,* 2023, p. 37 s.

760 ISO/IEC 27000 : 2018, p. IV. Ces deux organisations indépendantes à but non lucratif élaborent des normes internationales d'application volontaires sur la base d'un consensus international, cf. ISO/IEC, *Le recours et la référence aux normes ISO et IEC dans les politiques publiques,* 2015, p. 3 s.

761 Les autorités suisses renvoient fréquemment aux normes ISO dans le cadre des renvois à l'état de la science et de la technique, cf. notamment pour la cybersécurité auprès des autorités et des organisations de la Confédération, NCSC, *Si001,* 2022, p. 4. Sous-entendu au niveau de la loi, cf. art. 7 al. 1 LSI, FF 2017 2765, p. 2829.

762 ISO/IEC 27001 : 2022, p. V ; CF, *Rapport « Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense »,* 2021, p. 10 et 22 s. ; HUSI-STÄMPFLI/MORAND, p. 126 ; SALAMON, p. 110.

763 ISO/IEC 27000 : 2018, p. 1.

764 Pour une liste des normes ISO en fonction des étapes de gestion de cyberincidents, cf. KÖNIGS, p. 145.

normes sectorielles peuvent s'appliquer, à l'instar de la norme ISO/IEC 27011 pour le domaine des télécommunications ou encore l'ISO/IEC 27019 dans le domaine de l'industrie des opérateurs de l'énergie[765].

373 À noter que contrairement à de nombreux standards internationaux, les normes ISO sont payantes, ce qui soulève des questions d'accessibilité. La Cour de justice de l'Union européenne (CJUE) a estimé dans une situation que des normes ISO pouvaient être manifestement obligatoires pour un cercle d'assujetties, si un règlement européen y renvoie et qu'elles précisent le droit. Par conséquent, les normes devaient dans ce contexte être accessibles au titre de droit de l'Union[766]. Cette décision intervient dans un contexte particulier, où des normes harmonisées spécifiaient des droits et des obligations, prévues dans un règlement, pour les justiciables. Ces normes leur étaient nécessaires pour vérifier si un produit ou un service était conforme aux exigences de la législation. Cette décision est européenne, donc elle ne s'applique pas telle quelle en Suisse[767]. Cette décision n'impacte par ailleurs pas l'accessibilité des normes ISO auxquelles des lois ne renvoient pas. En ce qui concerne les normes auxquelles des lois renvoient, mais sans que le respect de la norme constitue une condition à la conformité à des exigences légales, la question demeure ouverte.

4. D'autres documents fréquemment utilisés

374 *Control Objectives for Information and Related Technology* (COBIT) est un référentiel développé par l'*Information Systems Audit and Control Association* (ISACA)[768], prévoyant un cadre de plusieurs processus de contrôle représentant la dépendance des processus d'entreprise aux informations et ressources informatiques. Le cadre assiste les entreprises dans la réalisation de leurs objectifs en matière de gestion de gouvernance pour leur utilisation des technologies de l'information[769]. COBIT décrit les objectifs exigeant un traitement des informations sûr et ordonné. Il s'articule autour de sept exigences qui sont la confiance, la disponibilité, l'intégrité, l'effectivité, l'efficience, la conformité

765 KÖNIGS, p. 146. Voir pour l'imbrication entre ces normes et les normes ISO générales : ISO/IEC 27009 : 2020, p. 4 s.

766 CJUE, C-588/21 P, Public.Resource.Org et Right to Know/Commission, 5 mars 2024, en particulier c. 79 s., 82 et 84.

767 Bien que la Suisse ait tout intérêt à prendre en compte les décisions européennes dans sa pratique.

768 ISACA est une association internationale composée de professionnelles de l'informatique et est active dans la certification dans le domaine de l'audit, du contrôle et de la sécurité informatique, cf. WEBER/WILLI, p. 75.

769 ISACA, COBIT 5, p. 13.

et la fiabilité. COBIT comprend des éléments de mesure de la performance, des facteurs de succès et ainsi de suite[770]. Le cadre COBIT 5, adopté en 2012, a été remplacé par COBIT 2019.

Le *Bundesamt für Sicherheit in der Informationstechnik* (BSI) allemand, 375
fondé en 1991, est une agence neutre et indépendante pour la sécurité informatique. Ses tâches sont prévues dans la *Deutsches Gesetz für Sicherheit in der Informationstechnik* (BSIG-D) et comprennent surtout l'investigation des risques de sécurité dans l'utilisation des technologies de l'information ainsi que le développement de mesures et de solutions de sécurité adaptées[771]. Dans le cadre de ses compétences et se basant sur les normes internationales susmentionnées[772], le BSI met à disposition également des standards de bases pour les TIC, importants en pratiques[773]. Ils sont élaborés en prenant déjà en considération d'autres référentiels tels que celui du NIST ou de l'ISO[774], et sont pris en compte en Suisse dans l'élaboration des normes minimales sectorielles pour l'utilisation des technologies de l'information et de la communication. La norme BSI 200-1 prévoit des exigences générales pour un SGSI. Le BSI Standard 200-2 présente une méthodologie pour la protection informatique, et le BSI Standard 200-3 fait part d'une méthode pour effectuer une analyse de risques pouvant être utilisée avec les principes du BSI Standard 200-2. Le BSI standard 100-4 se concentre sur la gestion d'incidents et la continuité des activités[775]. Ce dernier prévoit la continuité de l'activité, même en cas de situation critique[776]. Ce standard prévoit des compétences en matière de réponse aux incidents, en proposant l'institution d'une cellule de crise, d'un personnel de crise élargi et de différentes unités, sans se limiter aux CERT[777]. Le standard s'intéresse à la mise en place d'une planification et de son implémentation pour les situations d'urgence, avec une distinction opérée entre les vulnérabilités, les situations d'urgence et les crises[778].

770 WEBER/WILLI, p. 70.

771 Le BSI effectue également des évaluations de la sécurité de systèmes informatiques et des analyses de tendances en la matière, WEBER/WILLI, p. 76.

772 BSI-Standard 100-4, p. 5 ss.

773 WEBER/WILLI, p. 76.

774 Ainsi que d'autres normes internationalement reconnues, voir BSI-Standard 100-4, pp. 5-9 ; BSI, *Informationssicherheit mit System*, 2021, p. 11.

775 BSI-Standard 100-4, p. 4.

776 BSI-Standard 100-4, p. 7 s. Pour les autres standards, voir BSI-Standard 100-4, p. 4 ; BSI, *Informationssicherheit mit System*, 2021, p. 10.

777 BSI-Standard 100-4, p. 20 ss.

778 BSI-Standard 100-4, p. 65.

376 Au niveau américain et outre le NIST, le SANS et l'*US Industrial Control Systems Cyber Emergency Response Team* (ICS-CERT) ont publié des recommandations sur lesquelles se fondent des normes suisses, comme les mesures générales de protection pour les systèmes de contrôle industriels (SCI), dont l'importance est reconnue pour la disponibilité et l'intégrité de nombreuses infrastructures critiques[779]. L'Agence européenne chargée de la sécurité des réseaux et de l'information (*European Union Agency for Cybersecurity,* ENISA) a également publié plusieurs directives *(guidelines)* ayant vocation à guider des pratiques respectant la cybersécurité[780]. Il existe encore d'autres standards internationaux, parfois applicables à certains domaines spécifiques ou à portée plus transversale[781].

C. Les lois applicables aux secteurs et sous-secteurs critiques

1. Une introduction aux réglementations sectorielles

377 Comme la présente étude l'a déjà mentionné, le cadre légal et plus largement réglementaire[782], pour la cybersécurité auprès des infrastructures critiques en Suisse, se développe principalement de façon sectorielle. Pour cette raison, il n'existe pas une loi centralisée en droit suisse imposant des exigences minimales de cybersécurité à l'ensemble des infrastructures critiques.

378 Il existe en Suisse neuf secteurs critiques dont font actuellement partie vingt-sept sous-secteurs critiques[783]. Les autorités et organisations actives dans ces différents sous-secteurs ne sont pas soumises aux mêmes exigences. Certaines normes s'appliquent à des cercles plus ou moins étendus d'organisations. Il convient de parcourir les différents sous-secteurs critiques et les

779 NCSC, *Rapport semestriel 2021/1,* 2021, p. 29. Le SCI est un système commandant ou surveillant un processus physique, terme largement utilisé dans le domaine de la production industrielle, NCSC, *Mesures de protection pour les SCI,* 2020, p. 3.

780 Voir notamment son *Good Practice Guide on National Cyber Security Strategies* pris en compte notamment dans la Norme minimale pour améliorer la résilience informatique de l'OFAE, cf. OFAE, *Norme minimale pour améliorer la résilience informatique,* 2023, p. 5 ; CF, *Rapport « Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense »,* 2021, p. 11.

781 Cf. par exemple, OCDE, *Recommandation du Conseil sur la sécurité numérique des activités critiques,* 2023. Dans le domaine des télécommunications, il y a les recommandations et des normes de l'UIT comme ITU-T X.1051. Pour d'autres exemples, cf. CF, *Rapport « Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense »,* 2021, p. 10 ss.

782 Le terme de réglementation englobe dans le cadre de la présente étude l'activité législative et les autres normes par essence non contraignantes adoptées par différentes entités, à l'instar des normes minimales ou circulaires sectorielles. Pour une utilisation similaire, cf. CF, *La FINMA et son activité de réglementation et de surveillance*, 2014, p. 23.

783 Cf. *supra* N 74 et 77 ; FF 2023 1659, p. 6 et 24 ss.

réglementations prévues en droit suisse afin de comprendre comment le cadre réglementaire appréhende la cybersécurité des infrastructures critiques. Une diversité de normes est susceptible de s'appliquer aux organisations considérées comme telles. Au vu de la multitude d'instruments existants, la présente analyse cherche principalement à illustrer la diversité de normes à prendre en considération par les infrastructures critiques lorsqu'il en va de leur cybersécurité. L'objectif n'est pas de lister de manière exhaustive l'ensemble des normes existantes en constante évolution.

2. Le secteur critique des autorités

a. Le secteur

Le secteur critique des autorités regroupe la recherche et l'enseignement, les biens culturels ainsi que le parlement, le gouvernement, la justice et l'administration. Le sous-secteur critique de l'enseignement et de la recherche couvre les organisations offrant des prestations basées sur les résultats des recherches en cas de catastrophe et de situation d'urgence (par exemple par le service sismologique). Le sous-secteur critique des biens culturels englobe les organisations qui offrent des prestations d'importance majeure lorsqu'il en va de la création d'une identité culturelle et de la garantie de la sécurité du droit (en particulier en rapport avec les archives étatiques)[784]. Les autorités et organisations actives dans le sous-secteur critique du parlement, du gouvernement, de la justice et de l'administration offrent des prestations essentielles par la législation, par la conduite et l'exécution des tâches de l'État, par la jurisprudence et l'application de la loi ou encore par les tâches administratives d'ordre général comme le maintien de la sûreté intérieure ou l'alerte et l'alarme en cas de danger[785]. 379

Les organisations visées par ces différents sous-secteurs peuvent être communales, cantonales ou fédérales. Il va donc de soi que les actes législatifs applicables ne sont pas uniquement adoptés par la Confédération. À titre d'exemples et indépendamment des questions de cybersécurité, les archives fédérales et cantonales sont réglées à différents niveaux de législation. Sur le plan fédéral, l'art. 1 de la Loi sur l'archivage (LAr) s'applique. Au niveau cantonal et pour un exemple, l'art. 2 de la Loi vaudoise sur l'archivage (LArch-VD) et son règlement d'application sont applicables aux autorités du canton de Vaud, aux communes ainsi qu'aux délégataires de tâches publiques cantonales et communales. Il en va de même pour l'enseignement qui englobe les écoles fédérales à l'instar de l'École polytechnique fédérale de Zurich (EPFZ), 380

784 Pour d'autres définitions de la notion de bien culturel, cf. BANDLE/RENOLD, p. 18 ss.

785 FF 2018 491, p. 521 ; FF 2023 1659, p. 24.

soumise à la Loi fédérale sur les écoles polytechniques fédérales (Loi sur les EPF), ainsi que les universités et les hautes écoles cantonales, comme l'Université de Lausanne (UNIL) régie par la Loi vaudoise sur l'Université de Lausanne (LUL-VD) et ses règlements d'application[786].

381 Les différentes autorités du gouvernement sont, de la même manière, réglées au niveau fédéral comme au niveau cantonal ou communal. Ces autorités administratives revêtent d'une part un statut particulier du fait qu'elles sont soumises au principe de la légalité. C'est pourquoi celles-ci seront prises comme exemple, en se limitant au niveau fédéral et au niveau cantonal, pour illustrer le cadre légal leur étant aujourd'hui applicable. D'autre part, de nouvelles lois sont adoptées pour ce sous-secteur et illustrent la volonté de légiférer sur la cybersécurité.

b. La Loi sur la sécurité de l'information et son ordonnance

382 La nouvelle Loi fédérale sur la sécurité de l'information (LSI) s'applique dans son ensemble à l'Assemblée fédérale (AF), au Conseil fédéral (CF), aux tribunaux de la Confédération, au Ministère public de la Confédération et à son autorité de surveillance, ainsi qu'à la Banque nationale suisse (art. 2 al. 1 LSI). Dans la mesure où ces autorités délèguent fréquemment des tâches à des organisations, une partie importante des dispositions de la loi s'appliquent à ces dernières. Il en va des Services du Parlement, de l'administration fédérale, des services administratifs des tribunaux de la Confédération, de l'armée et des organisations de l'art. 2 al. 4 de la loi sur l'organisation du gouvernement et de l'administration (LOGA). Certaines dispositions s'appliquent aux infrastructures critiques (art. 2 al. 5 LSI, concernant les mesures de la Confédération visant à protéger la Suisse contre les cyberrisques) ou aux cantons lorsqu'ils traitent des informations classifiées de la Confédération ou accèdent aux moyens informatiques de celle-ci, à condition qu'ils ne garantissent pas une sécurité de l'information au moins équivalente (art. 3 al. 1 LSI)[787]. L'art. 2 de l'Ordonnance sur la sécurité de l'information (OSI) reprend l'art. 2 LSI et précise les dispositions de l'ordonnance s'appliquant aux différentes autorités et organisations.

383 Les exigences concrètes entre sécurité de l'information, sécurité informatique et cybersécurité sont étroitement liées. La LSI suit une approche intégrale en matière de sécurité de l'information, visant tout d'abord la protection des

786 À noter que certaines lois s'appliquent tant aux entités fédérales que cantonales, voir par exemple la LEHE.

787 FF 2017 2765, p. 2786 s. ; CF, *Rapport « Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense »* 2021, p. 13 ; HUSI-STÄMPFLI, N 26 ss ; MEYER/MÉTILLE, *Loi fédérale sur la sécurité de l'information : version 2.0,* 2022, N 5 ss.

informations, ensuite la sécurité informatique, puis finalement la sécurité des personnes et de l'exploitation[788]. La loi, technologiquement neutre, ne vise pas exclusivement les traitements informatisés d'informations et n'a donc pas comme objet la stricte cybersécurité. Elle contient néanmoins des considérations de cybersécurité. La cybersécurité couvre la sécurité de l'information traitée par le biais de moyens informatiques et la sécurité de ces moyens informatiques[789]. Cette loi poursuit notamment l'objectif d'améliorer la capacité de résistance de la Suisse face aux cyberrisques. Elle est donc naturellement centrale dans le domaine de la cybersécurité (art. 1 al. 1 litt. b LSI2)[790].

La LSI a un impact sur la cybersécurité en Suisse de deux façons différentes. 384
Elle impose d'une part aux autorités et organisations des art. 2 s. LSI des exigences minimales pour garantir la sécurité de l'information et la sécurité des moyens informatiques. D'autre part, elle prévoit les signalements de cybermenaces et de cyberattaques, principalement par les infrastructures critiques[791].

La LSI impose des exigences minimales aux autorités et organisations de 385
la Confédération (qui nous intéressent présentement) pour garantir la sécurité de l'information. Les art. 6 ss LSI imposent des obligations générales aux autorités pour garantir la confidentialité, la disponibilité, l'intégrité et la traçabilité des informations. Celles-ci doivent assurer la protection contre les utilisations abusives et les perturbations des moyens informatiques auxquelles elles recourent (art. 6 al. 2 et 3 LSI)[792]. Pour ce faire, les autorités doivent évaluer les besoins de protection des informations relevant de leurs compétences ainsi que les risques (art. 6 al. 1 et art. 8 LSI) ou encore être aptes à gérer des violations de la sécurité de l'information (art. 10 LSI). En parallèle, la loi prévoit les principes guidant la classification des informations (art. 11 ss LSI) ainsi que les mesures à mettre en place pour assurer la sécurité des moyens informatiques compte tenu de la catégorie de protection à laquelle ils appartiennent (art. 16 ss LSI)[793].

788 CF, *Rapport « Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense »,* 2021, p. 24.

789 Sur la délimitation entre ces notions, cf. *supra* N 45 ss.

790 NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques,* 2022, p. 13. À noter que son entrée en vigueur a pour conséquence la reprise et l'abrogation de l'aOPCy et de l'aOPrI, cf. art. 47 al. 1 OSI ; SG-DDPS, *Législation d'exécution relative à la LSI, Rapport explicatif,* 2022, p. 6 et 24.

791 Pour plus d'informations sur l'obligation de signaler les cyberattaques ciblant les infrastructures critiques, cf. *infra* N 521 ss ; FF 2017 2765, p. 2787 s. ; FF 2023 84, p. 35 ; MEYER/MÉTILLE, *Loi sur la sécurité de l'information : version 2.0,* 2022, N 8 s.

792 OA, *Enquête administrative « Fuite de données »,* 2024, N 240 s. ; HUSI-STÄMPFLI, N 29.

793 FF 2017 2765, p. 2790 s. et 2822 ss ; OA, *Enquête administrative « Fuite de données »,* 2024, N 242 ; MEYER/MÉTILLE, *Loi fédérale sur la sécurité de l'information : version 2.0,* 2022, N 14 ss.

386 La loi impose des mesures générales, en prévoyant par exemple que les autorités et organisations soumises à la loi veillent à ce que les risques en matière de sécurité de l'information soient constamment évalués (art. 8 al. 1 LSI) ou que les violations de la sécurité de l'information soient détectées rapidement, leurs causes clarifiées et leurs conséquences limitées au maximum (art. 10 al. 1 LSI). Elle impose également aux autorités et organisations soumises à la loi de garantir la sécurité des moyens informatiques qu'elles exploitent (art. 19 al. 1 LSI). La loi ne définit pas de mesures détaillées, mais elle constitue la base légale formelle sur laquelle les autorités compétentes peuvent s'appuyer pour adopter des ordonnances et des directives sur la sécurité de l'information.

387 Plusieurs ordonnances d'exécution de la LSI existent aujourd'hui. L'OSI est l'ordonnance principale et elle détaille les mesures prévues par la loi. Elle impose des obligations plus concrètes, à l'instar de la formation et de la sensibilisation des collaboratrices par les unités administratives (art. 11 OSI) pour que celles-ci soient en mesure d'identifier les dangers et les menaces, de réagir correctement et de procéder aux communications correspondantes[794].

c. Un exemple d'autre loi pertinente

388 La LSI est la loi centrale pour la cybersécurité, mais sa première version vise expressément la sécurité de l'information et des moyens informatiques pour les autorités et organisations de la Confédération. En parallèle, d'autres lois tiennent compte de considérations ayant trait à la sécurité de l'information. Il en va typiquement de la sorte pour la nouvelle Loi fédérale sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités (LMETA). La loi se coordonne avec la LSI pour ce qui a trait à la sécurité de l'information dans le contexte de l'utilisation des moyens électroniques par les autorités de l'administration fédérale centrale.

389 La LMETA est entrée en vigueur en janvier 2024. La loi vise à créer les conditions permettant d'assurer la collaboration entre les autorités et différentes collectivités en matière d'utilisation des moyens électroniques facilitant l'exécution des tâches des autorités, ainsi que d'élargir et développer l'utilisation de ces moyens censés faciliter l'exécution des tâches des autorités (art. 1 LMETA). Elle s'applique à l'administration fédérale centrale. Les autorités assujetties doivent tenir compte des risques pour la sécurité de l'information, pour la sécurité et la disponibilité des données et des services, et pour la protection des données (art. 3 al. 5 LMETA). Le message de la LMETA prévoit que les mesures permettant de garantir la sécurité de l'information se fondent sur la LSI, tout en insistant sur la nécessité pour les autorités d'adopter une

794 SG-DDPS, *Législation d'exécution relative à la LSI, Rapport explicatif*, 2022, p. 15.

approche fondée sur le risque également dans le contexte de l'utilisation des moyens électroniques[795]. Ces différents aspects sécuritaires doivent également, si nécessaire, être déterminés par les conventions, entre les autorités assujetties et des collectivités, sur la mise en œuvre technique et organisationnelle de la collaboration en matière d'utilisation des moyens électroniques (art. 4 al. 2 litt. d LMETA)[796]. La loi anticipe également d'autres aspects de sécurité dans ce contexte, notamment lorsqu'il en va de la publication de code source de logiciels développés par les autorités assujetties ou pour l'exécution de leurs tâches (art. 9 LMETA), de l'exploitation des données ouvertes (art. 10 LMETA), ou encore des projets pilotes (art. 15 LMETA)[797].

d. D'autres instruments pour les autorités de la Confédération

En parallèle, l'art. 85 LSI et différentes dispositions de l'ordonnance habilitent 390
les autorités compétentes à élaborer des directives de sécurité informatique pour les unités administratives. Le CF a délégué en vertu de l'art. 85 al. 2 LSI la compétence au Centre national pour la cybersécurité (NCSC) d'édicter des normes techniques[798]. C'est sur ce fondement que le NCSC a adopté la directive Si001 pour la protection informatique de base dans l'administration fédérale[799]. Cette directive restera applicable durant les trois ans qui suivent son entrée en vigueur (art. 51 al. 1 OSI). L'OFCS a repris depuis le mois de janvier 2024 la compétence du NCSC d'adopter de telles directives jusqu'à 2025, date à partir de laquelle le service spécialisé de la Confédération disposera de cette compétence réglementaire (art. 29 al. 1 OSI par renvoi de l'art. 51 al. 6 OSI)[800].

La directive Si001 est une norme pour la catégorie de sécurité « protection 391
de base », constitutive d'exigences standard conformément aux art. 17 al. 1 et 85 LSI[801]. De telles directives ont une valeur de recommandations, à moins que les autorités soumises à la LSI les déclarent obligatoires (art. 85 al. 3 LSI). Les art. 17 al. 1 et 18 al. 2 LSI prévoient que tous les moyens informatiques exploités par les autorités soumises à la loi doivent satisfaire aux exigences minimales

795 FF 2022 804, p. 56.

796 FF 2022 804, p. 57.

797 Le message de la LMETA prévoit par ailleurs que, lors de la réalisation de projets pilotes ayant trait à la numérisation des prestations de l'administration fédérale, le NCSC doit systématiquement être consulté pour les aspects liés à la sécurité de l'information (art. 15 al. 5 LMETA), cf. FF 2022 804, p. 88.

798 FF 2017 2765, p. 2879 s.

799 NCSC, *Si001*, 2022. La directive a initialement été adoptée sur la base de l'art. 11 al. 1 litt. e aOPCy. Elle va demeurer en vigueur durant les six années suivant l'entrée en vigueur de l'OSI (art. 48 al. 1 OSI).

800 SG-DDPS, *Législation d'exécution relative à la LSI, Explications*, 2023, p. 26 s.

801 FF 2017 2765, p. 2879.

de la catégorie de sécurité « protection de base », sous réserve de relever d'une catégorie supérieure au sens de l'art. 17 al. 2 et 3 LSI. La LSI attribue donc un caractère contraignant à la directive Si001 pour les autorités de l'art. 2 al. 1 LSI (art. 18 al. 2 LSI)[802]. Des normes à l'instar de cette directive peuvent typiquement être reprises par d'autres autorités et par les cantons[803].

392 La directive Si001 tend à développer des procédures de sécurité et la sécurité des réseaux. Elle sert à concrétiser la protection informatique de base et s'accompagne de documentation[804]. Inspirée de la norme ISO/IEC 27002, elle pose des exigences concernant l'organisation, le personnel, la technique et les informations. D'autres exigences relatives aux systèmes informatiques, aux applications et aux zones doivent être respectées lorsque des objets à protéger correspondants sont utilisés[805].

393 Il existe d'autres instruments de droit souple ayant trait à certaines questions plus spécifiques, à l'instar des lignes directrices pour l'intelligence artificielle au sein de l'administration fédérale. Ces lignes directrices constituent un cadre d'orientation général[806]. Elles prévoient des généralités en termes de sécurité, et imposent la résilience des systèmes d'intelligence artificielle, leur robustesse et leur sûreté. Ces orientations doivent être prises en compte dès la conception de systèmes d'intelligence artificielle afin d'éviter leur utilisation à des fins abusives ou de façon erronée[807]. La ligne directrice sur la sécurité est générale et devrait être concrétisée. En outre, bien que l'Office fédéral de la communication (OFCOM) soit satisfait de la prise en compte des lignes directrices par l'administration fédérale et que les collaboratrices des autorités semblent trouver la ligne directrice au sujet de la sécurité adéquate, force est de constater que cette dernière ne semble pas ressortir davantage du rapport de l'OFCOM, ce qui questionne au sujet de son implémentation au sein de l'administration fédérale. Les personnes interrogées par l'OFCOM considèrent qu'il n'est pas nécessaire de préciser davantage cette ligne directrice, contrairement à celle qui consiste à placer l'être humain au centre de l'IA, raison pour laquelle il semble que les questions de sécurité ne sont, pour le moment, pas suffisamment considérées (ou que la sécurité ne pose pas spécialement de questions, car déjà parfaitement maîtrisée, ce qui nous semble

802 NCSC, *Protection de base*, avril 2022.

803 FF 2017 2765, p. 2880.

804 NCSC, *Si001,* 2022, p. 1.

805 NCSC, *Si001,* 2022, p. 8.

806 CF, *« Intelligence artificielle » – lignes directrices pour la Confédération,* 2020, p. 2.

807 CF, *« Intelligence artificielle » – lignes directrices pour la Confédération,* 2020, p. 5 ; OFCOM, *Suivi des lignes directrices « Intelligence artificielle » pour la Confédération,* 2022, p. 5.

difficile à admettre)[808]. Malgré le manque de clarté des lignes directrices quant aux questions de cybersécurité, la LSI et son ordonnance permettent d'appréhender des technologies comme l'intelligence artificielle (IA). Les organisations soumises à la LSI doivent veiller à la sécurité des moyens informatiques qu'elles exploitent, ce qui inclut implicitement la sécurité des systèmes informatiques auxquels l'IA est intégrée. La LSI est naturellement insuffisante pour appréhender toutes les questions juridiques gravitant autour de l'IA.

e. Les normes cantonales

En raison du fédéralisme, les cantons sont responsables de légiférer pour la sécurité de l'information qui les concerne[809]. La LSI ne s'applique aux cantons que dans deux situations : premièrement, lorsqu'ils traitent des informations classifiées de la Confédération ou qu'ils accèdent aux moyens informatiques de cette dernière (art. 3 LSI). Pour respecter le principe de subsidiarité, la LSI s'applique aux cantons dans les cas uniquement où les cantons en question n'assurent pas une sécurité au moins équivalente à celle de la Confédération[810]. Deuxièmement, elle s'applique aux cantons dans le cadre de la protection de la Suisse contre les cyberrisques qui sont soumis à l'obligation de signaler les cyberattaques et dans le cadre de la coopération entre le NCSC et les infrastructures critiques (art. 73*a* ss LSI2, en particulier art. 74*b* al. 1 litt. b LSI2). 394

Peu de cantons ont réglementé la cybersécurité, mais certains ont élaboré, au fil des années, des normes en partie similaires à la LSI. Le canton de Lucerne dispose par exemple d'un art. 12 dans son Ordonnance sur la sécurité informatique (*Informatiksicherheitsverordnung*-LU) qui prévoit la protection tant des infrastructures informatiques que des informations traitées. Dans la mesure où l'on se situe dans un cadre cyber, l'on peut admettre que l'ordonnance impose la garantie de la cybersécurité, du moins par une partie de l'administration cantonale ou lorsque ses infrastructures informatiques sont utilisées (voir le champ d'application de la loi à l'art. 2 *Informatiksicherheitsverordnung*-LU). Le canton de Berne est actuellement en train d'adopter une loi sur la sécurité de l'information et la cybersécurité (LSIC-BE), dont le contenu devrait se rapprocher de la LSI. 395

Autrement, la majorité des cantons ont édicté des lois ou des ordonnances prévoyant d'une part les compétences principales en matière de cybersécurité, de sécurité de l'information ou de sécurité informatique et, d'autre part, les 396

808 Au sujet de la sécurité, CF, *« Intelligence artificielle » – lignes directrices pour la Confédération*, 2020, p. 5 ; OFCOM, *Suivi des lignes directrices « Intelligence artificielle » pour la Confédération*, 2022, p. 5.

809 FF 2017 2765, p. 2787.

810 FF 2017 2765, p. 2787 s.

mesures à prendre pour assurer un niveau adéquat de sécurité, les questions de responsabilité et de contrôle y étant liées[811]. En d'autres termes, la majorité des cantons ont adopté les lignes directrices de leur stratégie et ont prévu les compétences principales[812], ainsi que des principes généraux, typiquement par l'obligation faite aux autorités cantonales de protéger des incidents leurs systèmes informatiques et les informations qu'elles traitent[813].

397 Il en va de la sorte dans le canton de Vaud qui instaure les différentes compétences pour l'élaboration et la mise en œuvre de la politique de sécurité des systèmes d'information, et qui pose le principe de la propre responsabilité des services de l'administration cantonale pour assurer leurs besoins en matière de sécurité (en particulier art. 10 al. 1 Règlement relatif à l'informatique cantonale, RIC-VD)[814]. À noter que les hautes écoles sont expressément exclues du champ d'application du règlement (art. 2 al. 1 RICVD). Genève prévoit aux art. 34 s. de son Règlement genevois sur l'organisation et la gouvernance des systèmes d'information et de communication (ROGSIC-GE) les bases relatives à la sécurité de l'information ; ces dispositions prévoient les principes directeurs de la sécurité de l'information et l'élaboration d'une politique de sécurité de l'information. Le canton de Zurich a légiféré en termes de sécurité de l'information. L'ordonnance en vigueur mentionne les niveaux de protection pour les informations traitées par les organes publics ainsi que la définition d'un plan et de mesures appropriées pour protéger celles-ci (art. 12 s. de l'ordonnance zurichoise sur la gestion et la sécurité de l'information, *Verordnung über die Informationsverwaltung und -sicherheit*, IVSV-ZH)[815]. Le canton de Berne

811 Par exemple IKTV-SZ à Schwyz ou à St. Gall, le Règlement sur l'exploitation et la sécurité de l'informatique municipale.

812 Les cantons attribuent souvent des compétences au Conseil d'État, au département compétent pour la sécurité informatique et à d'autres autorités lorsqu'il en va respectivement du pilotage et de la mise en œuvre des stratégies, cf. par exemple les art. 5 s. ISV-BS, l'ITV-ZG ou, de manière plus générale, la Convention de Schaffhouse sur l'*e-government* (E-GovV-SH) et la stratégie informatique. À Bâle-Ville, c'est la Chancellerie d'État qui édicte notamment les directives sur les mesures organisationnelles et techniques pour la protection des informations (art. 11 *Geschäftsordnung Information und Datenschutz*-BS).

813 Il en va de la sorte pour le canton d'Appenzell Rhodes-Extérieures à l'art. 4 eGovG-AR ou encore dans les Grisons avec l'art. 12 IKTV-GR.

814 Cf. art. 4, 7 et 15 RIC-VD pour les compétences du Conseil d'État et du Département de la sécurité informatique (DSI, aujourd'hui DGNSI pour Direction générale du numérique et des systèmes d'information).

815 Un renvoi est effectué à l'art. 3 litt. 2 IDG-ZH, qui ne limite pas la notion d'information aux seules données personnelles mais inclut tous les enregistrements qui concernent l'accomplissement d'une tâche publique. Il en va de même pour le canton de Lucerne qui a édicté une Ordonnance sur la sécurité informatique (cf. art. 3 al. 1 *Informatiksicherheitsverordnung*-LU).

dispose également d'ordonnances prévoyant les compétences pour la gestion et le pilotage des technologies de l'information et de la communication (TIC) dans l'administration cantonale et imposant des responsabilités et obligations pour assurer la sûreté de l'information et la protection des données dans l'utilisation des TIC (voir l'Ordonnance de Direction concernant la sûreté de l'information et la protection des données, OD SIPD-BE, et l'Ordonnance sur les technologies de l'information et de la communication de l'administration cantonale, OTIC-BE). Le pouvoir législatif lucernois détaille déjà dans la loi (davantage comparé aux autres cantons) les principes et obligations s'imposant dans les traitements d'informations et dans l'utilisation de systèmes informatiques au sein des autorités soumises à la loi (art. 12 ss *Informatiksicherheitsverordnung*-LU)[816].

398 D'autres cantons, à l'instar d'Appenzell Rhodes-Intérieures, ont réglé quelques-unes des questions du domaine de la cybersécurité à l'aide d'autres instruments[817]. De multiples cantons se dotent actuellement de stratégies et d'autres instruments administratifs pour guider les autorités cantonales dans la mise en œuvre de la cybersécurité ou de la sécurité de l'information. Le canton de Genève a par exemple adopté une politique de la sécurité de l'information ainsi que d'autres instruments politiques pour compléter et détailler le ROGSIC-GE[818]. En plus de sa réglementation sur la sécurité de l'information, le canton de Schaffhouse a donné la possibilité à la prestataire de services informatiques cantonale de réglementer davantage les mesures à prendre[819]. À noter qu'en parallèle des normes de droit, certains instruments guident les cantons dans la mise en œuvre de la Cyberstratégie nationale (CSN) et de la cybersécurité en leur sein[820].

399 Parallèlement à ces normes, la majorité des cantons ont plus largement légiféré en matière de cyberadministration, en posant les principales compétences de pilotage et de mise en œuvre de leur stratégie ou en réglementant la gestion de portails sécurisés. Ces instruments législatifs prévoient quelques dispositions supplémentaires de sécurité des données, généralement personnelles, traitées dans le cadre des prestations fournies par l'État

816 Pour un exemple analogue, cf. art. 23 ss IKTV-SZ qui imposent des mesures techniques à l'instar de la pseudonymisation et de l'anonymisation.

817 Le canton d'Appenzell Rhodes-Intérieures a effectivement prévu les mécanismes de base pour la sécurité de l'informatique dans l'activité des membres d'autorités cantonales dans une décision de la Commission de déontologie (cf. en particulier art. 7 *InfoBeschluss-AI*).

818 DGSI, *Politique de Sécurité de l'Information*, 2014, p. 6.

819 Cf. respectivement art. 3 al. 1 litt. c, 5 ss et 13 ISV-SH.

820 Voir, comme instrument, RNS, *Recommandations de mise en œuvre des organisations cantonales pour la cybersécurité*, 2021.

aux administrées. L'application de ces lois plus ou moins détaillées est souvent limitée soit à un guichet virtuel servant de point de contact entre les autorités publiques et les personnes utilisant des prestations électroniques, soit aux traitements de données personnelles par les autorités soumises à ces réglementations[821]. La réglementation fribourgeoise prévoit, dans cet ordre d'idées, quelques normes visant à la sécurité notamment de l'utilisation systématique du numéro assurance-vieillesse et survivants (AVS) (art. 21 de la Loi fribourgeoise sur la cyberadministration, LCyb-FR) et des numéros uniques d'identification des entreprises (IDE) et numéros d'enregistrement non significatif (REE) (art. 24 LCyb-FR) ou concernant les données personnelles traitées (art. 25 LCyb-FR). Au-delà de tels traitements de données personnelles, l'annexe 5 du projet pilote de l'Ordonnance fribourgeoise concernant la mise en œuvre du Référentiel cantonal de données de personnes (ORCDo-FR), vient préciser que la sécurité de l'information et la sécurité informatique doivent être garanties par le Service de l'informatique et des télécommunications (SITel) (art. A5-1 de l'annexe 5). Cette annexe spécifie également que les opérations de traitement sur les données du Référentiel cantonal doivent faire l'objet d'une procédure de journalisation en vue d'analyser les accès aux données, de mettre en évidence la survenance de dysfonctionnements et de répondre aux besoins de surveillance (art. A5-2 ORCDo-FR)[822].

400 Les cantons sont également soumis à un cadre particulier en matière de vote électronique. Cela implique que des exigences de cybersécurité peuvent être applicables sur cette question en particulier. Le vote électronique est progressivement mis en place depuis plusieurs années en Suisse et trouve maintenant son ancrage principalement dans l'Ordonnance sur les droits politiques (ODP) et l'Ordonnance de la Chancellerie fédérale (ChF) sur le vote électronique (OvotE). La restructuration de la législation en matière de vote

821 La sécurité est encore régulièrement traitée dans la législation par le biais de la protection des données personnelles, cf. SOLOVE/HARTZOG, p. 137. À titre exemplatif, l'art. 3 litt. e LCyb-FR prévoit que le « guichet virtuel désigne l'infrastructure sécurisée s'appuyant sur les technologies de l'information et de la communication par laquelle les usagers et usagères obtiennent des informations ou des prestations de l'administration » ; l'art. 3 litt. a LGSU-NE prévoit que le « guichet virtuel sécurisé désigne l'infrastructure sécurisée de communication utilisée entre les autorités cantonales et communales et les utilisateurs pour toutes les prestations s'appuyant sur les technologies de l'information et de la communication » ; cf. également art. 5 litt. g LAEL-GE.

822 Le Référentiel cantonal consiste en un « *ensemble de données communes à plusieurs applications* » (art. 17 al. 2 LCyb-FR) ou une « infrastructure numérique [...] [qui] propose un annuaire de données pouvant être partagées, contenant des données de référence des personnes et organisations qui sont en interaction et/ou en relation directe avec un organe de l'État » (art. 2 ORCDo-FR).

électronique cherchait entre autres à renforcer la sécurité des systèmes[823]. L'ODP et l'OvotE prévoient des exigences à respecter pour les essais de vote électronique, des dispositions relatives à l'agrément en vue de la tenue d'un scrutin électronique, au contrôle des systèmes et des modalités d'exploitation, à la gestion des incidents ou encore à la vérification de l'exactitude du résultat du vote électronique[824].

Finalement, certains cantons soutiennent leurs communes dans la cybersécurité de ces dernières, notamment par le biais de conventions. Par exemple, le canton de Vaud a conclu une convention avec les communes vaudoises. Celle-ci concerne pour le moment davantage des questions de collaboration et de soutien par le canton plutôt que des exigences minimales. Elle recommande cependant déjà la mise en place de mesures minimales pour bénéficier du soutien du canton. La convention prévoit que des standards minimaux vont être adoptés par le canton et transmis aux communes[825]. 401

f. Les obligations d'annonce

Les autorités fédérales, cantonales et communales sont soumises à l'obligation de signaler les cyberattaques en vertu de l'art. 74*b* al. 1 litt. b LSI2. Il est particulièrement important de connaître la fréquence et l'origine des attaques ciblant les autorités de tous les niveaux[826]. 402

Elles sont également susceptibles d'être soumises à l'obligation d'annoncer des violations de la sécurité des données si les conditions de l'art. 24 de la Loi sur la protection des données (LPD) sont réunies. 403

Ces obligations transversales de signaler seront approfondies plus tard, dès lors qu'elles ne sont pas limitées à un secteur critique, mais qu'elles s'appliquent transversalement à un cercle d'organisations plus large[827]. 404

g. En conclusion

La LSI pose une série d'exigences pour inciter les autorités et les organisations de la Confédération d'assurer un certain niveau de cybersécurité. La loi, son ordonnance et les autres actes d'exécution adoptés par les autorités compétentes permettent un réel pas en avant. 405

823 ChF, *Révision partielle de l'ordonnance sur les droits politiques et révision totale de l'ordonnance de la ChF sur le vote électronique*, 2022, p. 4.

824 Cf. notamment art. 11 ODP, ch. 14 de l'Annexe OVotE.

825 UNION DES COMMUNES VAUDOISES / ASSOCIATION DE COMMUNES VAUDOISES / ÉTAT DE VAUD, *Convention de cybersécurité entre le Canton et les communes (Mandat de prestations, contrat de droit administratif)*, 4 juillet 2023.

826 FF 2023 84, p. 35.

827 Cf. *infra* N 521 ss.

406 La majorité des cantons disposent de compétences principales et réglementent en tout cas les aspects stratégiques liés à la cybersécurité. Sur le plan opérationnel, nous pouvons voir que certaines questions sont traitées, mais pas la cybersécurité dans son ensemble. Il n'existe que peu d'exigences minimales de cybersécurité pour les autorités cantonales. Il semble délicat pour les autorités communales de disposer de réglementations pour assurer leur cybersécurité, bien que toujours plus d'initiatives impliquant un canton et ses communes existent. En revanche, l'ensemble des autorités fédérales, cantonales et communales sont soumises à l'obligation de signaler les cyberattaques sur la base des art. 74a LSI2.

407 Les organisations actives dans le sous-secteur critique de l'enseignement et de la recherche ne sont pas soumises à des exigences minimales légales de cybersécurité. Il n'est pas exclu que les organisations concernées disposent de lignes directrices internes, mais le cadre réglementaire n'impose pas d'obligations aux institutions soumises à la compétence législative fédérale. Il semble en aller de même en ce qui concerne les institutions à qui s'applique une compétence législative cantonale. Le sous-secteur critique des biens culturels n'est pas non plus réglementé en termes de cybersécurité.

Schéma 10 : la réglementation du secteur critique des autorités[828]

Secteur critique des autorités	Réglementé	Partiellement réglementé			Non réglementé
		Exigences légales	Exigences non contraignantes	Obligation(s) de signaler	
Parlement, gouvernement, justice, administration					
Fédéral	×				
Cantonal		×	×	×	
Communal				×	
Recherche et enseignement				×	
Biens culturels					×

828 Certaines autorités communales disposent d'exigences non contraignantes, à l'instar de ce qui commence à prévaloir dans le canton de Vaud ; néanmoins, la situation dans le canton évolue encore et de nombreuses communes en Suisse ne disposent pas d'exigences de cybersécurité, même non contraignantes. C'est pourquoi le schéma ne compte pas de coche pour les exigences de cybersécurité applicables aux autorités communales.

3. Le secteur critique de l'énergie

a. Le secteur

Le secteur critique de l'énergie se compose de l'approvisionnement en gaz naturel, en pétrole et en électricité ainsi que du chauffage à distance et la chaleur industrielle. L'approvisionnement en gaz naturel englobe son commerce, son transport, son stockage et sa distribution. L'approvisionnement en pétrole (en combustibles et carburants de type essence ou kérosène) couvre également la chaîne d'approvisionnement en entier et il en va de même pour l'électricité. La production et la distribution de chaleur à distance et de chaleur industrielle composent le dernier sous-secteur critique[829]. 408

Plusieurs instruments légaux s'appliquent à ces différents sous-secteurs. Il existe des compétences fédérales et cantonales s'agissant de la législation sur l'énergie (art. 89 à 91 Cst.) Il n'est donc pas exclu que des cantons légiférant sur les aspects sécuritaires, à leur niveau et dans les limites de leurs compétences, lorsqu'il en va de la sécurité informatique ou de la cybersécurité auprès de certaines actrices dans la chaîne d'approvisionnement de différentes énergies. Les cantons exigent comme la Confédération que l'approvisionnement énergétique soit, entre autres, sûr. Sur le plan fédéral et comme nous allons le voir avec quelques exemples, certaines lois prévoient la mise en place de mesures et des obligations d'annonce applicables à certaines actrices actives dans ces sous-secteurs. 409

b. Les lois générales

(i) La Loi fédérale sur l'énergie

L'art. 7 de la Loi fédérale sur l'énergie (LEne) introduit les principes directeurs gouvernant l'approvisionnement énergétique. Parmi ceux-ci, l'art. 7 al. 1 LEne dispose que l'approvisionnement énergétique doit être sûr, ce qui « implique une disponibilité énergétique suffisante en tout temps, une offre d'énergie diversifiée ainsi que des systèmes d'approvisionnement et de stockage techniquement sûrs et efficaces ». Ce principe implique également que les infrastructures critiques doivent être protégées, y compris les infrastructures d'information et de communication y étant liées. Cette protection, devant être assurée par les actrices compétentes pour l'approvisionnement en électricité, en pétrole et en gaz naturel, doit être garantie contre les événements et incidents tels que les catastrophes naturelles, mais également contre les cyberattaques malveillantes. À ce titre doivent être protégées toutes les installations, les 410

829 FF 2018 491, p. 521 ; FF 2023 1659, p. 24.

processus, les équipements techniques, organisations et produits de service nécessaires au fonctionnement sûr, fiable et performant de l'approvisionnement en énergie du pays. Cette protection consiste en des mesures préventives ayant vocation à réduire la probabilité de survenance, ou par des mesures réactives visant à réduire l'ampleur du dommage causé par un incident ou par sa durée. L'intégrité et la disponibilité des systèmes TIC et des informations sauvegardées, traitées et transmises par ces systèmes doivent être assurées[830].

411 L'art. 8 LEne attribue à la Confédération et aux cantons la responsabilité de créer les conditions pour assurer les capacités voulues de production, de réseau et de stockage s'il apparait que l'approvisionnement énergétique de la Suisse n'est pas suffisamment assuré à long terme (art. 8 al. 1 LEne)[831]. La Confédération et les cantons doivent agir pour tous les sous-secteurs critiques de l'approvisionnement en énergie du pays[832].

(ii) La Loi sur la sécurité de l'information

412 Les organisations œuvrant dans les domaines de l'approvisionnement énergétique au sens de l'art. 6 al. 1 LEne sont soumises à l'obligation de signaler les cyberattaques en vertu des art. 74a ss LSI2 (art. 74*b* al. 1 litt. d LSI2). Il en va donc des organisations actives dans « la production, la transformation, le stockage, la fourniture, le transport, le transfert et la distribution d'énergie et d'agents énergétiques jusqu'à leur livraison au consommateur final, y compris l'importation, l'exportation et le transit » (art. 6 al. 1 LEne)[833].

413 L'obligation s'applique également aux organisations actives dans le commerce, la mesure et la gestion de l'énergie, à l'exception des détentrices d'une autorisation au sens de la Loi sur l'énergie nucléaire (LENu) conformément à l'art. 74*b* LSI2, en raison de leur assujettissement à une obligation de signaler à l'Inspection fédérale de la sécurité nucléaire (IFSN) pour les événements susceptibles de mettre en cause la sécurité nucléaire et la sûreté, y compris les cyberattaques contre les installations nucléaires[834].

c. La révision de la Loi fédérale sur l'approvisionnement en électricité

414 L'art. 8 de la Loi sur l'approvisionnement en électricité (LApEl) impose aux gestionnaires de réseau de pourvoir à un réseau sûr, performant et efficace. Des dispositions relatives à la sécurité des systèmes de mesure intelligents ont été

830 FF 2013 6771, p. 6875 s. ; KRATZ, art. 7 EnG N 9 ss.

831 KRATZ, art. 8 N 11 s.

832 FF 2013 6771, p. 6876.

833 Sur l'obligation de signaler les cyberattaques, cf. *infra* N 521 ss.

834 FF 2023 84, p. 36.

adoptées sur la base de l'art. 8 LApEl dans l'Ordonnance sur l'approvisionnement électrique (OApEl) compte tenu d'aspects de cybersécurité. L'art. 8*a* OApEl prévoit que seuls les systèmes de mesure intelligents[835] ayant réussi une vérification peuvent être exploités (art. 8*b* al. 1 OApEl). Les éléments à vérifier, les exigences auxquelles il faut répondre et les modalités de vérification sont fixées dans des directives élaborées par l'Office fédéral de l'énergie (OFEN), les gestionnaires de réseau et les fabricants sur la base d'une analyse de protection (art. 8*b* al. 2 OApEl)[836]. C'est ensuite l'Institut fédéral de métrologie (METAS) qui est compétent pour effectuer la vérification, compétence qu'il peut déléguer (art. 8*b* al. 3 OApEl)[837].

Suivant la logique existante de réglementation décentralisée, le sous- 415
secteur de l'approvisionnement en électricité a fait l'objet d'une analyse[838]. Le rapport de l'OFEN a mis en évidence un besoin de réglementation important, dans la mesure où les directives sectorielles mises en place au fil du temps ne se sont pas traduites par une protection adéquate contre les cybermenaces[839]. Pour cette raison, la LApEl et son ordonnance sont en voie de révision afin qu'elles imposent des exigences minimales de cybersécurité adéquate[840]. Le nouvel art. 8*a* al. 1 LApEl prévoit que « les gestionnaires de réseau, les producteurs et les agents de stockage prennent des mesures pour protéger adéquatement leurs installations contre les cyberrisques »[841]. Ces

835 Les systèmes de mesure intelligents, concernés par les art. 8*a* s. OApEl, sont des « installation[s] de mesure servant à mesurer le flux d'énergie électrique et leur variation réelle dans le temps, qui permet une transmission bidirectionnelle des données avec l'exploitant de la station de mesure, [pouvant être] assimilé au gestionnaire de réseau », cf. OFEN, *Bases pour l'introduction de systèmes de mesure intelligents auprès du consommateur final en Suisse*, 2014, p. 6.

836 Voir AES, *Directives pour la sécurité des données des systèmes de mesure intelligents pour la certification et l'exploitation de systèmes de mesure intelligents*, 2018, qui fait foi pour les organisations de la branche ayant déclaré la directive comme partie intégrante d'un contrat spécifique.

837 CF, *Rapport « Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense »*, 2021, p. 16. L'AES a élaboré une recommandation à ce sujet, cf. AES, *Directives pour la sécurité des données des systèmes de mesure intelligents pour la certification et l'exploitation de systèmes de mesure intelligents*, 2018. Sur la procédure de METAS, cf. METAS, *Contrôles sur la sécurité des données*.

838 CF, *CSN*, 2023, p. 21.

839 DETEC, *Rapport explicatif concernant l'avant-projet relatif à la révision de mai 2024 de l'ordonnance sur l'approvisionnement en électricité*, 2023, p. 1 ; OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »*, 2021, p. 24 et 131.

840 FF 2023 84, p. 56.

841 L'art. 8*a* al. 2 LApEl prévoit que le Conseil fédéral peut étendre cette obligation à d'autres parties exerçant une influence déterminante sur la sécurité de l'approvisionnement comme les prestataires importants actifs dans le commerce ou la mesure de l'énergie, la mobilité électrique ou encore le traitement de données, cf. FF 2023 84,

mesures doivent permettre une prévention et une réaction efficaces face aux cyberincidents[842].

416 Les exigences ont été développées par le CF dans l'ordonnance, en prenant en considération les normes spécifiques du domaine[843]. Un nouvel art. 5*a* de l'ordonnance rend la Norme minimale pour améliorer la résilience informatique de l'OFAE contraignante pour les organisations actives dans l'approvisionnement électrique du pays sur la base de l'art. 5a al. 1 OApEl) à partir de 2024[844]. L'art. 5*a* al. 3 OApEl attribue la compétence à la Commission de l'électricité (ElCom) de surveiller que les organisations atteignent le niveau de protection requis. La Norme minimale pour améliorer la résilience informatique de l'OFAE, se basant sur le cadre NIST[845], l'ordonnance opère une distinction entre les valeurs à atteindre pour les mesures découlant du cadre NIST en fonction des niveaux de protection des différentes organisations (Annexe 1*a* OApEl)[846].

d. La Loi fédérale sur l'énergie nucléaire et ordonnances relatives

417 Les art. 4 s. LENu et 7 ss de son ordonnance (Ordonnance sur l'énergie nucléaire, OENu) règlent la sécurité applicable aux exploitantes d'installations nucléaires. Ces dispositions ne se concentrent pas sur la cybersécurité, la sécurité informatique ou la sécurité de l'information, mais se focalisent principalement sur la protection physique des installations nucléaires[847]. Au vu de l'automatisation de nombreux processus, il est primordial de considérer la cybersécurité dans la sécurité des installations nucléaires.

p. 56 s. ; NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques,* 2022, p. 26 s.

842 NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques*, 2022, p. 26 ; FF 2023 84, p. 56.

843 NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques*, 2022, p. 26.

844 DETEC, *Rapport explicatif concernant l'avant-projet relatif à la révision de mai 2024 de l'ordonnance sur l'approvisionnement en électricité,* 2023, p. 1 et 4 ; OFCS, *Rapport semestriel 2023/II,* 2024, p. 9.

845 Cf. *supra* N 370.

846 DETEC, *Rapport explicatif concernant l'avant-projet relatif à la révision de mai 2024 de l'ordonnance sur l'approvisionnement en électricité,* 2023, p. 2 et 5.

847 IFSN, *Les installations nucléaires suisses préparées aux attaques informatiques*. Cette situation peut avoir trait d'une part au fait que l'accent doit être mis sur les libérations de substances radioactives et, d'autre part, que lorsque la loi et son ordonnance ont été édictées, les TIC paraissaient davantage être sources de progrès que de risques, cf. FF 2001 2529, p. 2568. Pour une illustration, l'art. 10 al. 1 litt. f OENu prévoit que les fonctions de sécurité doivent être automatisées dans la mesure du possible, mais l'Ordonnance ne mentionne pas la protection contre les cyberrisques en particulier ; KESSLER/COENDET/SCHEFER, art. 5 KEG N 31.

L'art. 5 LENu fait mention de principes reconnus sur le plan international devant être pris en compte par les personnes qui conçoivent, construisent ou exploitent des installations nucléaires. L'Agence internationale d'énergie atomique (AIEA), qui détient des relations avec l'IFSN, élabore des guides et des normes qui traduisent les réglementations des traités internationaux pour les réglementations nationales[848]. L'agence a publié en 2021 un guide d'implémentation pour que les États impliquent la sécurité de l'information dans leur sécurité nucléaire[849]. On peut donc voir une prise en compte toujours plus importante de la cybersécurité pour la garantie de la sécurité nucléaire, en tout cas sur le plan international. 418

Il n'est pas exclu que les autorités suisses compétentes, en particulier l'IFSN, prennent position à la suite des avancées internationales. Une prise en compte de la sécurité de l'information dans la sécurité de l'énergie, particulièrement dans la sécurité nucléaire, serait bienvenue. En attendant de savoir si ces autorités suisses estiment que la loi et l'ordonnance doivent être concrétisées ou modifiées pour tenir davantage compte de la cybersécurité, la formulation de certaines dispositions de l'OENu peut éventuellement guider vers une interprétation prenant en compte la cybersécurité. Plus particulièrement, selon l'art. 8 al. 1 OENu, les mesures de protection contre les défaillances internes et externes doivent être prises au sein des installations nucléaires. La disposition prévoit comme exemples de défaillance les incendies, les effets mécaniques de la défaillance d'un composant ou encore la panne d'un système d'exploitation (art. 8 al. 2 OENu). Partant, l'on peut considérer que les cyberincidents sont compris dans cette notion. 419

À titre d'exemples typiquement pour les défaillances externes, l'Ordonnance mentionne les tremblements de terre, les pertes d'alimentation externe en électricité ou les coupures d'alimentation externe en eau de refroidissement (art. 8 al. 3 OENu). L'alimentation étant aujourd'hui largement automatisée, les pertes et coupures d'alimentation peuvent avoir une composante informatique ou constituer la conséquence d'une cyberattaque. L'art. 9 OENu impose des obligations plus concrètes visà-vis d'actes malveillants : son al. 1 prévoit la protection des installations et matières nucléaires contre les actes de sabotage, les actes de violence ou le vol. Cette protection doit reposer sur un système de défense échelonné comprenant des mesures architecturales, techniques, organisationnelles, personnelles et administratives. 420

848 KESSLER COENDET/SCHEFER, art. 4 KEG N 8.

849 AGENCE INTERNATIONALE D'ÉNERGIE ATOMIQUE AIEA, *Computer Security for Nuclear Security, Implementing Guide,* IAEA Nuclear Security Series N 42-G, 2021.

421 En parallèle, une obligation de notification à l'IFSN est imposée aux détentrices d'une autorisation lors d'actes et tentatives de sabotage, de menaces de chantage, de défaillances, dommages et pannes des installations et systèmes de sûreté de plus de vingt-quatre heures ainsi que d'autres événements portant atteinte à la sécurité ou pouvant y porter atteinte (art. 11 LENu et 21 al. 2 OENu). Cette déclaration sert à faciliter le contrôle et le respect des obligations internationales[850]. L'obligation vaut également pour les cyberattaques contre les installations nucléaires, dès lors que l'IFSN dispose d'un guichet de signalement sectoriel comptant sur une organisation prête à intervenir avec un personnel technique qualifié également dans le domaine de la cybersécurité[851].

422 Le Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC) est compétent pour fixer les principes s'appliquant aux hypothèses de risque et aux mesures de sûreté (art. 9 al. 3 OENu). Il a édicté une Ordonnance sur les hypothèses de risque et sur les mesures de sûreté pour les installations et les matières nucléaires. Les mesures peuvent être architecturales, organisationnelles et administratives (art. 5 s. Ordonnance sur les hypothèses de risque et sur les mesures de sûreté pour les installations et les matières nucléaires, OHyRiENu-DETEC). Parmi ces mesures de sûreté, certaines mesures sont de nature technique et comprennent notamment des systèmes de détection, de communication et de contrôle d'accès (art. 5 al. 2 OHyRiENu-DETEC). L'ordonnance ne précise pas que les mesures peuvent être liées à la sécurité informatique. Ces mesures, détaillées dans une directive secrète par l'autorité de surveillance, ne peuvent par conséquent pas être traitées plus avant (art. 5 al. 3 et 6 al. 2 OHyRiENu-DETEC). En parallèle, l'Ordonnance sur les contrôles de sécurité relatifs aux personnes dans le domaine des installations nucléaires (OCSPN) prévoit d'autres mesures. Plus précisément, elle impose un contrôle de sécurité aux personnes ayant accès à des informations classifiées concernant des systèmes de sûreté ou de sécurité relatifs à des installations et matières nucléaires (art. 1 OCSPN)[852].

e. Quelques autres exemples de bases légales

423 L'Ordonnance sur la sécurité des installations de transport par conduites (OSITC) s'applique notamment à certaines organisations actives dans l'approvisionnement en gaz en Suisse. L'ordonnance prévoit depuis janvier 2024, un art. 39*a,* imposant aux organisations assujetties d'assurer la protection

850 MERKER/CONRADIN-TRIACA, art. 11 KEG, N 2.

851 FF 2023 84, p. 36.

852 CF, *Rapport « Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense »,* 2021, p. 16.

adéquate des installations de transport par conduites face aux cybermenaces par les mesures techniques et organisationnelles appropriées (art. 39*a* al. 1 OSITC)[853]. La disposition vient s'ajouter à l'art. 39 al. 3 OSITC qui impose aux organisations assujetties de protéger leurs équipements des influences perturbatrices extérieures, dont les cybermenaces. L'art. 39*a* OSITC prévoit l'élaboration conjointe des directives en matière de cybersécurité avec la consultation de l'OFEN, des cantons et des milieux intéressés[854]. Les directives doivent s'appuyer sur la Norme minimale pour améliorer la résilience informatique de l'OFAE. Dans un second temps, les directives pourront possiblement être intégrées à l'ordonnance en fonction des résultats l'examen du DETEC[855].

424 L'Ordonnance sur le courant fort et l'Ordonnance sur le courant faible ont été adoptées par le CF dans le cadre de sa compétence d'édicter des prescriptions pour prévenir les dangers et les dommages causés par les installations à fort et à faible courant (art. 3 de la Loi sur les installations électriques, LIE). L'art. 4 al. 1 de l'Ordonnance sur le courant fort requiert un établissement, une modification, un entretien et un contrôle des installations à courant fort et des équipements électriques selon les prescriptions de l'ordonnance et, si elle ne prescrit rien, des règles techniques reconnues (art. 4 al. 2 Ordonnance sur le courant fort)[856]. À défaut de telles règles, les normes suisses s'appliquent et à défaut de ces dernières, un renvoi aux normes applicables par analogie ou aux directives techniques éventuelles est effectué (art. 4 al. 3 Ordonnance sur le courant fort). L'ordonnance pose un autre type d'obligation liée à la cybersécurité qui est l'obligation de communiquer à l'organe de contrôle compétent tout accident corporel ou dommage important (art. 16 Ordonnance sur le courant fort)[857]. L'art. 4 de l'Ordonnance sur le courant faible institue le même principe de sécurité et le même renvoi en cascade.

853 DETEC, *Rapport explicatif relatif à la révision de novembre 2023 de l'ordonnance concernant les prescriptions de sécurité pour les installations de transport par conduites,* 2023, p. 3.

854 La Norme minimale pour améliorer la résilience informatique devrait être rendue obligatoire dès 2025, cf. OFCS, *Rapport semestriel 2023/II,* 2024, p. 9.

855 DETEC, *Rapport explicatif relatif à la révision de novembre 2023 de l'ordonnance concernant les prescriptions de sécurité pour les installations de transport par conduites,* 2023, p. 1ss.

856 Ces règles techniques reconnues sont en particulier les normes internationales harmonisées de la Commission Électrotechnique Internationale ou du Comité Européen de Normalisation électrotechnique. La liste des normes peut être obtenu contre paiement auprès de la SNV, cf. art. 4 Ordonnance sur le courant fort ; art. 4 Ordonnance sur le courant faible. Il existe différentes lignes directrices et standards applicables pour la cybersécurité dans l'industrie énergétique, cf. IEC, *Cyber security,* 2018, p. 3 ; MERKER, art. 3 EleG N 14. Il conviendrait d'analyser si ces normes font partie des règles techniques internationales reconnues selon les ordonnances susmentionnées.

857 L'organe de contrôle compétent doit prendre les mesures utiles et établir les causes de l'accident ; le devoir de l'exploitante se limite à la notification et à l'apport d'une aide (art. 16 al. 2 et 3 Ordonnance sur le courant fort).

425 Un mécanisme similaire existe à l'art. 3 de l'Ordonnance sur les installations électriques à basse tension (OIBT). L'OIBT et l'Ordonnance du DETEC sur les installations électriques à basse tension prévoient la remise à l'Inspection compétente d'un rapport de sécurité qui semble viser des questions étroitement liées au domaine et avoir une vocation plus générale que la cybersécurité (art. 37 OIBT et 13 Ordonnance du DETEC sur les installations électriques à basse tension).

426 L'Ordonnance sur la radioprotection (OraP) prévoit des compétences, des mesures générales de sécurité et leur communication à une autorité de surveillance[858]. L'Ordonnance du DFI sur l'utilisation des matières radioactives (OUMR), basée sur cette première ordonnance, développe les mesures de sécurité à mettre en place. Concrètement, elle requiert la protection contre les accès non autorisés, par des moyens techniques et administratifs, des informations sensibles concernant la sécurité des sources radioactives scellées de haute activité. Les mesures prises, figurant dans un plan de sécurité soumis au contrôle de l'autorité de surveillance (en l'occurrence l'IFSN), doivent servir à empêcher, repérer ou retarder le vol ou les actes non autorisés afin de rendre possible une intervention (art. 3 al. 3 et 4 OUMR).

427 En parallèle des bases légales sectorielles, les organisations actives dans le secteur de l'énergie sont soumises, lorsqu'elles traitent des données personnelles, aux lois de protection des données personnelles, tantôt cantonales, tantôt fédérale. Cela implique que les organisations soient soumises à des obligations supplémentaires en termes de sécurité des données et, par conséquent, à l'obligation d'annoncer les violations de la sécurité des données lorsque des données personnelles sont compromises par un cyberincident[859].

f. Les normes minimales

428 Plusieurs secteurs de l'approvisionnement économique du pays ont adopté des normes minimales pour l'utilisation des technologies de l'information et de la communication et pour améliorer la résilience informatique[860]. La norme sur laquelle se basent celles-ci est la Norme minimale pour améliorer la résilience informatique de l'OFAE[861]. Ces normes ne sont par principe pas

858 Voir respectivement art. 99 ORaP ou 10 al. 6 Ordonnance du DFI sur l'utilisation des matières radioactives, ainsi que 124 ss et 202 ORaP.

859 Sur l'obligation d'annoncer les violations de la sécurité des données, cf. *infra* N 525 ss. Sur l'obligation d'assurer la sécurité des données, cf. *infra* N 531 s.

860 KRATZ, art. 7 EnG N 12.

861 OFAE, *Norme minimale pour améliorer la résilience informatique,* 2023. Sur cette norme, cf. *infra* N 534 ss.

contraignantes et servent de recommandations, sous réserve qu'une législation y renvoie ou que les organisations parties à un contrat en acceptent un caractère contraignant[862].

Les secteurs de l'approvisionnement ayant adopté de telles normes se 429
regroupent avec des sous-secteurs critiques. L'association des entreprises électriques suisses (AES) en a adopté une pour l'électricité[863], de la même façon que la Société Suisse de l'Industrie du Gaz et des Eaux (SSIGE) pour l'approvisionnement en gaz[864] et l'OFAE en collaboration avec la SSIGE et les Réseaux Thermiques pour l'approvisionnement du chauffage et du froid à distance[865]. Ces normes reprennent un mécanisme semblable à celui de la Norme minimale pour améliorer la résilience informatique de l'OFAE. Elles mentionnent des mesures techniques et organisationnelles permettant aux organisations du secteur d'être guidées dans l'implémentation de ces dernières pour garantir la sécurité de l'information et des moyens informatiques. Néanmoins, elles détaillent davantage les notions et compétences pour le secteur concerné. Les mesures sont en principe relativement similaires[866].

g. En conclusion

La LEne s'applique largement au secteur critique de l'énergie en imposant 430
une obligation générale de garantir un approvisionnement sûr. Au-delà de ce qui est prévu par cette « loi-parapluie », plusieurs bases légales imposent des obligations plus concrètes pour les organisations des différents sous-secteurs critiques. Les bases légales diffèrent en fonction des prestations fournies par les organisations des différents sous-secteurs critiques.

Peu de bases légales dans le secteur de l'énergie mentionnent la cyber- 431
sécurité comme composante de la sécurité de l'approvisionnement. Alors qu'il est primordial de tenir compte de la cybersécurité, il n'est pas certain qu'elle soit prise en compte par les législations en vigueur ou par les autorités dans

862 CF, *Rapport « Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense »* 2021, p. 23 ; DETEC, *Rapport explicatif concernant l'avant-projet relatif à la révision de mai 2024 de l'ordonnance sur l'approvisionnement en électricité,* 2023, p. 4.

863 AES, *Handbuch Grundschutz für « Operational Technology» in der Stromversorgung,* 2018.

864 SSIGE, *Norme minimale pour garantir la sécurité des technologies de l'information et de la communication (TIC) requises pour l'approvisionnement en gaz,* 2020.

865 OFAE/RETS/SSIGE, *Norme minimale pour garantir la sécurité des technologies de l'information et de la communication (TIC) requises pour l'approvisionnement du chauffage et du froid à distance,* 2023.

866 Voir par exemple dans le secteur de l'approvisionnement en électricité, AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung,* 2018, p. 103 ss.

l'application des lois, ce bien qu'il soit possible d'interpréter différentes dispositions en l'y intégrant. L'OFEN a conclu à la nécessité de modifier la LApEl et la modification subséquente de la loi et de son ordonnance pour encadrer la cybersécurité et améliorer la résilience auprès des organisations actives dans le sous-secteur critique de l'approvisionnement en électricité. Cette décision montre qu'il est préférable que les bases légales contiennent des dispositions prévoyant expressément la cybersécurité. Autrement, il dépend des autorités compétentes d'intégrer la cybersécurité à l'interprétation à faire des dispositions légales imposant aux infrastructures critiques du secteur de l'énergie d'assurer la sécurité de leurs installations.

432 Partant de ce constat, le temps permettra de savoir si le pouvoir législatif et les autorités compétentes estiment que les autres dispositions légales suffisent ou si, au contraire, il deviendra nécessaire de développer les bases légales applicables à la cybersécurité auprès des différentes organisations du sous-secteur de l'énergie. Il semble en tout cas que le pouvoir législatif estime nécessaire de préciser des obligations pour la cybersécurité dans le sous-secteur de l'approvisionnement en électricité comme dans les sous-secteurs de l'approvisionnement en gaz naturel et en pétrole.

Schéma 11 : la réglementation du secteur critique de l'énergie[867]

Secteur critique de l'énergie	Réglementé	Partiellement réglementé			Non réglementé
		Exigences légales	Exigences non contraignantes	Obligation(s) de signaler	
Approvisionnement en gaz naturel	×		×	×	
Approvisionnement en pétrole	?			×	
Approvisionnement en électricité	×	×	×	×	
Chauffage à distance et chaleur industrielle			×	×	

867 Le sous-secteur critique de l'approvisionnement en gaz est considéré comme réglementé depuis janvier 2024. Il se peut que le sous-secteur critique de l'approvisionnement en pétrole soit concerné également par la modification de l'OSITC. Le sous-secteur critique de l'approvisionnement en électricité sera réglementé une fois la révision de la LApEl et de l'OApEl entrées en vigueur.

4. Le secteur critique de l'élimination

a. Le secteur

Le secteur critique de l'élimination se divise en deux sous-secteurs, celui des déchets et celui des eaux usées. Le premier sous-secteur englobe la collecte, l'élimination et la valorisation des déchets spéciaux, urbains et industriels. Le second vise l'élimination des eaux usées résidentielles, artisanales et industrielles pour protéger la population sur le plan de la santé et l'environnement[868]. 433

b. La protection de la population et de l'environnement

Les organisations exploitant des installations susceptibles de causer des dommages importants à l'homme en cas d'événements extraordinaires sont soumises à l'art. 10 al. 1 Loi fédérale sur la protection de l'environnement (LPE). La disposition leur impose de prendre les mesures propres à assurer la protection de la population et de l'environnement. Parmi les mesures de protection de l'environnement figure l'obligation de prendre les mesures de sécurité technique. La LPE contient des dispositions similaires à ses art. 28 et 29a. Ces dispositions imposent à toute personne utilisant des substances ou organismes et leurs déchets de ne pas constituer une menace pour l'humain ou l'environnement. 434

D'autres exigences découlent de la nécessité de protéger la population. Par exemple, les art. 9 s. de l'Ordonnance sur les mouvements de déchets (OMoD) soumettent les entreprises d'élimination des déchets spéciaux à une autorisation de l'autorité cantonale portant notamment sur le procédé d'élimination (art. 10 al. 2 litt. b OMoD). L'autorisation porte également sur les conditions, l'utilisation d'installations et d'équipements spécifiés et le recours à des spécialistes devant être respectées pour que les déchets soient éliminés de manière respectueuse de l'environnement (art. 10 al. 2 litt. c OMoD). Pour un autre exemple, l'art. 11 al. 2 OPAM impose aux entreprises dépassant les seuils quantitatifs des substances, des préparations ou des déchets spéciaux au sens de l'annexe 1.1 (art. 1 al. 2 litt. a OPAM) de combattre immédiatement les accidents majeurs qu'elles rencontrent. Elles doivent également éviter toute nouvelle atteinte et remédier aux atteintes le plus rapidement possible. 435

Toutes ces normes ne visent pas directement la cybersécurité, mais la cybersécurité peut être un moyen d'assurer la protection de l'humain et de l'environnement. Cette réflexion délicate doit être menée en tenant compte du fait que le respect de l'environnement ne se recoupe pas complètement avec le concept de cybersécurité. 436

868 FF 2018 491, p. 522 ; FF 2023 1659, p. 24.

c. Les obligations d'annonce

437 Les organisations chargées du traitement des eaux usées et de l'élimination des déchets sont tout d'abord soumises à l'obligation de signaler les cyberattaques ciblant les infrastructures critiques (art. 74*b* al. 1 litt. c LSI2). L'obligation s'applique uniquement lorsqu'une cyberattaque au sens de l'art. 74*d* LSI2 vise une tâche relevant de la puissance publique de l'organisation[869].

438 La LPE contient également une obligation faite aux exploitantes d'informer l'organe d'alerte de tout événement extraordinaire (art. 10 al. 3 LPE). La loi ne fait à nouveau pas état explicitement des événements liés au cyberespace, mais si une panne informatique occasionne un événement extraordinaire, l'on peut supposer que l'exploitante doive l'annoncer à l'organe d'alerte. Les communications sur des événements extraordinaires concernent probablement aussi les cyberattaques susceptibles d'engendrer des dommages importants à l'homme ou à l'environnement.

439 L'art. 11 al. 2 litt. a OPAM impose aux entreprises dépassant les seuils quantitatifs des substances, des préparations ou des déchets spéciaux d'annoncer à l'organe d'alerte (la Centrale d'alarme, CENAL) les accidents majeurs qu'elles rencontrent.

440 Il n'est pas exclu que des données personnelles soient compromises par un cyberincident affectant une organisation active dans le secteur de l'élimination. Si tel est le cas, l'organisation traitant les données personnelles est susceptible d'être soumise à l'obligation d'annoncer les violations de la sécurité des données au sens de l'art. 24 LPD[870].

d. Les normes minimales non contraignantes

441 En parallèle, les deux sous-secteurs critiques disposent d'une norme minimale visant à assurer la sécurité informatique. Les deux normes sont basées sur la Norme minimale pour améliorer la résilience informatique adoptée par l'OFAE[871]. Le standard minimal pour le sous-secteur des eaux usées a été adopté en 2021 et la norme minimale pour l'élimination des déchets en 2022[872].

869 FF 2023 84, p. 35. Sur l'obligation de signaler les cyberattaques, cf. *infra* N 521 ss.

870 Sur l'obligation d'annoncer les violations de la sécurité des données, cf. *infra* N 525 ss.

871 BWL/VSA, *Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie in Abwasserbetrieben*, 2021.

872 OFAE/ASED, *Norme minimale pour la sécurité des TIC dans le domaine de l'élimination des déchets*, 2022.

e. En conclusion

Le secteur critique de l'élimination dispose de bases légales impliquant des considérations de sécurité. En revanche, les lois applicables en tout cas sur le plan fédéral (à l'instar de la LPE) ne se focalisent pas sur la cybersécurité. Il en va bien plus de la protection de la population et de l'environnement, dont les risques sont bien plus larges et ne font que se recouper avec la cybersécurité. La question de la compréhension de la cybersécurité dans ces bases légales soulève des questions similaires à celles se posant dans le sous-secteur critique de l'énergie : la loi ne semble pas imposer d'obligations de cybersécurité bien qu'une interprétation des dispositions légales incluant la cybersécurité soit théoriquement envisageable. 442

Schéma 12 : la réglementation du secteur critique de l'élimination

Secteur critique de l'élimination	Réglementé	Partiellement réglementé			Non réglementé
		Exigences légales	Exigences non contraignantes	Obligation(s) de signaler	
Déchets			×	×	
Eaux usées			×	×	

5. Le secteur critique des finances

a. Le secteur

Le secteur critique des finances couvre les services financiers, à savoir les entités qui œuvrent dans l'exécution des opérations de paiement, l'approvisionnement de la population en argent liquide, la capitalisation de tiers, la rémunération de dépôts et le maintien de la stabilité des prix. Il couvre aussi les services d'assurances, qui comprennent la garantie de la couverture d'assurance, l'aide financière en cas de dommages ainsi que les prestations dans le cadre de la prévention des dommages (y compris les assurances maladie et les assurances sociales)[873]. Ce sous-secteur englobe les institutions offrant des prestations légales et surobligatoires, telles que la prévoyance professionnelle ou l'assurance complémentaire à l'assurance-maladie obligatoire[874]. 443

873 FF 2018 491, p. 522 ; FF 2023 1659, p. 24.

874 NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques*, 2022, p. 18.

444 Les entités actives dans les deux sous-secteurs répondent à diverses obligations légales et sont soumises à différentes normes pour leur activité. Les organisations dans le sous-secteur des assurances comme dans le sous-secteur des services financiers sont en principe soumises à la surveillance de l'Autorité fédérale de surveillance des marchés financiers (FINMA), conformément à l'art. 1 de la Loi sur l'Autorité fédérale de surveillance des marchés financiers (LFINMA).

b. L'Autorité fédérale de surveillance des marchés financiers

445 La cybersécurité dans le secteur des finances fait l'objet de réglementations transversales et sectorielles, comprenant notamment les circulaires de la FINMA[875]. La LFINMA constitue le cadre pour les compétences de surveillance de la FINMA pour les marchés financiers en vertu de différentes bases légales (art. 1 al. 1 LFINMA). L'art. 7 al. 1 LFINMA et d'autres bases légales sur les marchés financiers à l'instar de la Loi sur les banques (LB) ou la Loi fédérale sur les établissements financiers (LEFin) délèguent expressément des compétences législatives à la FINMA pour l'adoption d'ordonnances lorsque la législation sur les marchés financiers le prévoit. Elle est aussi compétente pour l'adoption de circulaires visant à préciser les modalités d'application de la législation sur les marchés financiers[876]. Elle contribue au processus législatif et à l'élaboration d'une réglementation technique[877].

446 C'est notamment sur cette base qu'elle a par exemple adopté sa circulaire 2018/3 sur l'*outsourcing,* sa circulaire 2023/1 les risques opérationnels ou sa circulaire 2017/1 sur la gouvernance d'entreprise[878]. La circulaire révisée sur les risques opérationnels est en outre basée sur les art. 1b al. 3 litt. b LB et 9 LEFin, qui imposent aux organisations soumises à ces lois de disposer d'une gestion de risque adéquate[879]. La circulaire révisée est entrée en vigueur le 1er janvier 2024[880]. La circulaire n'est pas applicable à l'ensemble des organisations soumises à la surveillance de la FINMA et elle est contraignante unique-

875 WEBER/YILDIZ, p. 33.

876 FF 2006 2741, p. 2773 ; BSK FINMAG-WINZELER, art. 7 N 18 notamment ; ZUFFEREY/CONTRATTO, p. 77 et 81 ss.

877 FF 2006 2741, p. 2755.

878 Voir FINMA, *Circulaire 2017/1, Gouvernance d'entreprise – banques, Gouvernance d'entreprise, gestion des risques et contrôles internes des banques,* 22 septembre 2016 ; FINMA, *Circulaire 2018/3 Outsourcing – Externalisation dans le secteur des banques, des entreprises d'assurance et de certains établissements financiers au sens de la LEFin,* 21 septembre 2018 ; FINMA, *Circulaire 2023/1,* 2022.

879 L'art. 9 al. 2 LEFin prévoit plus spécifiquement que les établissements financiers doivent identifier, gérer et surveiller leurs risques ainsi que mettre sur pied des contrôles internes efficaces.

880 FINMA, *Circulaire 2023/1,* 2022, p. 1 ; FINMA, *Rapport annuel 2022,* 2023, p. 69 s.

ment pour les organisations visées par la circulaire et pour lesquelles les lois habilitent la FINMA à adopter des instruments (à l'instar de la LB ou de la LEFin)[881]. Elle prévoit une série de considérations et de mesures techniques et organisationnelles que les organisations mettent en place afin de tenir compte des cyberrisques. Ces mesures vont de la sensibilisation des collaboratrices et de l'élaboration d'inventaires des composantes TIC à l'établissement de processus de gestion de cyberincidents ainsi qu'à l'évaluation des mesures en place[882]. À noter que la FINMA soutient l'autorégulation (art. 7 al. 3 LFINMA), à savoir que l'autorégulation des secteurs concernés sert de référentiel dont la FINMA tient compte lorsqu'elle élabore ses actes réglementaires[883].

c. Les obligations d'annonce

Les organisations assujetties à la surveillance de la FINMA sont soumises à une obligation de signaler à l'autorité tout fait important susceptible de l'intéresser en vertu de l'art. 29 al. 2 LFINMA. Sur cette base, la FINMA a élaboré une communication sur l'obligation d'annoncer les cyberattaques en vertu de l'art. 29 al. 2 LFINMA[884]. Les événements importants en lien avec des cyberattaques ayant atteint partiellement ou entièrement leur but doivent être annoncés à la FINMA pour contribuer à assurer la fiabilité de la place financière suisse. L'obligation de signaler à la FINMA concerne un nombre bien plus important d'organisations que l'obligation de signaler à l'OFCS. L'obligation de l'art. 29 al. 2 LFINMA vise en premier lieu les cyberattaques visant des fonctions d'importance critique et dont la défaillance ou le dysfonctionnement entraînerait des conséquences considérables sur la protection des individus et entraverait fortement cette protection. À ce titre, les cyberattaques visant des actifs d'importance critique (comme le personnel, l'infrastructure technologique, les informations, les bâtiments et les fournisseuses essentielles nécessaires aux processus de ces fonctions critiques) doivent dans tous les cas être signalées à la FINMA[885]. 447

881 CF, *La FINMA et son activité de réglementation et de surveillance*, 2014, p. 26 ; FINMA, *Circulaire 2023/1,* 2022, p. 1 s. En pratique en revanche, les circulaires offrent la possibilité à la FINMA de rendre une décision dont l'application devient contraignante, CF, *La FINMA et son activité de réglementation et de surveillance*, 2014, p. 27.

882 FINMA, *Circulaire 2023/1,* 2022, p. 5 ss.

883 Pour plus d'informations à ce sujet, cf. WEBER/YILDIZ, p. 97 ss ; ZUFFEREY/CONTRATTO, p. 78 ss.

884 FINMA, *Communication FINMA sur la surveillance 05/2020 – Obligation de signaler les cyberattaques selon l'art. 29 al. 2 LFINMA*, 7 mai 2020.

885 Pour plus d'informations sur cette obligation, cf. FINMA, *Communication FINMA sur la surveillance 05/2020 – Obligation de signaler les cyberattaques selon l'art. 29 al. 2 LFINMA*, 2020, p. 4 s. ; FINMA, *Circulaire 2023/1,* 2022, p. 10 ; HIRSCH, p. 206 ss ; PC LPD-BÉGUIN/VIGNIEU, art. 24 N 80. D'autres obligations de signaler coexistent dans ce secteur ; les gestionnaires de fortune et des trustees sont par exemple aussi soumises à

448 L'art. 74*b* al. 1 litt. e LSI2 impose aux entreprises soumises à la LB, à la Loi sur la surveillance des assurances (LSA) et à la Loi sur l'infrastructure des marchés financiers (LIMF) à l'obligation de signaler les cyberattaques à l'OFCS. L'assujettissement des organisations actives dans le secteur critique des finances se justifient par le fait que celles-ci constituent des cibles particulièrement attrayantes pour les délinquantes. Toutes les organisations actives dans le secteur bancaire et financier ne constituent en revanche pas des infrastructures nécessaires à l'économie nationale, raison pour laquelle seules les organisations de l'art. 74*b* al. 1 litt. e LSI2 sont soumises à l'obligation de signaler les cyberattaques à l'OFCS[886]. Cette obligation d'annonce s'impose en parallèle des autres obligations de signaler, par exemple à la FINMA[887].

449 Les organisations qui fournissent des prestations destinées à couvrir les conséquences de la maladie, des accidents, de l'incapacité de travail et de gain, de la vieillesse, de l'invalidité et de l'impotence sont aussi soumises à l'obligation de signaler les cyberattaques à l'OFCS (art. 74*b* al. 1 litt. i LSI2). L'obligation a vocation à s'appliquer au cercle le plus large possible de compagnies d'assurances, comprenant les compagnies d'assurances sociales soumises à la LPGA, mais également les compagnies d'assurances offrant des prestations surobligatoires. Il n'est pas exclu que le CF restreigne au niveau de l'ordonnance le cercle des assujetties[888].

450 Les organisations actives dans le secteur des finances sont susceptibles de traiter bon nombre de données personnelles. Elles sont en pratique probablement régulièrement amenées à annoncer des violations de la sécurité des données en vertu de l'art. 24 LPD, ce en parallèle des autres obligations[889].

d. En conclusion

451 Le secteur des finances constitue l'un des secteurs critiques les plus réglementés en termes de cybersécurité, par le biais de bases légales, mais surtout par le biais des circulaires de la FINMA. L'autorité de surveillance a pris conscience

l'art. 43*l* al. 2 LFINMA qui les soumet à l'obligation de renseigner l'organisme de surveillance de tout fait important pour la surveillance, ce qui pourrait comprendre les cyberattaques d'une façon similaire à ce qui prévaut à l'art. 29 al. 2 LFINMA, cf. HIRSCH, p. 223.

886 Le cercle d'organisations du secteur bancaire et financier assujetties à l'obligation de signaler les cyberattaques à la FINMA est plus large que ce qui est prévu à l'art. 74*b* al. 1 litt. e LSI2.

887 FF 2023 84, p. 36. Sur l'obligation de signaler les cyberattaques, cf. *infra* N 521 ss.

888 FF 2023 84, p. 37 s.

889 MÉTILLE/MEYER, *Annonce des violations de la sécurité des données : une nouvelle obligation de la nLPD,* 2021, p. 25 s. Sur l'obligation d'annoncer les violations de la sécurité des données, cf. *infra* N 525 ss.

des cybermenaces et de leur importance pratique pour le secteur. Pour cette raison, elle prend les devants, adopte et révise ses circulaires pour appréhender au mieux les cybermenaces[890]. Certains instruments sont contraignants lorsqu'ils restituent exactement le contenu de la loi. Les autres instruments de la FINMA sont théoriquement non contraignants. En raison de ses pouvoirs de surveillance étendus, les organisations à l'attention desquelles les circulaires et autres instruments sont publiées ont tout intérêt à se conformer aux instruments qu'elle a adoptés[891]. En revanche, ces circulaires ne sont pas forcément applicables à l'ensemble des organisations actives dans le secteur critique. Sa circulaire sur les risques et la résilience opérationnelles est par exemple applicable uniquement aux banques, aux groupes et conglomérats financiers et aux maisons de titres[892].

Des mesures pratiques ont été prises pour améliorer la résilience des organisations actives dans le secteur des finances face aux cybermenaces. L'établissement du *Swiss Financial Sector Cyber Security Centre* (FS-CSC), qui collabore notamment avec l'OFCS[893], a typiquement pour objectif d'accroître la cyberrésilience de la place financière suisse par le biais de l'échange d'informations[894]. 452

Schéma 13 : la réglementation du secteur critique des finances[895]

Secteur critique des finances	Réglementé	Partiellement réglementé			Non réglementé
		Exigences légales	Exigences non contraignantes	Obligation(s) de signaler	
Services financiers	×				
Services d'assurance			×	×	

890 FINMA, *Rapport annuel 2022*, 2023, p. 33 s. et 69 s.

891 CF, *La FINMA et son activité de réglementation et de surveillance*, 2014, p. 27 ; BSK FINMAG-WINZELER, art. 7 N 18.

892 FINMA, *Circulaire 2023/1*, 2022, p. 1 et 3.

893 Interpellation 22.3749 « Faut-il différencier entre les secteurs économiques sous l'angle des exigences en matière de cybersécurité ? » déposée le 16 juin 2022 par Gherard Andrey.

894 SWISS FINANCIAL SECTOR CYBER SECURITY CENTRE FS-CSC, *Statuts Swiss FS-CSC*, version du 6 juin 2023, p. 3.

895 Il convient d'analyser si l'ensemble des services financiers est soumis à la circulaire sur les risques opérationnels de la FINMA pour confirmer si le sous-secteur critique des services financiers est entièrement réglementé.

6. Le secteur critique de la santé

a. Le secteur

453 Le secteur critique de la santé regroupe tout d'abord les soins médicaux. Les soins médicaux comprennent le traitement et la prise en charge de la patientèle, à savoir la médecine de premier recours, la médecine spécialisée ou hospitalière ainsi que les soins vétérinaires de base. Ensuite, le secteur de la santé englobe les services de laboratoires, entendus comme les analyses de laboratoires dans le cadre de la protection des êtres humains, des animaux et de l'environnement. Finalement, le secteur couvre l'approvisionnement en produits chimiques et thérapeutiques (comme les médicaments et dispositifs médicaux), y compris les vaccins[896].

454 Le secteur de la santé est réglementé à plusieurs niveaux. Des cabinets médicaux, des cliniques privées, des hôpitaux cantonaux ou des entreprises pharmaceutiques sont concernées par ce secteur. Plusieurs législations leur sont applicables tant au niveau fédéral qu'au niveau cantonal. En outre, les cantons délèguent des tâches publiques à des organisations externes, à l'image des institutions médico-hospitalières délégataires d'une tâche publique. Par conséquent, la cybersécurité peut être prévue dans des contrats pour de tels établissements. Les prochains paragraphes serviront à illustrer les pratiques du secteur à l'aide de deux instruments légaux spécifiques parmi ceux qui réglementent expressément des questions de cybersécurité ou de sécurité des données[897].

b. L'Ordonnance sur les dispositifs médicaux

455 Pour qu'un dispositif médical au sens de l'art. 3 de l'Ordonnance sur les dispositifs médicaux (Odim) puisse être mis sur le marché, il doit être conforme aux exigences de sécurité prévues par l'art. 6 Odim. L'ordonnance renvoie pour cette question aux exigences contenues dans l'annexe I du Règlement (UE) 2017/745 relatif aux dispositifs médicaux (RDM) (art. 6 al. 2 Odim), qui sont précisées par des normes techniques ou spécifications (art. 6 al. 4 Odim)[898].

456 L'art. 74 Odim, intitulé « Cybersécurité », impose aux établissements de santé de prendre toutes les mesures techniques et organisationnelles néces-

896 FF 2018 491, p. 522.

897 La sécurité des données personnelles est plus souvent réglementée et elle est étroitement liée à la cybersécurité lorsqu'elle est appréhendée en lien avec le traitement informatisé de données personnelles.

898 Les exigences en matière de sécurité sont en voie d'augmentation, cf. DONZALLAZ, N 727 ss.

saires selon l'état de la technique en vue de protéger les dispositifs pouvant être connectés à un réseau des attaques et des accès électroniques non autorisés. Cette obligation s'impose aux établissements de santé, à savoir aux organisations ayant pour mission première de prendre en charge, de traiter une patientèle ou d'œuvrer en faveur de la santé publique (art. 4 al. 1 litt. k Odim). L'obligation s'applique dès lors à un nombre important d'organisations dans ce contexte. Les hôpitaux (qui constituent un type d'établissement de santé spécifique, cf. art. 4 al. 1 litt. l Odim) doivent en outre identifier, évaluer et documenter les mesures qu'ils prennent à cette fin, ce conformément aux principes d'un système de gestion du risque (pouvant faire partie intégrante du système de gestion de la qualité des hôpitaux)[899].

457 Parallèlement à la question de la cybersécurité, d'autres dispositions de l'ordonnance règlent des questions plus larges de sécurité. L'art. 57 ODim impose notamment aux fabricantes de dispositifs médicaux de prendre les mesures préventives ou correctrices appropriées si elles découvrent, lors de la surveillance après commercialisation, que de telles mesures s'imposent. En outre, si elles constatent un incident grave ou si des raisons médicales ou techniques les incitent à prendre une mesure destinée à empêcher que l'incident se produise ou à en réduire le risque, elles doivent déclarer cette mesure corrective à l'Institut suisse des produits thérapeutiques (Swissmedic) selon l'art. 66 al. 1 Odim. Par ailleurs, un rapport de sécurité doit être établi et mis à jour de manière échelonnée pour chaque dispositif et le cas échéant pour chaque catégorie ou groupe de dispositifs (art. 60 ss Odim).

c. La Loi fédérale sur le dossier électronique du patient

458 La Loi sur le dossier électronique du patient (LDEP) est un autre exemple d'exigences légales de cybersécurité. Elles s'appliquent à certaines organisations du secteur de la santé et pour la mise en œuvre du dossier électronique de la patientèle spécifiquement. La LDEP s'applique aux « communautés ». Ces communautés sont des unités organisationnelles de professionnelles de la santé et leurs institutions (art. 2 litt. d LDEP)[900]. Ces communautés sont soumises à

899 L'ordonnance ne précise ni les conséquences de cette obligation sur un éventuel droit ou une potentielle obligation de modifier un dispositif médical, ni son influence sur la certification des dispositifs médicaux.

900 Elles consistent plus précisément en des regroupements « de professionnels de la santé et de leurs institutions. Les communautés doivent notamment garantir que les patients et les professionnels de la santé disposant des droits d'accès nécessaires ont accès en tout temps aux données du dossier électronique du patient. […] Les membres d'une communauté ne peuvent participer au système global du DEP qu'après avoir été certifiés », cf. EHEALTHSUISSE, *Glossaire, Communauté*.

l'obligation de se doter d'un système de gestion de la protection et de la sécurité des données adapté aux risques. Aux termes de l'art. 12 al. 1 de l'Ordonnance sur le dossier électronique du patient (ODEP), ce système doit comprendre un système de détection et de gestion des incidents de sécurité, un inventaire des moyens informatiques et recueils de données ainsi que les exigences relatives à la protection et la sécurité des données imposées aux institutions de santé ou aux tiers affiliés à la communauté. Par ailleurs, une certification est prévue pour attester du niveau de sécurité garanti (art. 11 ss LDEP). La certification est concrétisée dans l'ODEP et dans l'Ordonnance du Département fédéral de l'intérieur (DFI) sur le dossier électronique du patient (ODEP-DFI)[901]. En outre, les communautés sont tenues de désigner une personne responsable pour la protection et la sécurité des données (art. 12 al. 2 ODEP). Les supports de données doivent se trouver en Suisse et être régis par le droit suisse (art. 12 al. 5 ODEP). Finalement, le dossier électronique reposant sur l'identité électronique des patientes, l'ordonnance pose des exigences relatives à la sécurité de ce moyen d'identification, allant du respect de standards internationaux à la mise en place d'une procédure d'authentification conforme aux progrès techniques, comportant au moins deux facteurs d'authentification (art. 23 ODEP).

459 Le DFI est compétent pour fixer les exigences techniques et organisationnelles applicables à la protection et à la sécurité des données selon l'art. 12 al. 4 ODEP). L'ODEP-DFI développe quelques mesures susmentionnées, dont principalement les critères de certification.

d. Les obligations d'annonce

460 L'obligation de signaler les cyberattaques s'applique à différentes organisations du secteur critique de la santé. Les établissements de santé figurant sur une liste hospitalière cantonale conformément à l'art. 39 al. 1 litt. e de la Loi fédérale sur l'assurance-maladie (LAMal) sont soumis à l'obligation de signaler les cyberattaques en vertu des art. 74*a* ss LSI2 en vertu de l'art. 74*b* al. 1 litt. f LSI2. L'obligation vaut pour tous les établissements sur ces listes afin d'éviter que les cyberattaques compromettent la fourniture des soins de base. Le message de la loi précise que lorsqu'une attaque entraîne la mise en péril de données contenues dans le dossier électronique de patientes, l'obligation de signaler incombe à l'organisation visée par la cyberattaque[902]. Il en va de même pour les laboratoires médicaux titulaires d'une autorisation de l'art. 16 de la Loi sur les épidémies (Lep) en vertu de l'art. 74*b* al. 1 litt. g LSI2, dans la

901 FF 2013 4747, p. 4775 ; OFSP, p. 1 s.

902 FF 2023 84, p. 36 s.

mesure où ils dépendent dans une large mesure du bon fonctionnement de l'infrastructure informatique pour leurs analyses et pour leur collaboration avec le corps médical[903]. Les entreprises titulaires d'une autorisation de fabriquer, de mettre sur le marché ou d'importer des médicaments conformément à la Loi sur les produits thérapeutiques (LPTh) sont également soumises à l'obligation de signaler les cyberattaques[904].

461 Il existe une obligation faite aux fabricantes de dispositifs médicaux de déclarer à Swissmedic les incidents graves en rapport avec ces dispositifs dès qu'elles en ont connaissance (art. 66 Odim)[905]. L'ODEP impose également le signalement de tout incident exerçant une influence sur la sécurité survenu dans le système à l'Office fédéral de la santé publique (OFSP) en vertu de l'art. 12 al. 3 ODEP.

462 En parallèle, les organisations actives dans le secteur de la santé présentent un important niveau de criticité. Elles traitent un volume important de données personnelles dont des données sensibles (principalement en termes de données relatives à la santé ou de données génétiques, art. 5 litt. c ch. 2 et 3 LPD)[906]. Partant, elles sont particulièrement susceptibles d'être soumises à l'obligation d'annoncer des violations de la sécurité des données au PFPDT en vertu de l'art. 24 LPD.

e. Les recommandations dans le secteur de la santé

463 La Conférence des directrices et directeurs cantonaux de la santé (CDS) a élaboré des recommandations pour la protection des données et la sécurité de l'information en renvoyant à la recommandation du NCSC en matière de cybersécurité dans le secteur de la santé. La recommandation du NCSC pose une série de mesures de sécurité informatique allant de la surveillance étroite des terminaux et du suivi étroit des données de journal au blocage de fichiers dangereux joints aux courriels, passant par la protection de l'authentification[907]. Le document élaboré par le NCSC en collaboration avec son équipe technique, GovCERT, est une recommandation, à savoir un instrument de droit souple. Le document fait état de mesures dites facultatives et d'autres dites obligatoires alors que le NCSC n'est vraisemblablement pas habilité à adopter des exigences contraignantes pour ce secteur.

903 FF 2023 84, p. 37 s.

904 FF 2023 84, p. 37 s.

905 Pour plus d'informations à ce sujet, cf. DONZALLAZ, N 717 ss.

906 CDS, *Recommandations de la CDS sur la planification hospitalière,* 2022, p. 29.

907 NCSC/GovCERT, *Cybersécurité dans le secteur de la santé : recommandations,* 2022.

464 Au niveau des recommandations de la CDS, une recommandation 16 a été ajoutée aux recommandations sur la planification hospitalière. Elle requiert des cantons qu'ils astreignent les hôpitaux répertoriés au respect des exigences relatives à la protection des données selon le droit cantonal et selon le droit fédéral, au recours à un système de gestion de la sécurité de l'information (SGSI), à l'utilisation des outils techniques du NCSC[908] ainsi qu'à la participation à l'échange d'informations avec le NCSC. Si l'obligation de recourir à un SGSI est disproportionnée, les hôpitaux devraient selon la CDS mettre en œuvre en tout cas les mesures recommandées par le NCSC[909].

465 D'autres recommandations existent. Par exemple, l'association professionnelle H+ pour les hôpitaux de Suisse a publié une série d'exigences pour responsabiliser les hôpitaux quant aux infrastructures et systèmes d'organisations tierces à l'instar de fournisseuses et de prestataires[910]. Le *Swiss Personalized Health Network* (SPHN) a également adopté de la documentation pour la sécurité de l'information dans la recherche biomédicale se basant entre autres sur des standards internationaux de cybersécurité[911] et la *Foederatio Medicorum Helevticorum* (FMH) a publié à l'attention des cabinets médicaux des informations générales sur la cybersécurité ou sur la sécurité des données[912].

f. En conclusion

466 Le secteur de la santé est régi par des compétences législatives et des pratiques fédérales et cantonales. Bien que les législations cantonales sortent du cadre de la présente étude, elles semblent régler des aspects déviant de la cybersécurité. Au niveau fédéral, des exigences légales de cybersécurité existent, mais uniquement pour différents cercles d'organisations pour certaines technologies spécifiques, par exemple lorsqu'il en va de la mise sur le marché ou l'exploitation de dispositifs médicaux, ou lorsqu'il en va de l'exploitation du dossier électronique des patientes. Il existe en revanche des recommandations applicables à de nombreuses institutions actives dans le secteur, à tout le moins aux établissements hospitaliers, dont le caractère contraignant est discutable.

908 GovCERT, *Cyber Security for the Healthcare Sector During Covid19*.

909 CDS, Recommandations de la CDS sur la planification hospitalière, 2022, p. 28 s.

910 H+, *Sécurité de l'information et protection des données, Exigences concernant la sécurité informatique de systèmes tiers,* 2020, p. 3.

911 SPHN, Sur les standards internationaux, cf. *supra* N 366 ss.

912 Voir par exemple FMH, *Newsletter FMH sur la cybersécurité 2/2022* ; FMH, *Protection des données et sécurité*.

Schéma 14 : la réglementation du secteur critique de la santé[913]

Secteur critique de la santé	Réglementé	Partiellement réglementé			Non réglementé
		Exigences légales	Exigences non contraignantes	Obligation(s) de signaler	
Soins médicaux		×	×	×	
Prestations de laboratoire		×	?	×	
Chimie et produits thérapeutiques		×	?	×	

7. Le secteur critique de l'information et de la communication

a. Le secteur

Le secteur critique de l'information et de la communication est particulièrement important dans le domaine de la cybersécurité. Il comprend des sous-secteurs présentant un haut niveau de criticité. Certaines organisations en faisant partie sont d'une part des infrastructures critiques et, d'autre part, des organisations dont d'autres infrastructures critiques dépendent[914]. Certaines organisations actives dans ce secteur revêtent donc un statut particulier. 467

Le secteur de l'information et de la communication se divise en quatre sous-secteurs : les services informatiques, les télécommunications, les médias et les services postaux. Les services informatiques regroupent les organisations qui fournissent des services informatiques à l'intention de l'économie ; ils concernent en particulier le traitement et le stockage de données. Les télécommunications visent les appels d'urgence, Internet, ainsi que la transmission de signaux de radio et de télévision. Les médias couvrent l'information de la population en cas de catastrophes ou de situations d'urgence et la formation de l'opinion politique[915]. Les services postaux sont les services relevant du service universel, en particulier dans les domaines de la correspondance officielle et de la correspondance commerciale[916]. 468

913 Les trois sous-secteurs sont considérés comme partiellement réglementés et non complètement réglementés bien que des exigences légales existent, dans la mesure où ces exigences ne s'appliquent pas à l'ensemble des organisations actives dans les sous-secteurs ou à l'ensemble de leurs systèmes informatiques et des traitements d'informations par le biais de moyens informatiques.

914 OFPP, *Beschreibung der Teilsektoren Kritischer Infrastrukturen in der Schweiz – Telekommunikation,* 2010, p. 1 ; OFPP, *Factsheet zum kritischen Teilsektor IT-Dienstleistungen,* 2012, p. 1 ; OFPP, *Protection de la population 27,* 2017, p. 14. Il en va de même pour le secteur critique de l'énergie.

915 Sur des définitions de la notion de média en droit suisse, cf. FRATTOLILLO, p. 51 ss.

916 FF 2018 491, p. 522 s.

469 Les législations abordées dans ce contexte donnent un aperçu de ce qui est prévu ou au contraire ce qui pourrait manquer. Les médias et les services postaux ne semblent pas être tenus au respect d'exigences légales de cybersécurité particulières, ou à des exigences adoptées par une autorité sectorielle. Ils sont en revanche soumis à des obligations de signaler ou à des obligations découlant de l'Ordonnance sur le courant faible, applicables pour la lutte contre les perturbations (bien que l'ordonnance ne concerne pas expressément des considérations de cybersécurité)[917]. En revanche, les services informatiques et les télécommunications sont plus réglementés.

b. Les services informatiques

(i) Les organisations concernées

470 Les services informatiques constituent, au même titre que les services de télécommunication, l'un des sous-secteurs les plus importants parmi les infrastructures critiques en Suisse. Ils détiennent un rôle particulier dans la mesure où, en plus de constituer des infrastructures critiques, ils fournissent des prestations importantes pour l'ensemble de la population, de l'économie et des autres infrastructures critiques[918].

471 Les fournisseuses de services informatiques offrent de nombreuses prestations différentes, allant de la vente et la maintenance de matériel informatique ou de logiciel, à des prestations de services de sécurité, de stockage ou de calcul[919]. Bien que l'Office fédéral pour la protection de la population (OFPP) distingue entre les fabricantes de matériel informatique et de logiciels, l'office admet que les prestataires de services de maintien, de maintenance et de sécurité en général entent dans cette notion[920]. Sont donc incluses des prestataires fournissant tant des produits que des prestataires offrant des prestations de services.

472 L'art. 74*b* LSI2 mentionne différents groupes d'actrices actives dans ce sous-secteur (soumises à l'obligation de signaler les cyberattaques dont elles pourraient faire l'objet). Le premier groupe vise les fabricantes de matériel informatique ou de logiciels dont les produits sont utilisés par des infrastructures critiques, si le matériel ou les logiciels concernés sont utilisés par des infrastructures critiques, à condition qu'ils disposent d'un accès de télémain-

917 Cf. *supra* N 424.

918 OFPP, *Factsheet zum kritischen Teilsektor IT-Dienstleistungen,* 2012, p. 1. La FINMA a par ailleurs reconnu dans le secteur bancaire l'importance de sécuriser la chaîne d'approvisionnement contre les cybermenaces, FINMA, *Communication sur la surveillance 03/2024,* 2024, p. 4 s.

919 OFPP, *Factsheet zum kritischen Teilsektor IT-Dienstleistungen,* 2012, p. 1.

920 OFPP, *Factsheet zum kritischen Teilsektor IT-Dienstleistungen,* 2012, p. 1.

tenance *(remote access)*[921], qu'ils soient utilisés pour commander et surveiller *(command and control)* des systèmes et des processus techniques (notamment dans le cas de systèmes de contrôle industriels ou de solutions d'automatisation qui remplissent des fonctions de contrôle et de réglage) ou qu'ils soient utilisés pour garantir la sécurité publique, à l'instar de systèmes d'enquête policière (art. 74b al. 1 litt. u LSI2)[922].

Le second groupe englobe les fournisseuses et les exploitantes « d'informatique en nuage, de moteurs de recherche, de services numériques de sécurité ou de confiance[923] ainsi que de centres de calcul », à condition qu'elles aient un siège en Suisse (art. 74*b* al. 1 litt. t LSI2). La notion de services numériques de sécurité inclut les solutions de chiffrement ou encore les moyens informatiques servant à se protéger des cyberattaques, à l'instar des programmes antivirus ou des pare-feux[924]. 473

Le troisième groupe cité dans la loi est celui des fournisseuses et des exploitantes de services et d'infrastructures servant à l'exercice des droits politiques (art. 74*b* al. 1 litt. s LSI2). L'on entend par là typiquement les systèmes de vote électronique *(e-voting)*, de gestion des registres électoraux, les entreprises chargées d'imprimer le matériel de vote ou les systèmes électroniques de récolte de signatures *(e-collecting)*[925]. 474

(ii) Le cas particulier des pirates éthiques

Parmi les différentes intervenantes dans la cybersécurité auprès des infrastructures critiques faisant l'objet de débat à l'heure actuelle, les pirates éthiques peuvent avoir des compétences semblables à celles des services numériques de sécurité. Les pirates éthiques conduisent des recherches de vulnérabilités. Cette tâche peut être complexe à assumer par les personnes compétentes pour la sécurité des fabricantes et des exploitantes de produits et systèmes informatiques[926]. Parmi les questions qui peuvent être abordées au sein de la présente étude, la première est celle liée aux possibles conséquences pénales liées à leur activité. 475

921 L'accès de télémaintenance permet à une fabricante d'accéder depuis l'extérieur et en principe par le biais d'Internet aux composants informatiques et de technologie opérationnelle du réseau local pour la maintenance ou le dépannage, cf. FF 2023 84, p. 41.

922 FF 2023 84, p. 42.

923 Les services de confiance englobent « les services de signature électronique, de cachet ou d'horodatage électroniques, d'envoi recommandé électronique, de certificats d'authentification ainsi que de conservation de signatures électroniques, de cachets électroniques ou de certificats relatifs à ces services », cf. FF 2023 84, p. 41.

924 FF 2023 84, p. 41.

925 FF 2023 84, p. 41.

926 CF, *La promotion du piratage éthique en Suisse,* 2023, p. 3.

476 Les pirates éthiques sont susceptibles d'être considérées comme des prestataires de services informatiques. Elles fournissent des services de sécurité informatiques, du moins lorsqu'elles agissent sur la base d'un contrat. En revanche, la situation est plus complexe hors contrat.

477 Les pirates éthiques ne sont aujourd'hui soumises qu'aux dispositions générales de droit pénal et de responsabilité civile en cas de comportement illicite, ou aux dispositions contractuelles du contrat les liant à leurs clientes, qu'elles agissent dans le cadre d'un contrat bilatéral avec une cliente ou sur la base conditions-cadres relatives à des contrats ouverts *(open contracts),* par exemple lorsqu'une organisation met en place des programmes de prime aux bogues *(bug bounty programs)*[927].

478 Les questions actuelles autour de leurs prestations ne visent pas réellement les cas où elles testent la robustesse des systèmes, réseaux et infrastructures informatiques de leurs clientes. En effet, dans ces cas, la cliente accepte en principe l'intrusion[928], ce qui permet à la prestataire de ne pas enfreindre de dispositions contractuelles, sous réserve du dépassement du mandat. Dans les cas où la cliente consent à l'intrusion dans son infrastructure informatique, la pirate pourrait se prévaloir du consentement de cette dernière[929]. La protection des données personnelles doit toujours être assurée par ces prestataires.

479 En revanche, certaines pirates éthiques recherchent des vulnérabilités sur les systèmes et infrastructures de tierces. Tel peut être le cas pour les pirates éthiques qui, dans le cadre d'un contrat avec une cliente, découvrent une vulnérabilité par exemple sur un logiciel, un réseau ou un système utilisé par sa cliente. Une telle situation peut également se produire lorsque des pirates agissent hors de tout contexte contractuel, par exemple en cas de soupçons qu'une organisation qui ne réagit pas fait l'objet d'une intrusion ou qu'elle a une vulnérabilité importante dans un de ses systèmes. La délimitation entre les pirates éthiques et les pirates non éthiques réside dans l'intention de la

927 Au sujet des primes aux bogues, cf. CF, *La promotion du piratage éthique en Suisse,* 2023, p. 7 et 13 ; OFCS, *Rapport sur la sécurité informatique de la Confédération en 2023,* 2024, p. 9.

928 Dans le cadre de tests de pénétration, cf. CF, *La promotion du piratage éthique en Suisse,* 2023, p. 7.

929 CF, *La promotion du piratage éthique en Suisse,* 2023, p. 8. Le consentement peut être invoqué à condition que les règles de l'art de la profession soient respectées, que la cliente soit suffisamment informée quant à la pratique et à sa signification et à ses conséquences pour avoir conscience du consentement donné et de ses limites ainsi qu'à condition que les principes généraux du droit soient respectés, cf. pour une comparaison en droit médical, ATF 133 III 121, c. 3.1, 4.1. Par ailleurs, les dispositions risquant principalement d'être enfreintes dans ce contexte sont poursuivies uniquement sur plainte, comme les art. 143*bis* al. 1 ou 144*bis* al. 1 CP.

personne s'introduisant dans un système informatique. Cette intention est difficilement déterminable[930]. Il est préférable pour ces actrices d'éviter de s'immiscer dans les systèmes d'une organisation hors de toute relation préalable afin de ne pas courir le risque d'engager leur responsabilité. En effet, l'infraction d'accès indu à un système informatique (art. 143*bis* al. 1 CP) peut être réalisée même si elle repose sur une motivation éthique[931]. Dans le cadre d'une éventuelle procédure pénale et si l'intention de s'introduire de manière indue dans un système informatique (art. 143*bis* al. 1 CP) ou de soustraire des données (art. 144*bis* al. 1 CP)[932] peut être amenée par l'accusation, des motifs justificatifs tels l'état de nécessité[933], le consentement présumé ou hypothétique ou la gestion d'affaires sans mandat[934] pourraient potentiellement entrer en considération, selon les circonstances de chaque cas d'espèce.

Au-delà des questions sur l'intrusion dans des systèmes informatiques, 480
les pirates éthiques occupent un rôle particulier pour la cybersécurité en lien avec les signalements de vulnérabilités. Les vulnérabilités peuvent être signalées à l'OFCS de façon anonyme (art. 73*b* al. 1 LSI2)[935]. Ces signalements ont pour conséquence que l'OFCS informe la fabricante du matériel informatique ou du logiciel concerné en lui fixant un délai pour l'éliminer, faute de quoi cette dernière peut être sanctionnée en vertu du droit des marchés publics et la vulnérabilité peut être rendue publique (art. 73b al. 3, 73*c* al. 2 LSI2)[936]. Le caractère anonyme du signalement permet de protéger les pirates éthiques qui seraient susceptibles de découvrir de telles vulnérabilités ou d'autres cyberincidents et cybermenaces, conformément à l'art. 73*b* al. 1 LSI2.

Si l'OFCS soupçonne que la personne à l'origine du signalement a commis 481
une infraction, il serait en théorie susceptible de la dénoncer aux autorités de poursuite pénale en vertu de l'art. 73*d* al. 2 LSI2[937]. Une telle communication risquerait de conduire à l'ouverture d'une poursuite pénale contre la pirate,

930 CF, *La promotion du piratage éthique en Suisse,* 2023, p. 5.

931 CF, *La promotion du piratage éthique en Suisse,* 2023, p. 5.

932 Pour plus d'informations au sujet des infractions liées à l'activité des pirates éthiques, ISLER/KUNZ/MOLL, N 40 ss.

933 Voir pour un avis sur l'état de nécessité dans ce contexte, ISLER/KUNZ/MOLL, N 137 ss.

934 À condition que les règles de l'art et les principes généraux du droit soient respectés et, surtout, que l'acte soit fait dans l'intérêt de la personne lésée, ce qui peut ou non être admis en pratique selon les circonstances de chaque situation.

935 L'OFCS dispose d'un formulaire pour annoncer une faille, avec la possibilité de rester anonyme, cf. OFCS, *Annonce d'une faille ou divulgation coordonnée d'une vulnérabilité (Coordinated Vulnerability Disclosure, CVD)*.

936 CF, *La promotion du piratage éthique en Suisse,* 2023, p. 10 s.

937 La disposition prévoit en effet que la personne à la direction de l'OFCS, qui doit être mise au courant, peut dénoncer en fonction de la gravité de l'infraction.

dans la mesure où un *legal safe harbour* pour les pirates éthiques a été refusé dans le cadre de la révision de la LSI. C'est pourquoi il est préférable que ces personnes passent par un signalement anonyme le cas échéant[938].

(iii) Les limites du cadre légal

482 À l'inverse des fournisseuses de services de télécommunication, les fournisseuses de services informatiques ne sont pas soumises à une législation centralisée. La cybersécurité peut être traitée, explicitement ou implicitement, de manière dispersée au sein d'autres bases légales. Ces bases légales ne se limitent pas à un cercle d'infrastructures critiques, mais ont une portée plus vaste et sont souvent destinées à l'industrie plus largement.

483 Les différentes actrices du sous-secteur ne sont pas toutes soumises aux mêmes réglementations en matière de sécurité. La loi principale pour ce sous-secteur est la Loi fédérale sur la sécurité des produits (LSPro), qui concerne notamment aux fabricantes de matériel informatique ou de logiciels. Elle est subsidiaire aux autres actes spécifiques de droit fédéral (art. 1 al. 3 LSPro). Plusieurs ordonnances s'appliquent à certains types de produits spécifiques, dont l'Ordonnance sur la sécurité des machines (Omach) ou l'Ordonnance sur les appareils à gaz (OAG).

484 La LSPro est susceptible de concerner les fabricantes de matériel et logiciel informatiques *(hardware* et *software)*. Elle requiert des produits mis sur le marché qu'ils remplissent les exigences essentielles en matière de sécurité et de santé (art. 3 al. 1 LSPro), afin de ne pas mettre l'humain en danger. Les produits sur le marché ne doivent comporter aucun risque ou se limiter à des dangers minimes compte tenu de l'usage normal ou raisonnablement prévisible du produit. Cette loi pourrait avoir vocation à s'appliquer aux fabricantes de matériel et de logiciel informatiques[939]. La LSPro et les ordonnances en découlant visent à garantir la sécurité physique et la santé et non pas la sécurité numérique. La LSPro ne prévoit aucune obligation contraignante en termes de cybersécurité.

485 En parallèle de la LSPro, les lois sur la protection des données personnelles protègent la sécurité numérique ou, en d'autres termes, la sphère privée des individus[940]. Par ailleurs et comme relevé dans une interpellation en 2017 dans le contexte plus spécifique de la sécurité des jouets, il n'est pas certain que toutes les fabricantes soient soumises à des lois de protection des données

938 FF 2023 84, p. 26.

939 FF 2008 6771, p. 6800 ; HOLLIGER-HAGMANN, art. 3 PrSG N 5. Ces fabricantes entrent dans le sous-secteur critique des services informatiques, OFPP, *Factsheet zum kritischen Teilsektor IT-Dienstleistungen,* 2012, p. 1.

940 CF, *« Intelligence artificielle » – lignes directrices pour la Confédération,* 2020, p. 9 s.

comme la LPD[941]. En effet, la fabricante mettant à disposition un jouet, mais en laissant l'exploitation à d'autres organisations du marché, n'est pas considérée comme responsable du traitement ou comme sous-traitante si elle ne traite pas de données personnelles elle-même. En revanche, les fabricantes de produits, notamment de systèmes et programmes de traitement des données, de produits matériels ou de services et processus en lien avec le traitement de données personnelles, peuvent certifier leurs produits par la certification facultative admise par l'Ordonnance sur les certifications en matière de protection des données (OCPD) en vertu de l'art. 1 al. 2 OCPD[942]. Un tel processus peut revêtir un intérêt lorsqu'une fabricante est à l'origine d'un matériel informatique ou d'un logiciel servant à traiter des données personnelles. Ce mécanisme reste toutefois limité aux aspects de protection des données personnelles.

La LSPro et la LPD se limitent à des aspects de santé et de sécurité physique 486
ou numérique. La sécurité des produits a été conçue dans un premier temps pour imposer le respect d'exigences techniques de sécurité, dans un sens marqué par l'utilisation de produits physiques. La LPD vise la protection de la sphère privée. En revanche, ce bases légales ne couvrent pas les informations qui ne constituent pas des données personnelles ou des informations couvertes par des secrets, les processus de technologie opérationnelle ou de technologie informatique ou la continuité des opérations. Ce constat est problématique dans la mesure où les fabricantes doivent tenir compte des enjeux de cybersécurité dans la conception et le développement des produits, ainsi que pour l'élaboration de correctifs lorsque des vulnérabilités sont trouvées[943].

En outre, les fabricantes ne sont pas soumises à des obligations de protec- 487
tion des données dès la conception (*privacy by design,* sous réserve qu'elles traitent elles-mêmes des données personnelles et qu'elles soient soumises aux obligations de l'art. 7 LPD) ou de cybersécurité dès la conception *(cybersecurity by design).* De nombreuses infrastructures critiques sont des utilisatrices finales et s'appuient sur une chaîne d'approvisionnement et sur des systèmes et logiciels provenant des fabricantes et fournisseuses, raison pour laquelle elles doivent particulièrement être soumises à des obligations légales de cybersécurité. La cybersécurité et la protection des données personnelles doivent être assurées dès le début de la chaîne d'approvisionnement et pour l'entier du cycle de vie des produits et des services[944].

941 Interpellation 17.4128 « Jouets connectés. Comment éviter des dérives ? » déposée le 13 décembre 2017 par Mathias Reynard.

942 OFJ, *Rapport explicatif OCPD*, 2022, p. 6 s. ; HUSI-STÄMPFLI/MORAND, p. 150.

943 SALAMON, p. 79.

944 NCSC, *Rapport semestriel 2021/2*, 2022, p. 7.

488 Pour les autres prestataires qui ne sont pas à l'origine de matériel ou de logiciel informatiques, mais qui fournissent des prestations de services comme de la maintenance ou du soutien technique, la situation est plus opaque encore. Le cadre légal suisse ne semble pas prévoir à l'heure actuelle de normes spécifiques applicables à ces organisations.

489 Certaines organisations actives dans ce sous-secteur sont susceptibles de devoir se conformer aux exigences applicables à leur clientèle. Il en va de la sorte lorsqu'elles fournissent leurs services à une autorité ou à une organisation soumise aux art. 6 ss LSI. L'art. 9 LSI prévoit que les autorités et organisations de l'art. 2 LSI reprennent les exigences de la loi dans les contrats qu'elles concluent pour collaborer avec des personnes tierces (art. 9 al. 1 LSI). Elles doivent en outre veiller à ce que la mise en œuvre des mesures soit contrôlée de manière adéquate[945]. De plus, d'autres bases légales spécifiques à certains cercles d'assujetties sont susceptibles d'être applicables par ricochet à leurs prestataires de services informatiques. Tel est le cas s'agissant de l'art. 5*a* OApEl, qui assortit d'un effet contraignant la Norme minimale pour améliorer la résilience informatique de l'OFAE pour les prestataires externes qui gèrent les systèmes TIC sur mandat d'organisations de l'art. 5*a* al. 1 litt. a et b OApEl, lorsque les prestataires ont un accès durable aux systèmes de pilotage de l'organisation (art. 5*a* al. 1 litt. c OApEl)[946].

490 Outre les normes susmentionnées et les bases légales générales en termes de responsabilité, les standards internationaux sont souvent appliqués par ces infrastructures, dès lors qu'il en va de leur intérêt et que certaines entreprises utilisent même des arguments de sécurité interne pour se distinguer des concurrentes[947]. En outre, les contrats sont déterminants dans l'encadrement de la pratique des fournisseuses des services informatiques. Ces contrats peuvent être encadrés, en tout cas lorsqu'une autorité de l'administration publique contracte avec une prestataire de services informatiques.

491 Des contrats types et des conditions générales (CG) existent pour les contrats entre bénéficiaires et prestataires de services informatiques. L'administration numérique suisse formule des recommandations, et met à disposition des collectivités des CG de la Conférence suisse sur l'informatique pour les services informatiques ainsi que des modèles de contrats[948]. Jusqu'à l'entrée en vigueur de la LSI, il était recommandé que les autorités et organisations, notamment étatiques, qui se lient avec des prestataires de gestion de cyber-

945 FF 2017 2765, p. 2831.

946 DETEC, *Rapport explicatif concernant l'avant-projet relatif à la révision de mai 2024 de l'ordonnance sur l'approvisionnement en électricité,* 2023, p. 3.

947 ChF, *Normes de sécurité pour les appareils connectés à Internet,* 2020, p. 16.

948 CONFÉRENCE SUISSE SUR L'INFORMATIQUE, *Conditions générales pour les prestations TIC*.

incidents, s'appuient sur ces modèles de contrats et sur les CG[949]. Les CG prévoient notamment des considérations relatives à la mise en demeure des prestataires, à leur responsabilité ou à la mise en place de correctifs dans le cadre de la maintenance de logiciels. En parallèle des CG, l'Administration numérique suisse met à disposition des modèles de contrats pour les prestations relevant d'un contrat d'entreprise, les prestations de services informatiques, l'achat de matériel, les licences de logiciels, la maintenance de matériel et l'entretien de logiciels, ainsi que le *Software as a Service*[950].

492 À partir du 1er janvier 2024 et l'entrée en vigueur de la LSI, les recommandations qu'élaborera le service spécialisé de la Confédération pour la sécurité de l'information devront également être intégrées dans les contrats avec des prestataires de cybersécurité. Ces contrats doivent garantir la protection des informations et des données de la Confédération, prévoir l'annonce par les prestataires des incidents liés à la sécurité de l'information ainsi qu'un droit d'audit pour la Confédération et préciser les modalités visant à démontrer la mise en œuvre des consignes de sécurité (les unités administratives devant pouvoir contrôler la mise en œuvre des mesures en vertu de l'art. 9 al. 2 LSI)[951]. Récemment, des CG et des clauses contractuelles types spécifiques ont été révisées et adoptées pour la Confédération. Ces CG et clauses contractuelles types seront analysées lors de l'examen du cadre légal applicable aux prestataires de gestion de cyberincidents. Le service spécialisé de la Confédération pour la sécurité de l'information devrait bientôt élaborer d'autres clauses et directives dans ce contexte[952]. Nous allons voir ces différentes clauses plus en détails avec l'exemple des prestataires de gestion de cyberincidents[953].

c. Les télécommunications

493 L'art. 48*a* de la Loi fédérale sur les télécommunications (LTC) impose aux fournisseuses de services de télécommunication de lutter contre toute manipulation non autorisée d'installations de télécommunication par des transmissions au moyen des TIC[954]. En ce sens, les fournisseuses peuvent dévier ou empêcher des communications ainsi que supprimer des informations (art. 48*a* al. 1 LTC).

949 Les directives et les check-lists pour les modèles de contrats sont en cours de révision, cf. ADMINISTRATION NUMÉRIQUE SUISSE, *Modèles de contrats (contrats types) conformes aux CG de la CSI*, édition 2020.

950 ADMINISTRATION NUMÉRIQUE SUISSE, *Modèles de contrats (contrats types) conformes aux CG de la CSI*, édition 2020.

951 SG-DDPS, *Législation d'exécution relative à la LSI, Explications,* 2023, p. 13.

952 SERVICE SPÉCIALISÉ DE LA CONFÉDÉRATION POUR LA SÉCURITÉ DE L'INFORMATION, *Train de mesures pour éviter de nouvelles fuites de données*, 2024, p. 2.

953 Cf. *infra* N 668 ss.

954 GCSCC, *Cybersecurity capacity review – Switzerland,* 2020, p. 11.

494 L'art. 48*a* al. 2 LTC confère au CF la compétence d'édicter des dispositions sur la sécurité des informations, des infrastructures et des services de télécommunication. Aux termes de l'art. 96*a* de l'Ordonnance sur les services de télécommunication (OST), les fournisseuses d'accès à Internet sont autorisées à bloquer des accès à Internet ainsi que des ressources d'adressage, ou à en restreindre l'utilisation si ces accès ou ces ressources d'adressage menacent de compromettre le bon fonctionnement des installations de télécommunication (art. 96*a* al. 1 OST)[955]. Ces organisations doivent également empêcher par des moyens techniques appropriés les attaques en déni de service distribué *(distributed denial of service (DDoS) attacks)*. Il leur revient en outre de configurer les caractéristiques de sécurité des installations de télécommunication mises à disposition de leurs clientes dans le respect des règles reconnues de la technique et les actualiser ou les remplacer lorsque ce n'est plus possible et qu'un risque pour la sécurité en résulte (art. 96*a* al. 2 et 3 OST)[956].

495 Les art. 96a ss OST ont un impact sur l'Internet des objets (IdO) et l'Internet industriel des objets (IIdO). Ces dispositions doivent être respectées pour garantir la cybersécurité des appareils sans fil connectés à Internet. L'Ordonnance de l'OFCOM sur les installations de télécommunication (OOIT) s'applique également dans ce contexte[957]. Les fournisseuses d'accès à Internet, qui endossent un rôle important dans la mesure où les objets de l'IdO et de l'IIdO se connectent justement à Internet, sont appréhendées par ce biais. Cela étant, les fabricantes et exploitantes d'objets connectés ne sont pas toutes des fournisseuses d'accès à Internet.

496 Le CF délègue des compétences pour l'élaboration de prescriptions de sécurité techniques et administratives à l'OFCOM (art. 96*c* OST)[958]. Ce dernier a adopté des lignes directrices, se basant sur des standards internationaux reconnus à l'instar des normes de l'UIT, des normes de l'Institut européen des normes de télécommunication (ETSI) ou ISO. Ces lignes directrices, dans un premier temps non contraignantes, peuvent être intégrées aux ordonnances. Elles prévoient des mesures pour le développement, la mise en œuvre et le réexamen en continu d'un SGSI, d'un plan de gestion de la continuité opérationnelle ou encore d'un plan de gestion d'incidents[959].

955 Voir pour les numéros attribués individuellement l'art. 24*h* ORAT.

956 Pour plus d'informations à ce sujet, cf. CF, *Infrastructure numérique. Réduire les risques géopolitiques,* 2023, p. 10 s. ; OFCOM, *Modification de l'ordonnance sur les services de télécommunication (OST),* 2022, p. 3 ss.

957 CF, *CSN,* 2023, p. 21.

958 OFCOM, *Modification de l'ordonnance sur les services de télécommunication (OST),* 2022, p. 10.

959 OFCOM, *Lignes directrices relatives à la sécurité et la disponibilité des infrastructures et des services de télécommunication,* 2023, particulièrement p. 6 ss.

Parallèlement, l'Ordonnance sur les installations de télécommunication (OIT), basée également sur la LTC, prévoit les exigences essentielles en vue de protéger la santé et la sécurité des personnes. Ces exigences doivent être respectées pour pouvoir mettre à disposition sur le marché une installation de télécommunication. L'ordonnance prévoit des mécanismes de contrôle (voir respectivement art. 7 et art. 36 OIT). Sur cette base, l'OOIT renvoie à l'OIT et soumet les exploitantes d'installations de radiocommunication et télécommunication à certaines exigences dont les celles éditées par l'OFCOM, qui peuvent prévoir des considérations de cybersécurité (voir par exemple art. 7 al. 3 litt. e OIT qui exige que des sauvegardes soient faites pour assurer la protection des données des utilisatrices). 497

Le CF a chargé le DETEC d'élaborer un projet de consultation sur la réglementation de l'activité des grandes plateformes de communication. Il n'est pas exclu que des considérations de sécurité y figurent, bien que la sécurité et la cybersécurité ne semblent pas être les points majeurs de cette potentielle future réglementation[960]. 498

d. Les obligations d'annonce

L'obligation de signaler les cyberattaques ciblant les infrastructures critiques s'applique à différentes organisations faisant partie des sous-secteurs critiques relatifs à l'information et la communication. Premièrement concernant les prestataires services informatiques, l'art. 74*b* al. 1 litt. t LSI2 prévoit tout d'abord que sont soumises à l'obligation de signaler les fournisseuses et exploitantes d'informatique en nuage, de moteurs de recherche, de services numériques de sécurité ou de confiance ainsi que de centres de calcul, pour autant qu'elles aient un siège en Suisse. Ensuite, les fabricantes de matériel informatique ou de logiciels dont les produits sont utilisés par des infrastructures critiques sont soumises à l'obligation des art. 74*a* ss LSI2 en vertu de l'art. 74*b* al. 1 litt. u LSI2, à condition que le matériel ou les logiciels concernés disposent d'un accès de télémaintenance, qu'ils soient utilisés pour commander et surveiller des systèmes et processus techniques ou qu'ils servent à la garantie de la sécurité publique. Finalement, les fournisseuses et exploitantes de services et d'infrastructures servant à l'exercice des droits politiques sont soumises à l'obligation de signaler les cyberattaques en vertu de l'art. 74*b* al. 1 litt. s LSI2. 499

Deuxièmement, le sous-secteur des télécommunications est également concerné par l'obligation de signaler les cyberattaques, dès lors que les fournisseuses de services de télécommunication enregistrés auprès de l'OFCOM 500

960 CF, *Grandes plateformes de communication : le Conseil fédéral aspire à une réglementation*, 5 avril 2023.

en vertu de l'art. 4 al. 1 LTC sont soumises à l'obligation (art. 74*b* al. 1 litt. q LSI2). Il en va de même pour les registres et registraires de domaines Internet au sens de l'art. 28*b* LTC (art. 74*b* al. 1 litt. r LSI2).

501 Troisièmement, le sous-secteur des médias est visé par l'obligation. Les agences de presse d'importance nationale et la Société suisse de radiodiffusion et télévision sont soumises à l'obligation de signaler les cyberattaques en vertu de l'art. 74*b* al. 1 litt. j et k LSI2.

502 Quatrièmement et en ce qu'il en va du sous-secteur des services postaux, les prestataires de services postaux enregistrés auprès de la Commission de la poste conformément à l'art. 4 al. 1 de la Loi sur la poste (LPO) doivent signaler les cyberattaques au sens de l'art. 74*d* LSI2 au NCSC.

503 En parallèle, d'autres obligations d'annonce sont susceptibles de s'appliquer telles que celle prévue par l'art. 24 LPD concernant les violations de la sécurité des données. Il en va de même pour certains cercles d'organisations actives dans le secteur critique, à l'instar de l'obligation pour les fournisseuses de services de télécommunication d'annoncer à la CENAL toute perturbation de l'exploitation de leurs réseaux touchant un nombre élevé de clientes (art. 96 al. 1 OST)[961].

e. En conclusion

504 Les sous-secteurs critiques des médias et des services postaux semblent être soumis uniquement à des obligations d'annonce. En revanche, la réglementation du sous-secteur critique des télécommunications se développe entre les lignes directrices de l'OFCOM et l'OST. Les mesures actuellement imposées ou recommandées sont limitées à certaines fournisseuses de télécommunication ainsi qu'à certaines mesures ou menaces. Les autorités compétentes doivent de plus examiner si les lignes directrices non contraignantes de l'OFCOM constituent une incitation suffisante pour les organisations auxquelles elles s'appliquent ou s'il devient au contraire nécessaire d'envisager de les rendre contraignantes en les intégrant à l'OST.

505 En revanche, les fournisseuses de services informatiques ne sont soumises qu'à des bases légales s'éloignant de la cybersécurité, à la réglementation contractuelle qu'elles rédigent conjointement à leur clientèle, et elles ne sont pas guidées par de plus amples instruments de droit souple. La situation est d'autant plus surprenante dès lors que ces organisations sont susceptibles de jouer un rôle particulièrement important pour la cybersécurité, notamment auprès des autres infrastructures critiques. Bien que certaines bases légales les

961 GCSCC, *Cybersecurity capacity review – Switzerland*, 2020, p. 57. La CENAL informe ensuite l'OFCOM (art. 96 al. 2 OST), cf. OFCOM, *Modification de l'ordonnance sur les services de télécommunication (OST)*, 2022, p. 8.

soumettent à des exigences minimales de cybersécurité lorsqu'elles agissent pour certaines clientes, leur activité n'est pas réglementée dans sa globalité.

Finalement, la Loi sur la sécurité des produits (LSPro) s'applique aux fabri- 506
cantes lorsqu'il s'agit de protéger la santé et la sécurité physique des utilisatrices. Les lois sur la protection des données personnelles s'appliquent lorsque de telles données sont traitées par ces biais, de même que d'autres lois transversales, par exemple relatives à la propriété intellectuelle. Des normes de droit souple s'appliquent également, prévoyant quelques considérations au sujet de la sécurité des objets connectés à Internet notamment dans le contexte des SCI[962].

Schéma 15 : la réglementation du secteur critique de l'information et de la communication[963]

Secteur critique de l'information et communication	Réglementé	Partiellement réglementé			Non réglementé
		Exigences légales	Exigences non contraignantes	Obligation(s) de signaler	
Services informatiques		×		×	
Télécommunications		×	×	×	
Médias				×	
Services postaux				×	

8. Les autres secteurs critiques

a. Le secteur critique de l'alimentation

Le secteur critique de l'alimentation se divise entre l'approvisionnement de la 507
population en denrées alimentaires et l'approvisionnement de la population ainsi que de l'économie en eau potable et en eau non potable[964]. Un approvisionnement sûr doit être garanti. L'aspect sécuritaire des denrées alimentaires

962 Voir NCSC, *Mesures de protection pour les SCI*, 2020, p. 6.

963 Les organisations actives dans le sous-secteur critique des télécommunications sont soumises à une diversité d'exigences légales et non contraignantes, mais ces exigences ne couvrent pas tous les aspects de la cybersécurité et ne s'appliquent pas forcément à l'ensemble des fournisseuses de services de télécommunication. Les fournisseuses de services informatiques sont soumises à certaines obligations légales, mais limitées à des aspects tels que la protection des données ou la sécurité des produits. Les médias et les services postaux ne semblent pas être soumis à des exigences particulières en matière de cybersécurité.

964 FF 2018 491, p. 523.

et de l'eau se concentre sur la sécurité sanitaire et ne semble pas s'étendre à la sécurité dans le cyberespace[965].

508 Quelques aspects relatifs à la sécurité informatique ont été réglés dans certaines bases légales de façon limitée. C'est le cas pour l'Ordonnance sur les denrées alimentaires et les objets usuels (ODAIOUs), concernant les jouets à l'exclusion des denrées alimentaires. Les art. 65 ss ODAIOUs prévoient les qualités que doivent revêtir les jouets pour être conformes aux exigences du marché[966].

509 En outre, l'art. 74*b* al. 1 litt. c LSI2 oblige les organisations chargées de tâches de droit public dans le domaine de l'approvisionnement en eau potable à signaler les cyberattaques de l'art. 74*d* LSI2 à l'OFCS[967]. Elle s'applique aussi « aux entreprises qui approvisionnent la population en biens d'usage quotidien indispensables et dont la défaillance partielle ou complète entraînerait de graves difficultés d'approvisionnement » (art. 74*b* al. 1 litt. p LSI2)[968].

510 À défaut d'être prévues dans des instruments purement légaux, des considérations concrètes de sécurité des TIC sont consacrées dans des normes minimales applicables au sous-secteur critique de l'approvisionnement en eau[969] et à celui de l'approvisionnement en denrées alimentaires[970]. Elles découlent de la Norme minimale pour améliorer la résilience informatique de l'OFAE et appréhendent l'utilisation de systèmes informatiques, notamment de systèmes de contrôle industriel (SCI) ou de contrôle et d'acquisition de données (*Supervisory Control and Data Acquisition,* SCADA)[971].

965 Cf. par exemple art. 7 LDAI.

966 Sur la base de l'art. 66 ODAIOUs, le DFI a adopté l'OSJo, dont l'art. 4 ch. 7 de l'annexe 2 prévoit que « les jouets dotés d'un système de commande électronique doivent être conçus et fabriqués de manière à fonctionner en tout sécurité, même en cas de dysfonctionnement ou de panne du système de commande, y compris découlant d'un facteur extérieur ». L'application de l'OSJo étant limitée aux jouets, les équipements électroniques, à l'instar d'ordinateurs et consoles de jeu utilisant des logiciels interactifs et les périphériques associés, n'y sont soumis que dans la mesure où ils ont une valeur ludique intrinsèques et sont spécifiquement conçus pour les enfants et destinés à ces derniers (art. 1 ch. 14 Annexe 1 OSJo).

967 L'obligation de signaler ne s'appliquant qu'aux tâches relevant de la puissance publique de ces organisations, cf. FF 2023 84, p. 35.

968 Il s'agit de l'approvisionnement de denrées alimentaires sans s'y limiter. L'ordonnance devra par ailleurs préciser cette catégorie d'organisations, cf. FF 2023 84, p. 39 s.

969 SSIGE, *Norme minimale pour garantir les TIC requises pour l'approvisionnement en eau,* 2019.

970 OFAE, *Norme minimale pour sécuriser la technologie de l'information et de la communication dans la filière alimentaire* 2019.

971 OFAE, *Norme minimale pour sécuriser la technologie de l'information et de la communication dans la filière alimentaire* 2019, p. 4 ; SSIGE, *Norme minimale pour garantir les TIC requises pour l'approvisionnement en eau,* 2019, p. 19. Il existe effectivement des

Schéma 16 : la réglementation du secteur critique de l'alimentation[972]

Secteur critique de l'alimentation	Réglementé	Partiellement réglementé			Non réglementé
		Exigences légales	Exigences non contraignantes	Obligation(s) de signaler	
Approvisionnement en denrées alimentaires			×	×	
Approvisionnement en eau			×	×	

b. Le secteur critique de la sécurité publique

Le secteur critique de la sécurité publique comprend l'armée, les organisations d'urgence (dont la police, les sapeurs-pompiers et les services sanitaires) et la protection civile. Plus précisément, l'armée apporte un soutien militaire en cas de catastrophe, s'engage subsidiairement pour la sûreté, aide à la conduite pour la population civile et défend le pays. Les organisations d'urgence garantissent la sécurité publique, interviennent pour apporter un secours et un sauvetage ainsi que maîtrisent des catastrophes et des situations d'urgence. La protection civile soutien des organisations partenaires dans la maîtrise de catastrophes et de situations d'urgence[973]. 511

Certaines autorités et organisations actives dans le secteur critique de la sécurité publique sont assujetties à la LSI. Tel est par exemple le cas de l'armée conformément à l'art. 2 al. 2 litt. d LSI. L'armée est donc soumise aux exigences minimales des art. 6 ss LSI comme les autorités de la Confédération[974]. En outre, les organisations chargées de tâches de droit public dans les domaines de la sécurité et du sauvetage sont soumises à l'obligation de signaler les cyberattaques au NCSC en vertu de l'art. 74*b* al. 1 litt. c LSI2. Entrent dans le cercle des 512

spécificités liées à certains secteurs, comme l'utilisation de systèmes de contrôle industriels (SCI), systèmes de contrôle et d'acquisition de données (SCADA) ou de *smart grid,* qui requièrent certaines exigences particulières en termes de cybersécurité. Pour plus d'informations sur les SCI et les considérations de sécurité s'y rapportant, cf. par exemple ASGHAR /HU/ZEADALLY, p. 2 ss ; BISSON David, *3 ICS Security Inicidents that Rocked 2016 and What We Should Learn from Them*. Au sujet des systèmes SCADA, voir notamment ARPAGIAN, chapitre 2 N 22.

972 L'examen du secteur critique de l'alimentation au sein de la présente étude est superficiel. Il n'est pas exclu que d'autres exigences existent pour la cybersécurité des organisations actives dans ce secteur critique.

973 FF 2018 491, p. 523.

974 Cf. *supra* N 382. Notamment relativement à la classification d'informations, déjà prévues par l'aOPrI est abrogée et intégrée à la LSI, art. 47 al. 1 litt. b OSI ; SG-DDPS, *Législation d'exécution relative à la LSI, Rapport explicatif,* 2022, p. 6 et 24.

assujetties en particulier les organisations d'intervention d'urgence à l'instar de la police, des services du feu, des services sanitaires et des services de sauvetage[975].

513 Au vu de la diversité d'organisations concernées par le secteur, certaines réglementations sont particulièrement dispersées. Il existe par exemple de nombreuses lois prévoyant des considérations de protection des données en lien avec l'exploitation de systèmes d'information de police cantonales ou fédérale[976].

Schéma 17 : la réglementation du secteur critique de la sécurité publique[977]

Secteur critique de la sécurité publique	Réglementé	Partiellement réglementé			Non réglementé
		Exigences légales	Exigences non contraignantes	Obligation(s) de signaler	
Armée	×				
Services d'urgence				×	
Protection civile				×	

c. Le secteur critique des transports

514 Le secteur critique des transports comprend le trafic aérien, ferroviaire, fluvial et routier. Le trafic aérien et le trafic ferroviaire couvrent le transport, respectivement aérien et ferroviaire, de personnes et de marchandises. Le trafic routier englobe tant le trafic motorisé individuel que les transports publics. Le trafic fluvial se limite au transport par les fleuves de marchandises, en particulier aux ports maritimes[978].

515 De nombreuses organisations actives dans le secteur critique des transports sont soumises à l'obligation de signaler les cyberattaques au NCSC. Une pareille obligation est prévue à l'art. 74*b* al. 1 litt. m LSI2 pour les entreprises ferroviaires au sens de l'art. 5 ou 8c de la Loi fédérale sur les chemins de fer (LCdF) ainsi que les entreprises d'installations à câbles, de trolleybus et de navigation concessionnaires selon l'art. 6 de la Loi sur le transport des voyageurs (LTV). L'obligation de signaler s'applique au transport public de voya-

975 FF 2023 84, p. 35.

976 Voir par exemple l'Ordonnance RIPOL.

977 L'examen du secteur critique de la sécurité publique au sein de la présente étude est superficiel. Il n'est pas exclu que d'autres exigences existent pour la cybersécurité des organisations actives dans ce secteur critique.

978 FF 2018 491, p. 523.

geurs, au transport ferroviaire de marchandises ainsi qu'à l'infrastructure ferroviaire. Le transport frontalier et les petites entreprises d'installations à câbles ou d'autocar au bénéfice d'une autorisation cantonale en sont en revanche exclues[979]. Il en va de même pour les entreprises de l'aviation civile détenant une autorisation de l'Office fédéral de l'aviation civile (OFAC) ainsi qu'aux aéroports nationaux du Plan sectoriel de l'infrastructure aéronautique (art. 74*b* al. 1 litt. n LSI2). Entrent dans cette catégorie les entreprises de transports aériens commerciaux qui disposent d'une autorisation d'exploitation selon l'art. 27 de la Loi fédérale sur l'aviation (LA). Les entreprises transportant des marchandises sur le Rhin conformément à la Loi fédérale sur la navigation maritime sous pavillon suisse (LNMPV) et les entreprises effectuant l'enregistrement, le chargement ou le déchargement de marchandises dans le port de Bâle doivent finalement aussi signaler au NCSC les cyberattaques au sens de l'art. 74*d* LSI2 (art. 74*b* al. 1 litt. o LSI2)[980].

Comme dans une multitude d'autres secteurs et sous-secteurs critiques, il existe des obligations d'annonces parallèles. À titre d'exemple, l'art. 14*a* LCdF impose aux entreprises ferroviaires d'annoncer à l'Office fédéral des transports (OFT) tout accident ou incident qui survient dans l'exploitation des chemins de fer, dont doivent faire partie les cyberattaques ou les cyberincidents. L'art. 77 al. 4 de l'Ordonnance sur l'aviation (OSAv) prévoit une obligation similaire en imposant aux entités lui étant soumises de déclarer à l'OFAC les événements au sens du Règlement d'exécution (UE) 2015/1018 de la Commission du 29 juin 2015 (RAC-UE). Le règlement établit une liste classant les événements dans l'aviation civile devant être obligatoirement notifiés conformément au règlement (UE) nº 376/2014 du Parlement européen et du Conseil. Parmi ceux-ci peuvent figurer les dysfonctionnements, défauts et autres problèmes d'ordre technologique ou informatique[981]. Les obligations d'annonce dans le secteur des transports ont pour objectifs la prévention de futurs incidents et l'ouverture d'une enquête à des fins de prévention (art. 2 al. 1 de l'Ordonnance sur les enquêtes de sécurité en cas d'incident dans le domaine des transports, OEIT). 516

Il existe d'autres normes, notamment techniques, qu'il serait intéressant d'analyser au-delà de la présente étude[982]. Il existe par ailleurs dans des 517

979 FF 2023 84, p. 39.

980 FF 2023 84, p. 39 s.

981 Voir dans les annexes du Règlement d'exécution (UE) 2015/1018 de la Commission du 29 juin 2015 établissant une liste classant les événements dans l'aviation civile devant être obligatoirement notifiés conformément au RAC-UE.

982 Les questions de réglementation des voitures permettant la conduite automatisée (ou des voitures autonomes ou intelligentes) soulèvent des questions dépassant le cadre

domaines tels que l'aviation civile ou les transports publics une culture de l'erreur visant à améliorer la sécurité, laquelle se traduit dans les bases légales applicables notamment par le biais des obligations d'annonce[983]. Cela étant, certains sous-secteurs ont adopté des standards concernant ces questions. Les transports publics disposent aujourd'hui d'un manuel sur la cybersécurité, prenant en considération tant le sous-secteur du trafic ferroviaire que du trafic routier[984].

Schéma 18 : la réglementation du secteur critique des transports[985]

Secteur critique des transports	Réglementé	Partiellement réglementé			Non réglementé
		Exigences légales	Exigences non contraignantes	Obligation(s) de signaler	
Transport aérien		?		×	
Transport ferroviaire		?	×	×	
Transport fluvial		?		×	
Transport routier		?	×	×	

D. Des réglementations sectorielles aux réglementations transversales

1. Une explication

518 La cybersécurité se développe majoritairement de façon sectorielle. Des considérations y étant relatives peuvent tout de même s'appliquer de façon transversale. Certains aspects réglementaires de cybersécurité tendent en parallèle

de la présente étude, dans la mesure où les infrastructures considérées comme critiques dans le sous-secteur du transport routier englobent à l'heure actuelle les organisations et autorités œuvrant pour l'infrastructure routière et non pour la fabrication et l'exploitation de voitures permettant le transport routier individuel, cf. OFPP, *Factsheet zum kritischen Teilsektor Strassenverkehr,* 2010, p. 1.

983 Pour plus d'informations à ce sujet, cf. par exemple CF, *Culture de l'erreur : possibilités et limites de son ancrage juridique,* 2022, p. 7 et 15 s.

984 OFAE/UTP, *Manuel sur la cybersécurité destiné aux entreprises de transports publics,* 2021. La norme minimale sera prise en compte dans la directive CySec-Rail de l'OFT, qui décrit les exigences minimales d'un SGSI, cf. OFT, *Dir. CySec-Rail.* À ce sujet voir également OFCS, *Rapport semestriel 2023/II,* 2024, p. 9.

985 L'examen du secteur critique des transports au sein de la présente étude est superficiel. Au vu des bases légales spécifiques applicables aux différents sous-secteurs, il n'est pas exclu que des exigences implicites ou expresses existent pour la cybersécurité des organisations actives dans ce secteur critique.

à être centralisés. Des obligations d'annonce sont imposées à des organisations actives dans une multitude de sous-secteurs critiques. Parmi ces obligations d'annonce, l'obligation à venir de signaler les cyberattaques est prévue dans la version révisée de la LSI. Une multitude d'infrastructures critiques y seront soumises. D'autres obligations d'annonce s'appliquent aux organisations actives dans plusieurs secteurs critiques, à l'instar de l'obligation d'annoncer les violations de la sécurité des données ou de l'obligation d'annonce à la CENAL.

519 Certaines dispositions légales s'appliquent sans limitation à un secteur critique, à l'instar des lois sur la protection des données. Elles s'appliquent notamment aux organisations actives dans différents secteurs critiques et prévoient certaines exigences étroitement liées à la cybersécurité.

520 D'autres normes sont susceptibles de s'appliquer à des cercles plus ou moins étendus d'organisations, comme la Norme minimale pour améliorer la résilience informatique de l'OFAE et bien que différentes normes aient été adoptées pour la concrétiser.

2. Les obligations d'annonce

a. La Loi sur la sécurité de l'information

521 La LSI s'applique principalement aux autorités et organisations au sens de son art. 2. Outre les exigences qu'elle impose à ces organisations et autorités[986], elle est en voie de révision pour introduire une obligation de signaler les cyberattaques ciblant les infrastructures critiques (art. 74*a* ss LSI2). Cette obligation s'applique aux infrastructures critiques les plus importantes pour la Suisse (art. 74*b* LSI2). Le CF adoptera courant 2024 l'ordonnance relative à cette modification de la loi afin de la concrétiser[987].

522 Les infrastructures critiques de l'art. 74*b* LSI2 sont soumises à cette obligation transversale, à moins d'être exemptées en vertu de l'art. 74*c* LSI2. La disposition prévoit que le CF exempte des organisations de l'art. 74*b* LSI2 de l'obligation de signaler lorsque les perturbations provoquées par une cyberattaque n'ont qu'un effet limité sur le bien-être de la population ou sur le fonctionnement de l'économie. Ce cercle devrait être concrétisé par l'ordonnance à venir[988]. Cette obligation doit permettre à l'OFCS de disposer d'une meilleure vue d'ensemble des cybermenaces. Elle doit également offrir la possibilité aux

986 Cf. *supra* N 383 ss.

987 ChF, *Objectifs du Conseil fédéral 2024*, 2023, p. 10.

988 Voir art. 16 P-OCyS ; ChF, *Objectifs du Conseil fédéral 2024*, 2023, p. 10 ; FF 2023 84, p. 42 s. ; OFCS, *Commentaire concernant l'OCyS*, 2024, p. 21 ss ; NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques*, 2022, p. 17 ss ; MEYER/MÉTILLE, *Loi fédérale sur la sécurité de l'information : version 2.0*, 2022, N 49 s.

infrastructures critiques de bénéficier du soutien de l'autorité (art. 74*a* al. 3 et 4 LSI2)[989].

523 Les cyberattaques produisant un effet en Suisse et visant les activités de l'art. 74*b* al. 1 LSI2 des organisations soumises à l'obligation doivent être signalées à l'OFCS[990] dans le cas où elles revêtent l'une des caractéristiques de l'art. 74*d* LSI2[991]. Les cyberattaques doivent être signalées lorsqu'elles mettent en péril le fonctionnement de l'infrastructure critique touchée, lorsqu'elles entraînent une manipulation (à l'instar d'un chiffrement) ou une fuite d'informations, lorsqu'elles n'ont pas été détectées durant une certaine période (en particulier si des indices laissent à penser qu'elles ont été exécutées en vue d'une autre attaque, typiquement dans des cas d'espionnage) ou lorsqu'elles sont accompagnées de menaces, de contrainte ou de chantage (typiquement lors d'attaques par rançongiciel)[992].

524 Le signalement doit se faire auprès de l'OFCS dans les vingt-quatre heures suivant la détection de la cyberattaque. Des informations relatives à l'organisation, à la nature et à l'exécution de la cyberattaque, à ses conséquences et ainsi qu'aux mesures prises et envisagées doivent être fournies à l'office. Si toutes les informations ne sont pas encore connues dans le délai prévu par la loi, un rapport initial doit être fourni dans les vingt-quatre heures. Les informations manquantes peuvent être transmises de façon échelonnée dès que l'organisation dispose des informations (art. 74*e* LSI2)[993].

b. L'obligation d'annoncer les violations de la sécurité des données

525 L'infrastructure critique responsable du traitement ou sous-traitante au sens d'une loi de protection des données peut être soumise à des obligations d'annoncer les violations de la sécurité des données qui l'affectent. Une violation de la sécurité des données est « toute violation de la sécurité entraînant de manière accidentelle ou illicite la perte de données personnelles, leur modification,

989 FF 2023 84, p. 33 ; NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques*, 2022, p. 14 ss ; MEYER/MÉTILLE, *Loi fédérale sur la sécurité de l'information : version 2.0,* 2022, N 47 ss.

990 FF 2023 84, p. 33 ; PC LPD-BÉGUIN/VIGNIEU, art. 24 N 81. Les art. 74*a* ss LSI2 mentionnent le NCSC, mais l'art. 15*a* Org-DDPS, adopté après que la révision de la LSI a été acceptée, prévoit que l'OFCS est le NCSC et qu'il gère le guichet national en matière de cybermenaces (art. 15*a* al. 1 et al. 2 litt. c Org-DDPS).

991 FF 2023 84, p. 42.

992 FF 2023 84, p. 43.

993 FF 2023 84, p. 44 ; HUSI-STÄMPFLI/MORAND, p. 260. Pour plus d'informations sur cette obligation, cf. MEYER/MÉTILLE, *Loi fédérale sur la sécurité de l'information : version 2.0,* 2022, N 52 ss.

leur effacement ou leur destruction, leur divulgation ou un accès non autorisés à ces données » (art. 5 litt. h LPD). Certaines infrastructures critiques sont soumises pour leurs traitements de données personnelles à la LPD, à d'autres aux lois cantonales ou à des lois étrangères, à l'instar du règlement général sur la protection des données (RGPD)[994].

526 L'infrastructure critique qui agit comme sous-traitante soumise à la LPD doit annoncer dans les meilleurs délais à la responsable du traitement toute violation de la sécurité des données qu'elle subit (voir pour les organes fédéraux et les sous-traitantes privées art. 24 al. 3 LPD)[995].

527 Si elle agit comme une responsable du traitement soumise à la LPD, l'infrastructure critique doit annoncer dans les meilleurs délais à la Préposée fédérale à la protection des données et à la transparence (PFPDT) les violations de la sécurité des données entraînant vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées (art. 24 al. 1 LPD)[996]. Ces dernières doivent également être informées si cela est nécessaire à leur protection ou lorsque la PFPDT l'exige, sous réserve qu'un motif lui permette de restreindre, différer l'information ou d'y renoncer en vertu de l'art. 24 al. 5 LPD[997].

528 La responsable du traitement doit transmettre à la PFPDT des informations relatives à une personne de contact, à la nature de la violation, à ses conséquences et aux mesures prises ainsi que, dans la mesure du possible, au moment et à la durée de la violation, aux catégories et au nombre approximatif de données personnelles concernées ainsi qu'aux catégories et au nombre approximatif de personnes concernées (art. 15 al. 1 de l'Ordonnance sur la protection des données, OPDo)[998]. Lorsque l'information des personnes concernées est nécessaire, la responsable du traitement doit leur transmettre les informations en tout cas sur la nature de la violation, sur les conséquences,

994 Bien qu'il existe plusieurs lois de protection des données susceptibles de s'appliquer aux infrastructures critiques dans leurs traitements de données, la présente étude utilise la LPD comme exemple principal.

995 FF 2017 6565, p. 6681 ; CR LPD-MÉTILLE/MEYER, art. 24 N 92 ss ; HUSI-STÄMPFLI/MORAND, p. 252 ss.

996 FF 2017 6681 ; BSK DSG-MATHYS/THOMANN, art. 24 N 23 ss ; CR LPD-MÉTILLE/MEYER, art. 24 N 28 ss, particulièrement 39 ss ; PC LPD-BÉGUIN/VIGNIEU, art. 24 N 4 ss, en particulier 12 ss.

997 Pour plus d'informations au sujet des annonces de violations de la sécurité des données en droit suisse et européen, cf. PFPDT, *TOM,* 2024, p. 12 s. ; CR LPD-MÉTILLE/MEYER, art. 24 N 28 ss ; BIERI/POWELL, p. 780 ss ; MÉTILLE/MEYER, *Annonce des violations de la sécurité des données : une nouvelle obligation de la nLPD,* 2021, p. 23 ss.

998 FF 2017 6565, p. 6681 ; OFJ, *Rapport explicatif OPDo,* 2022, p. 38 ; PFPDT, *TOM,* 2024, p. 12 ; BSK DSG-MATHYS/THOMANN, art. 24 N 46 ss ; CR LPD-MÉTILLE/MEYER, art. 24 N 57 ss.

les mesures prises ainsi que sur le point de contact (art. 15 al. 3 OPDo)[999]. À noter que l'art. 15 al. 4 OPDo impose aux responsables du traitement de documenter les violations de la sécurité des données[1000].

3. Les autres obligations de protection des données personnelles

529 Les infrastructures critiques traitant des données personnelles sont en principe soumises à une loi sur la protection des données personnelles. Il peut s'agir pour certaines de la LPD, d'une loi cantonale (à l'instar dans le canton de Vaud de la Loi vaudoise sur la protection des données personnelles, LPrD-VD)[1001], du RGPD ou de plusieurs de ces réglementations simultanément.

530 La LPD s'applique *ratione personae* aux responsables du traitement ainsi qu'aux sous-traitantes privées et aux organes fédéraux traitant des données personnelles (art. 2 al. 1 LPD), sous réserve des exceptions prévues à l'art. 2 al. 2 à 4 LPD[1002]. Les lois cantonales s'appliquent plus spécifiquement à l'administration cantonale et communale ainsi qu'aux personnes privées délégataires de tâches publiques, dans l'exercice de ces tâches, comme prévu à l'art. 3 al. 2 LPrD-VD dans le canton de Vaud, sous réserve des exceptions de l'art. 3 al. 3 LPrD-VD pour ce canton. La LPD prévoit également expressément son champ d'application territorial à son art. 3. La disposition consacre dans la loi la théorie des effets, selon laquelle tout traitement de données personnelles produisant des effets en Suisse est soumis à la LPD (sous réserve de l'applicabilité d'une loi cantonale)[1003]. Parallèlement, des entités auxquelles s'applique la loi fédérale ou une loi cantonale peuvent également être soumises au RGPD, soit territorialement soit extraterritorialement (respectivement art. 3 par. 1 et 2 RGPD) selon le lieu d'établissement de la responsable du traitement ou de la sous-traitante[1004].

531 Chacune des réglementations en matière de protection des données personnelles prévoit des principes cardinaux à respecter par les responsables du

999 OFJ, *Rapport explicatif OPDo*, 2022, p. 39 ; BSK DSG-MATHYS/THOMANN, art. 24 N 62 ss ; CR LPD-MÉTILLE/MEYER, art. 24 N 74 ss.

1000 OFJ, *Rapport explicatif OPDo*, 2022, p. 39 ; BSK DSG-MATHYS/THOMANN, art. 24 N 105 ss. La documentation des violations de la sécurité des données doit être conservée durant au moins deux ans dès l'annonce (art. 15 al. 4 *in fine* OPDo), cf. CR LPD-MÉTILLE/MEYER, art. 24 N 19.

1001 Et possiblement la LPrDS-VD.

1002 FF 2017 6565, p. 6633 ; BELSER/NOUREDDINE, N 53 ss ; BSK DSG-MAURER-LAMBROU/KUNZ, art. 2 N 20 ss ; MEIER, N 355 ss, 375 ss.

1003 La théorie des effets découlait, avant la révision de la LPD, de la jurisprudence, cf. ATF 138 II 346, c. 3 ; BELSER/NOUREDDINE, N 59 ; BSK DSG-MAURER-LAMBROU/KUNZ, art. 2 N 19b.

1004 Cf. notamment SVANTESSON, art. 3 p. 81 ss.

traitement et les sous-traitantes, parmi lesquels figure le principe et l'obligation de sécurité des données[1005]. Ces lois et les ordonnances ou règlements en découlant posent notamment un principe de sécurité des données et définissent les exigences minimales pour garantir la sécurité des traitements de données personnelles[1006]. Le principe de sécurité est par exemple prévu à l'art. 8 LPD (concrétisé aux art. 1 ss OPDo), à l'art. 10 LPrD-VD ou à l'art. 5 par. 1 litt. f RGPD. D'après ce principe, il convient pour toute responsable du traitement (et, selon la base légale, de toute soustraitante) de prendre les mesures techniques et organisationnelles s'imposant afin de garantir la sécurité des données personnelles traitées. La garantie de la sécurité des données tend à protéger la personnalité et les droits fondamentaux des personnes concernées. Les entités soumises aux différenets lois de protection des données doivent assurer l'intégrité, la confidentialité, la disponibilité voire la traçabilité des données personnelles traitées (notamment art. 2 OPDo)[1007]. Les violations de la sécurité des données, telles que la destruction accidentelle ou la soustraction de données personnelles, doivent être évitées (notamment art. 5 litt. h LPD, ou des violations de données à caractère personnel conformément à l'art. 4 ch. 12 RGPD)[1008].

Certaines réglementations précisent ce qui doit concrètement être fait 532
pour assurer le respect du principe de sécurité lorsque des données personnelles sont traitées. Tel est le cas au niveau fédéral avec les art. 1 ss OPDo, au niveau européen avec l'art. 32 RGPD ou au niveau cantonal pour le canton de Fribourg avec le Règlement fribourgeois sur la sécurité des données (RSD-FR). Les approches reposent généralement sur le risque, ce qui implique que les mesures concrètes dépendent des risques relatifs aux traitements de données personnelles. Les organisations traitant des données personnelles tiennent compte de la finalité, de la nature et des circonstances de leurs traitements, de la probabilité d'une violation de la sécurité des données et de son impact potentiel sur les personnes concernées, de l'état de la technique ou encore des coûts de mise en œuvre (notamment art. 1 OPDo, art. 32 par. 1 et 2

1005 Pour une analyse du principe de sécurité des données dans le contexte concret de la gestion de cyberincidents, cf. *infra* N 873 ss.

1006 CF, *Rapport « Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense »* 2021, p. 14.

1007 OFJ, *Rapport explicatif OPDo,* 2022, p. 19 ; PFPDT, *Guide pour le traitement des données personnelles dans le secteur privé,* 2009, p. 8 ; BSK DSG-STAMM-PFISTER, art. 8 N 2 et 24 ss ; EPINEY, N 51 ; MEIER, N 786. Le RGPD se limite à la protection de la confidentialité, de l'intégrité et de la disponibilité des données (cf. notamment art. 32 par. 1 litt. b RGPD), contrairement à la LPD révisée qui a ajouté la traçabilité comme composante de la sécurité des données (art. 2 litt. d OPDo).

1008 DE TERWANGNE, art. 5 p. 318 ; MEIER, N 789.

RGPD ou art. 8 s. RSD-FR)[1009]. Les mesures concrètes citées par les différentes bases légales portent typiquement sur la mise en place de contrôles d'accès (physiques et informatiques, chiffrement, journalisation), de sauvegardes, de mécanismes de chiffrement ou de pseudonymisation[1010], sur des mesures de détection informatique ainsi que sur l'établissement de plans de continuité ou la formation et la supervision des collaboratrices (voir notamment les art. 3 ss OPDo, 32 par. 1 RGPD ou 17 ss RSD-FR). La sécurité passe également par des processus de surveillance, contrôle et évaluation pour s'assurer de l'efficacité des mesures[1011].

533 D'autres obligations liées à la protection des données personnelles présentent un lien avec la cybersécurité en étendant l'obligation d'assurer la sécurité des données. Il en va de la sorte pour les obligations de protection des données par défaut et dès la conception[1012]. L'art. 7 al. 1 LPD impose aux responsables du traitement la mise en place de mesures techniques et organisationnelles pour que le traitement respecte les principes de protection des données dès la conception du traitement (protection des données dès la conception ou *privacy by design*). Les solutions techniques doivent être utilisées pour garantir la protection des données et pour éviter des violations de la protection des données. Entrent dans les mesures à prendre typiquement l'effacement ou l'anonymisation systématique de données personnelles[1013]. Cette obligation implique que la sécurité des données doit être garantie dès la conception d'un traitement de données personnelles. L'art. 7 al. 3 LPD impose une obligation de protection des données par défaut en exigeant des responsables du traitement qu'elles garantissent par des préréglages appropriés que

1009 OFJ, *Rapport explicatif OPDo,* 2022, p. 15 s. ; CR LPD-FANTI/STAEGER, art. 8 N 94 ss ; MEYER/DAVIES, N 16 ss. Les mêmes critères valaient déjà sous l'aLPD, cf. art. 8 al. 2 aOLPD.

1010 La pseudonymisation est la modification de données personnelles de sorte que ces dernières ne puissent plus être reliées aux personnes concernées sans informations supplémentaires ou sans efforts disproportionnés. Les données pseudonymisées étant exposées à un risque de réidentification, elles sont toujours considérées comme des données personnelles. La pseudonymisation est à distinguer de l'anonymisation, qui consiste en une modification irréversible des données personnelles de sorte qu'elles ne puissent plus être liées à une personne spécifique sans efforts disproportionnés. Les données anonymisées ne sont pas considérées comme des données personnelles, cf. PFPDT, *TOM,* 2024, p. 26 s. ; BSK DSG-BLECHTA/DAL MOLIN/WESIAK-SCHMIDT, art. 5 N 34 s. ; HUSI-STÄMPFLI/MORAND, p. 61 ss.

1011 FF 2017 6565, p. 6650 ; OFJ, *Rapport explicatif OPDo,* 2022, p. 23 ss ; BURTON, art. 32 p. 636 ; CR LPD-FANTI/STAEGER, art. 8 N 87 ss ; MEYER/DAVIES, N 22 ss.

1012 Pour une analyse des obligations de protection des données dès la conception et par défaut dans le contexte concret de la gestion de cyberincidents, cf. *infra* N 878 ss.

1013 FF 2017 6565, p. 6648 s. ; CR LPD-FANTI/STAEGER, art. 7 N 21 ss.

le traitement de données personnelles est limité au minimum par la finalité poursuivie (sous réserve que la personne concernée en dispose autrement, *privacy by default*). Les mesures prises figurent dans des réglages prédéfinis qui s'appliquent de façon standardisée à moins que l'utilisatrice ne choisisse une autre voie[1014].

4. La norme de l'Office fédéral de l'approvisionnement économique

La mesure 8 de la SNPC 2018-2022 a requis l'établissement d'une norme minimale TIC pour l'approvisionnement du pays[1015]. En vertu du principe de subsidiarité, les secteurs et sous-secteurs critiques s'autoréglementent. L'État n'intervient que subsidiairement[1016]. Partant, la réglementation de l'utilisation sûre des TIC est laissée en priorité aux différents secteurs, critiques ou non. 534

Plusieurs secteurs critiques ont publié des normes minimales et des recommandations, mais une norme est particulièrement importante dans la mesure où elle a vocation à guider des organisations actives dans divers secteurs critiques. Il s'agit de la Norme minimale pour améliorer la résilience informatique élaborée par l'OFAE. L'OFAE a adopté en 2018 et parallèlement à la Loi sur l'approvisionnement du pays (LAP)[1017] une norme minimale pour améliorer la résilience informatique dans les secteurs de l'approvisionnement. Cette norme n'est pas directement contraignante et poursuit l'objectif de fournir aux entreprises et organisations, en particulier aux infrastructures critiques, un outil leur permettant d'améliorer, sur une base individuelle, la résilience de leur infrastructure informatique[1018]. La norme tient compte des recommandations et standards internationalement reconnus[1019]. 535

1014 FF 2017 6565, p. 6649 ; CR LPD-FANTI/STAEGER, art. 7 N 49 ss.

1015 Mesure 8, CF, *Plan de mise en œuvre de la SNPC 2018-2022,* 2019, p. 31 ss ; CF, *Rapport sur l'avancement des travaux concernant la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022,* 2020, p. 19. La nécessité de cette mesure avait été confirmée par un autre groupe d'expertes, cf. GROUPE D'EXPERTS « AVENIR DU TRAITEMENT ET DE LA SÉCURITÉ DES DONNÉES », *Rapport du groupe d'experts concernant le traitement et la sécurité des données,* 2018, p. 10 ; DE WERRA/BENHAMOU, N 42. Plusieurs secteurs critiques ont établi des normes minimales en partie en réponse à cette mesure.

1016 CF, *CSN,* 2023, p. 12 ; ChF, *Rapport « Suisse 2035, les grands défis de demain en 20 questions »,* 2022, p. 115 ; GCSCC, *Cybersecurity capacity review – Switzerland,* 2020, p. 13.

1017 Loi qui avait comme but premier la fourniture de biens essentiels, WEBER/WILLI, p. 152.

1018 CF, *Normes de sécurité pour les appareils connectés à Internet,* 2020, p. 12 ; OFCS, *Rapport semestriel 2023/II,* 2024, p. 9.

1019 NCSC, *Rapport semestriel 2021/1,* 2021, p. 31 ; GCSP, *Guide to Developing a National Cybersecurity Strategy,* 2021, p. 43 ; UIT, *Guide pour l'élaboration d'une stratégie nationale de cybersécurité,* 2018, p. 44.

536 En poursuivant l'objectif d'améliorer la résilience informatique, cette norme se base sur le *NIST Core Framework* et inclut des ajouts ponctuels d'autres normes reconnues au niveau international. Elle pose les principes de base sur la sécurité informatique et un catalogue de différentes mesures. La Norme minimale pour améliorer la résilience informatique compte une centaine de mesures ainsi qu'un outil d'auto-évaluation[1020]. Les 108 mesures prévues sont divisées en 23 catégories permettant d'évaluer et d'améliorer l'organisation de la cybersécurité au sein des organisations[1021]. Les mesures forment un cadre fixe, mais demeurent suffisamment flexibles pour être adaptées aux risques spécifiques des organisations et aux nouvelles menaces. En revanche, elles ne sont pas techniques et il appartient aux organisations d'élaborer leurs mesures concrètes[1022].

537 Cette norme minimale a une portée importante. Le secteur de l'énergie la prend en compte dans les révisions du cadre légal. L'OApEl devrait rendre obligatoire la Norme minimale pour améliorer la résilience informatique de l'OFAE. En parallèle, l'ajout d'un art. 39*a* à l'OSITC devrait permettre la prise en compte de cette norme minimale dans les directives en matière de cybersécurité. C'est également sur cette base que sont adoptées les différentes normes et manuels de certains secteurs de l'approvisionnement économique, comme vu précédemment avec l'électricité, les transports publics ou encore l'approvisionnement en denrées alimentaires[1023].

E. Une synthèse

538 En raison de la subsidiarité de l'intervention étatique sur le plan réglementaire, nous assistons à une réglementation particulièrement disparate pour la cybersécurité des infrastructures critiques en Suisse. Certains sous-secteurs critiques sont soumis à des exigences légales minimales de cybersécurité. Elles sont en revanche souvent limitées à certaines pratiques, à certaines informations ou à certaines organisations. L'introduction d'obligations d'annonce à l'instar de l'obligation de signaler les cyberattaques est positive. En outre, l'adoption de bases légales comme la LSI ou de normes minimales de droit souple constituent des incitations sensées. Ces nouvelles obligations et recommandations transversales permettent une meilleure incitation des infrastructures critiques à améliorer cybersécurité.

1020 OFAE, *Norme minimale pour améliorer la résilience informatique,* 2023, p. 4.

1021 OFAE, *Norme minimale pour améliorer la résilience informatique,* 2023, notamment p. 2.

1022 DETEC, *Rapport explicatif concernant l'avant-projet relatif à la révision de mai 2024 de l'ordonnance sur l'approvisionnement en électricité,* 2023, p. 2.

1023 Cf. *supra* N 428 s., 441, 510 et 517.

En revanche, les rares sous-secteurs critiques ayant conduit des analyses quant au niveau d'incitation réglementaire nécessaire pour la cybersécurité ont conclu qu'il était nécessaire de légiférer pour que les exigences minimales de cybersécurité aient un réel impact sur l'amélioration de la résilience des organisations assujetties. C'est typiquement le cas pour le secteur de l'énergie. L'OFEN a estimé en 2021 qu'il était nécessaire d'élaborer les bases légales adéquates malgré l'existence de normes minimales non contraignantes. Cette observation s'est traduite par des modifications de la LApEl, de l'OApEl ou encore de l'OSITC. Partant, lorsque l'on voit le nombre de sous-secteurs ne disposant pas d'exigences légales de cybersécurité, on peut supposer que la résilience est globalement insuffisante dans ces sous-secteurs également. 539

Outre le nombre important de sous-secteurs critiques ne disposant pas d'exigences minimales de cybersécurité contraignantes, la majorité des exigences contraignantes et des recommandations existantes ne sont pas suffisantes car elles ne tiennent pas compte de l'ensemble des organisations du sous-secteur, elles ne s'appliquent qu'à un type de technologie ou elles sont trop générales. Par exemple, le secteur des finances est particulièrement réglementé par le biais principalement des circulaires de la FINMA, mais ces dernières ne s'appliquent pas à l'ensemble des organisations, typiquement en ce qui concerne la gestion de risques opérationnels. De la même manière, le sous-secteur critique des soins médicaux est soumis à certaines obligations légales pour des considérations spécifiques, à l'instar de l'utilisation de dispositifs médicaux ou de l'exploitation du dossier électronique de la patientèle. Certains établissements sont également concernés par des recommandations de la CDS et du NCSC qui se limitent également à certains aspects. 540

Finalement, certains sous-secteurs critiques ne sont pas réglementés au-delà des obligations d'annonce. Pour certains sous-secteurs critiques, tels que celui des biens culturels, l'accent n'est pas mis sur la cybersécurité, bien que la numérisation y soit aussi en expansion. C'est pourquoi un manque de réglementation dans un sous-secteur critique comme celui des services informatiques est plus choquant. Le sous-secteur est particulièrement critique, car les organisations qui le composent participent souvent à la chaîne d'approvisionnement ou fournissent des prestations à d'autres infrastructures critiques. 541

Bien que la CSN de 2023 prévoie un examen en continu des besoins en termes réglementaires dans le domaine de la cybersécurité, il est important de prendre conscience de la diversité des secteurs et soussecteurs critiques à analyser et à réglementer, ainsi que de la durée des processus réglementaires. 542

II. Un survol des autres domaines de la protection contre les cybermenaces

A. Une remarque introductive

543 La cybersécurité est l'un des trois domaines composant la protection contre les cybermenaces. Elle ne peut donc pas être totalement isolée des deux autres domaines lorsqu'elle est analysée. La cybercriminalité et la cyberdéfense lui sont ainsi étroitement liées.

544 La réglementation de la cybersécurité vise en priorité les organisations susceptibles de mettre en œuvre des mesures pour diminuer les risques d'être la cible de cyberattaques et afin d'appréhender des aspects relatifs aux suites d'un cyberincident.

545 En parallèle de la cybersécurité, le cadre légal pour la cybercriminalité sert à la prévention et à la répression d'infractions commises dans le cyberespace. La répression d'actes délictuels se fait en parallèle des procédures de cybersécurité en réaction aux cyberattaques. Différentes intervenantes sont impliquées.

546 La cyberdéfense est aussi étroitement liée à la cybersécurité également. Elle permet à différentes autorités de prendre des mesures pour les situations impactant la défense nationale dans le cyberespace.

547 La présente étude ayant vocation à appréhender le cadre réglementaire pour la cybersécurité, les domaines de la cybercriminalité et de la cyberdéfense seront uniquement parcourus afin de dresser une vue d'ensemble globale et de soulever quelques questions se posant en pratique.

B. La cybercriminalité

1. La criminalisation comme point de départ

a. Les infractions dans le cyberespace

548 Contrairement à la cybersécurité, la cybercriminalité est plus réglementée dans l'ordre juridique suisse[1024]. Parmi les trois domaines composant la protection de la Suisse contre les cybermenaces, le « domaine de la poursuite pénale contre la cybercriminalité » regroupe les mesures prises par les autorités de poursuite pénale dans leur lutte contre la cybercriminalité (art. 6 litt. c aOPCy)[1025]. Les lois principalement concernées sont les lois de procédures.

1024 Pour une appréciation de la législation en matière de cybercriminalité, voir par exemple JAQUIER, p. 224 s.

1025 Cf. *supra* N 34 s. ; CF, *CSN*, 2023, p. 9 ; CF, *Plan de mise en œuvre de la SNPC 2018-2022*, 2019, p. 5.

Elles permettent aux autorités compétentes de prendre des mesures pour réprimer la cybercriminalité.

549 Lorsqu'il est question de lutter contre la cybercriminalité, il s'agit en premier lieu de la définir. Ainsi, doit être entendu au sens de cybercriminalité l'ensemble des infractions pénales commises sur les réseaux de télécommunication[1026]. En d'autres termes, la poursuite pénale des délinquantes opérant dans le cyberespace est conditionnée à la réalisation d'un ou plusieurs éléments constitutifs d'infractions[1027].

550 Les infractions susceptibles d'être commises à l'encontre d'infrastructures critiques dans le cadre de la protection de la Suisse contre les cybermenaces peuvent constituer des infractions informatiques typiques ou atypiques. Les infractions informatiques typiques ou infractions informatiques au sens strict sont les infractions dirigées contre un ordinateur ou des informations traitées par des moyens informatiques[1028]. La composante informatique leur est inhérente. Les infractions informatiques atypiques ou infractions informatiques au sens large existent au contraire indépendamment de l'information et de la communication ; elles peuvent être perpétrées par l'utilisation d'un système informatique ou des données, mais elles peuvent également s'en passer[1029]. Les infractions pouvant être perpétrées contre l'État ou les infrastructures critiques peuvent être typiques ou atypiques et elles peuvent viser des biens juridiques individuels tels que le patrimoine, la liberté ou mettre en danger la collectivité[1030].

551 De nombreuses autres infractions informatiques, typiques ou atypiques peuvent être perpétrées contre des infrastructures critiques ou contre leurs collaboratrices. Ces infractions s'éloignent des comportements propres à la protection des infrastructures critiques contre les cybermenaces d'une certaine importance et sont susceptibles de porter atteinte à d'autres biens juridiques individuels et causer d'importants torts. Elles ne seront toutefois pas analysées au sein de la présente étude, dès lors qu'elles n'ont qu'un impact limité et indirect sur des intérêts tels que la protection de la sécurité nationale[1031]. Les infractions réalisées spécifiquement en temps de guerre ne seront pas

1026 Cf. notamment OFS, *SPC*, 2023, p. 6.

1027 Le cadre légal doit en effet porter en partie sur les infractions informatiques, cf. GCSP, *Guide to Developing a National Cybersecurity Strategy*, 2021, p. 48.

1028 MÉTILLE/AESCHLIMANN, p. 285 ; PERRIN/ROUBATY, p. 204.

1029 MÉTILLE/AESCHLIMANN, p. 285.

1030 Pour une distinction entre infractions informatiques typiques et atypiques, cf. notamment MÉTILLE/AESCHLIMANN, p. 285. Pour une distinction entre la cybercriminalité au sens étroit et au sens large, cf. NICOLET/PEISSARD, p. 168.

1031 Il en va de la sorte pour les infractions de pédocybercriminalité (voir typiquement art. 187 et 197 CP) ou de harcèlement (voir l'application des art. 173 s., 177 ou 180 s. CP),

non plus traitées, la présente étude se limitant aux infractions susceptibles d'être perpétrées en tout temps à l'encontre des cibles d'importance nationale en Suisse.

b. Les infractions informatiques typiques principales

552 Les principales infractions informatiques typiques figurent dans le Titre 2 du CP, qui traite des infractions contre le patrimoine. Elles visent les systèmes informatiques et les données. Chronologiquement, les auteures d'infraction débutent souvent des cyberattaques par l'intrusion dans un système informatique. L'art. 143*bis* CP réprime l'accès indu à un système informatique[1032]. La disposition réprime le *hacking,* soit le fait de s'introduire sans droit dans un système informatique[1033]. Il permet la répression d'actrices malveillantes qui, cherchant à nuire par le biais de systèmes informatiques, doivent souvent, dans un premier temps, s'introduire dans un système informatique[1034]. Tel est par exemple le cas de l'individu qui souhaite accéder aux comptes d'une personne pour réaliser diverses infractions[1035], à l'image de la pirate informatique infiltrant le compte de la collaboratrice d'un établissement financier pour surveiller des activités, atteindre les serveurs de l'établissement dans le but de soustraire des données bancaires ou diffuser un logiciel malveillant au sein d'un réseau[1036]. Dans ce cas, l'art. 143*bis* al. 1 CP trouve application si la délinquante s'y introduit « au moyen d'un dispositif de transmission de données »[1037]. Néanmoins, pour que l'infraction soit retenue, le système informatique doit être « spécialement protégé » (art. 143*bis* al. 1 CP), ce qui requiert l'existence d'une protection informatique. Si le système n'est pas techniquement protégé, la personne qui s'introduit dans un système informatique et

qui constituent des problématiques alarmantes, mais qui sont moins spécifiques aux infrastructures critiques.

1032 L'infraction est absorbée par l'art. 143 CP lorsque des données sont soustraites ou par l'art. 144*bis* CP lorsque ces dernières sont détériorées.

1033 SPAS, N 14. La mention « sans droit » permet de mettre les pirates éthiques, dont l'activité est en principe autorisée par les détentrices de systèmes informatiques à s'y introduire, sans se rendre coupable d'infractions, cf. CR CP II-MONNIER, art. 143*bis* N 11. Pour plus d'informations sur les pirates éthiques, cf. *supra* N 475 ss et *infra* N 1350 ss.

1034 Au sujet de la notion de système informatique, cf. CR CP II-MONNIER, art. 143*bis* N 3-6 ; PERRIN/ROUBATY, p. 208.

1035 SPAS, N 16 s.

1036 TEICHMANN/GERBER, *Les chevaux de Troie,* 2021, N 6.

1037 La question de savoir si un piratage à distance est nécessaire ou si la personne s'introduisant dans un système par l'ordinateur du lésé a fait l'objet de débats, cf. BSK StGB/JStG-WEISSENBERGER, art. 143*bis* N 16 ; CR CP II-MONNIER, art. 143*bis* N 9 ; MÉTILLE/AESCHLIMANN, p. 300 ; PERRIN/ROUBATY, p. 209 s.

se limite à ce comportement n'est pas punissable[1038]. La poursuite de l'infraction par les autorités est conditionnée au dépôt d'une plainte pénale au sens des art. 30 ss CP. L'art. 143*bis* al. 2 CP réprime le fait pour un individu de mettre en circulation ou de rendre accessibles les données dont il sait ou doit présumer qu'elles doivent être utilisées dans le but d'accéder indûment à un système informatique[1039]. Cette infraction revêt une certaine importance compte tenu de la professionnalisation de la cybercriminalité et de la mise à disposition par certaines délinquantes de telles données, programmes et mot de passe à des fins malveillantes.

Une fois entrée dans le système informatique, l'actrice malveillante peut 553
poursuivre des objectifs variés, tels que mener des actes de sabotage (comme couper l'alimentation électrique d'une commune ou modifier le fonctionnement d'un système de commande et court-circuiter un système de contrôle industriel) ou chercher à soustraire ou à détériorer des données. Elle peut également chercher à chiffrer ou modifier l'intégrité de sets de données dans le but de formuler une demande de rançon ou encore causer un déni de service (*denial of service,* DoS)[1040]. Certaines de ces actions impliquent des infractions informatiques atypiques, d'autres des infractions informatiques typiques. Parmi ces dernières, les principales sont la soustraction de données (art. 143 CP), la soustraction de données personnelles (art. 179*novies* CP) ou encore la détérioration de données (art. 144*bis* CP)[1041].

La délinquante cherchant à détériorer des données est susceptible de 554
se rendre coupable de détérioration de données au sens de l'art. 144*bis* al. 1 CP. Cette infraction est majoritairement commise par le biais de TIC[1042]. L'art. 144*bis* CP ne requiert pas que les données modifiées soient spécialement protégées contre tout accès. Il suffit en effet que ces données soient modifiées, effacées ou mises hors d'usage sans droit[1043]. Il en va de la sorte s'agissant de l'organisation tierce qui cherche à défacer ou défigurer le site Internet d'une administration communale afin que les utilisatrices se connectant au site se

1038 L'art. 143*bis* al. 1 CP n'incrimine donc pas la personne accédant à un système informatique en dépit d'une protection morale, contractuelle ou physique, CR CP II-MONNIER, art. 143*bis* N 7 ; MÉTILLE/AESCHLIMANN, p. 298 ss ; PERRIN/ROUBATY, p. 209 ; TEICHMANN/GERBER, *Les attaques classiques par ransomware,* 2021, N 7.

1039 MÉTILLE/AESCHLIMANN, p. 302 s.

1040 PERRIN/ROUBATY, p. 213.

1041 Il en existe d'autres, voir par exemple pour l'art. 147 CP (utilisation frauduleuse d'un ordinateur) notamment MÉTILLE/AESCHLIMANN, p. 309 ss.

1042 En 2021, il est ressorti de la statistique policière de la criminalité que 90,2% des détérioration de données au sens de l'art. 144*bis* CP étaient commises par le biais des TIC, cf. OFS, *SPC 2022,* 2023, p. 6

1043 CR CP II-MONNIER, art. 144*bis* N 2 ; SPAS, N 107.

retrouvent non plus sur la page d'accueil du site de l'administration, mais sur une autre page, laquelle afficherait notamment des convictions politiques, idéologiques ou religieuses[1044]. Ce détournement de site Internet entraîne une modification des données, souvent limitée à la page d'accueil d'un site Internet. Ce comportement est constitutif de l'infraction de détérioration de données et est réprimé en Suisse par l'art. 144*bis* CP. L'attaque DDoS consiste en la mise hors d'usage, au moins temporaire, de données[1045]. À noter que, de la même manière que l'art. 143*bis* al. 2 CP en lien avec la mise en circulation de données, l'art. 144*bis* ch. 2 CP réprime la fabrication et la mise en circulation intentionnelle de programmes de détérioration de données[1046].

555 Souvent, les auteures de cyberattaques cherchent à dérober des données. L'art. 143 al. 1 CP peut trouver application s'agissant de tels actes. La disposition incrimine le fait pour une personne de soustraire, dans le dessein de procurer un enrichissement illégitime, des données spécialement protégées et enregistrées ou transmises électroniquement, alors qu'elles ne lui sont pas destinées (ou, en d'autres termes, auxquelles elles n'ont pas le droit d'accéder)[1047]. Contrairement à l'art. 143*bis* CP, l'art. 143 CP peut être réalisé si les données sont protégées par une barrière informatique ou physique[1048]. Nous soutenons qu'il suffit que l'auteure accède aux données et qu'elle puisse les exploiter selon ses besoins ; il n'est donc pas nécessaire qu'elle les enregistre effectivement sur un support lui appartenant[1049]. Si, en outre, les données soustraites constituent des données sensibles (art. 5 litt. c LPD)[1050] non accessibles à toute personne,

1044 D'autres infractions peuvent intervenir en concours, cf. Notamment MÉTILLE/AESCHLIMANN, p. 305 ss.

1045 Sur les attaques DDoS, cf. *supra* N 71 ; CR CP II-MONNIER, art. 144*bis* N 4 ; TEICHMANN/GERBER, *La qualification pénale des attaques DDoS en droit suisse*, 2021, N 24. Parmi les autres concours imaginables, l'individu agissant de la sorte par espièglerie ou par méchanceté et pour importuner ou inquiéter une personne tierce peut également se rendre coupable d'utilisation abusive d'une installation de télécommunication (art. 179*septies* CP). Si c'est le site d'un service d'intérêt général qui es mis hors d'usage, il faut également envisager l'application de l'art. 239 ch. 1 al. 1 CP (entraves aux services d'intérêt général), cf. SPAS, N 41, 43 et 45 ; TEICHMANN/GERBER, *La qualification pénale des attaques DDoS en droit suisse*, 2021, N 27 s. et 32.

1046 Cf. notamment MÉTILLE/AESCHLIMANN, p. 307 ss.

1047 PERRIN/ROUBATY, p. 206 s.

1048 Elle ne peut en revanche pas être morale ou contractuelle, cf. PERRIN/ROUBATY, p. 206 ; CR CP II-MONNIER, art. 143 N 6 s. ; MÉTILLE/AESCHLIMANN, p. 291.

1049 Du même avis, FF 2010 4275, p. 4283 ; PERRIN/ROUBATY, p. 212 ; TEICHMANN/GERBER, *Le phishing*, 2021, N 19. Soulevant la controverse, SPAS, N 104. Au sujet de la controverse, cf. notamment PERRIN/ROUBATY, p. 211 s.

1050 Les profils de la personnalité ne sont plus couverts par cette norme, la LPD révisée ne consacrant plus cette notion, FF 2017 6565, p. 6741.

l'art. 179*novies* CP peut s'appliquer (en concours avec l'art. 143*bis* CP)[1051]. Si les conditions de l'art. 143 CP et de l'art. 179*novies* CP sont réunies, les deux dispositions entrent en concours idéal, dans la mesure où la première protège les intérêts de la personne qui traite les données et la seconde protège la personne concernée par les données[1052]. En revanche, au contraire de l'art. 143 CP, l'art. 179*novies* CP n'est poursuivi que sur plainte.

Il est courant pour des délinquantes de faire usage de rançongiciels pour 556
chiffrer les données (ou pour modifier un set de données) de la lésée et, souvent, pour les soustraire (de manière lisible pour cette dernière. Les données ne sont en principe rendues accessibles à l'organisation lésée dans leur version originale que moyennant le paiement d'une rançon. Dans ce cas, la délinquante risque de se rendre coupable de différentes infractions dont, en tant qu'infractions typiques, d'une part la détérioration de données (mises hors d'usage) et, d'autre part, la soustraction de données au sens de l'art. 143 CP (et éventuellement de données personnelles selon l'art. 179*novies* CP). L'auteure se limitant à chiffrer les données ou à bloquer le système informatique d'autrui et requérir le paiement d'une rançon contre transmission de la clé de déchiffrement peut se rendre coupable, en concours, de détérioration de données (art. 144*bis* CP) et d'extorsion (art. 156 CP)[1053]. Au stade plus précoce de la diffusion de programmes malveillants, la criminalisation des comportements de l'auteure dépend du type de matériel informatique ou de logiciel malveillant utilisé et du but poursuivi par cette dernière[1054].

c. Les infractions informatiques atypiques principales

En parallèle des infractions informatiques typiques principales, de nom- 557
breuses infractions informatiques atypiques peuvent être commises par des cyberattaquantes à l'encontre d'infrastructures critiques. Certaines infractions s'appliquent à un large éventail de situations, d'autres sont plus spécifiques. Sans entrer dans les détails, certaines infractions atypiques sont en particulier rencontrées en pratique.

Dès lors que la commission de cyberattaques est couramment motivée par 558
des motifs de nature économique, d'autres infractions contre le patrimoine

1051 CR CP II-MONNIER, art. 179*novies* N 11.

1052 CR CP II-MONNIER, art. 143 N 17.

1053 TEICHMANN/GERBER, *Les attaques classiques par ransomware,* 2021, N 14 et 17. L'infraction d'extorsion est réalisée si la personne lésée succombe effectivement à la menace. Le logiciel malveillant Ryuk fonctionnait comme cela, TEICHMANN/GERBER, *Les chevaux de Troie,* 2021, N 5, 10 et 22.

1054 SPAS, N 37. Sur les art. 143 et 179*novies* CP, cf. notamment MÉTILLE/AESCHLIMANN, p. 289 ss.

peuvent trouver application. Tel est le cas de l'extorsion qui est l'une des infractions les plus perpétrées. En effet, un nombre important d'attaques par rançongiciel a été recensé ces dernières années en Suisse comme ailleurs, et ces attaques sont à l'origine de dommages considérables[1055]. Pour que l'infraction soit réalisée, la délinquante doit pousser autrui à des actes préjudiciables à ses intérêts pécuniaires ou à ceux d'une personne tierce en usant de violence ou de menace d'un danger sérieux ; elle doit de plus agir avec un dessein d'enrichissement illégitime (art. 156 ch. 1 CP). Cette infraction est souvent réalisée lors de l'utilisation de rançongiciels impliquant le chiffrement de données ou la congestion d'un serveur informatique comme moyens de pression sur les victimes pour exiger le paiement de rançons[1056].

559 Outre l'extorsion, l'infraction d'escroquerie (art. 146 CP) peut également s'appliquer à des agissements en ligne. C'est le cyberincident le plus fréquemment signalé au NCSC[1057]. Pour que l'infraction soit réalisée, les différents éléments constitutifs de l'escroquerie doivent être réunis[1058], en particulier la tromperie astucieuse et l'erreur de la dupe (art. 146 al. 1 CP)[1059]. Il est important que le mensonge de l'auteure soit échafaudé avec des artifices, des mises en scène, des édifices de mensonges ou d'autres manœuvres frauduleuses et que la personne trompée ne puisse pas se protéger avec le minimum d'attention que l'on peut attendre d'elle[1060]. Sont inclus dans les comportements réprimés les « arnaques au président » lors desquelles une délinquante se fait passer pour une membre de la direction d'une organisation et, ce faisant, détermine une collaboratrice à effectuer un versement urgent, confidentiel et exceptionnel préjudiciable pour l'organisation ou pour la collaboratrice[1061]. Dans de nombreux cas, les délinquantes se font également passer pour des

1055 Notamment NCSC, *Rapport semestriel 2023/I*, 2023, p. 25 ; NCSC, *Rapport semestriel 2021/2*, 2022, p. 18.

1056 NCSC, *Rapport semestriel 2021/2*, 2022, p. 21 ; SRC, *La sécurité de la Suisse* 2022, p. 75 ; TEICHMANN/GERBER, *La qualification des attaques DDoS en droit Suisse*, 2021, N 26.

1057 NCSC, *Rapport semestriel 2023/I*, 2023, p. 17 ; NCSC, *Rapport semestriel 2021/2*, 2022, p. 12. Les cas d'escroquerie, déjà très présents dans la SPC de 2022, ont encore augmenté entre 2022 et 2023, cf. OFS, *SPC*, 2023, p. 6. L'escroquerie est par ailleurs toujours le phénomène le plus annoncé à l'OFCS, cf. OFCS, *Rapport semestriel 2023/II*, 2024, p. 17.

1058 À savoir la tromperie, l'astuce, l'erreur, l'acte préjudiciable aux intérêt pécuniaires, le dommage, l'intention et le dessein d'enrichissement illégitime.

1059 SPAS, N 66.

1060 SPAS, N 66. Des artifices et autres manœuvres frauduleuses ne sont pas nécessaires s'il est impossible de contrôler la véracité des informations, si ce contrôle est possible mais que la victime en est dissuadée par l'escroc ou que l'auteure présume que la dupe accepterait ses dires sans vérification, en raison d'une relation de confiance particulière, d'un règlement ou d'assurances claires, SPAS, N 67 s.

1061 SPAS, N 60 ; NCSC, *Arnaque au président*, 4 décembre 2021.

entités telles que des autorités étatiques ou des services de livraison, dans quel cas elles partagent des informations plus ou moins cohérentes et disposent parfois même d'un site Internet. Elles mettent ensuite la pression sur la collaboratrice du service comptabilité d'une organisation qui pourrait la déterminer à verser à ces personnes malveillantes une somme leur permettant un enrichissement illégitime[1062].

L'usurpation d'identité (art. 179*decies* CP), infraction introduite en septembre 2023 en droit suisse, est également susceptible de s'appliquer. Est poursuivie toute personne qui utilise l'identité d'une autre personne sans son consentement, à condition que cet emploi poursuive un dessein de nuire à la personne concernée ou d'engendrer un avantage illicite[1063]. Replacée dans le contexte informatique, l'infraction est notamment réalisée dans le cas où une attaquante se fait passer pour la collaboratrice d'une organisation après l'avoir hameçonnée afin de se faire passer pour cette dernière, puis de s'introduire dans des systèmes informatiques spécialement protégés dans le but de soustraire des informations à l'organisation. La délinquante cherche par l'hameçonnage (ou le *phishing*) à soutirer frauduleusement des renseignements personnels sur sa cible[1064]. Elle peut soit procéder de façon « classique » en utilisant principalement des techniques d'ingénierie sociale, soit utiliser des moyens techniques, en installant par exemple un programme malveillant lui permettant d'agir comme une *« woman in the middle »* en interceptant les données transmises entre sa cible et des personnes tierces (ce qui constituera éventuellement déjà un accès indu dans un système informatique)[1065]. L'hameçonnage ne constitue pas en tant que tel une des infractions en droit pénal suisse ; c'est une fois que l'auteure se fait passer pour la personne hameçonnée et adopte certains comportements que des infractions de droit suisse sont susceptibles d'être réalisées[1066]. 560

1062 NCSC, *Rapport semestriel 2023/I*, 2023, p. 17. Pour des exemples d'escroquerie, NCSC, *Rapport semestriel 2021/2*, 2022, p. 12. Pour des statistiques sur les différentes manœuvres d'escroquerie, cf. OFS, *SPC*, 2023, p. 62.

1063 FF 2017 6565, p. 6741 s.

1064 Le nombre d'infractions par *phishing* recelé a par ailleurs doublé de 2020 à 2021, passant de 642 à 1210, OFS, *SPC*, 2022, p. 60.

1065 Pour plus d'informations au sujet des questions que soulève l'hameçonnage, voir notamment TEICHMANN/GERBER, *Le phishing*, 2021, N 9 ss, particulièrement 14 ss. Pour d'autres exemples démontrant les progrès effectués par les attaquantes dans l'utilisation ou la combinaison de techniques d'ingénierie sociale, cf. par exemple NCSC, *Rapport semestriel 2021/2*, 2022, p. 32 ss.

1066 À l'instar de l'infraction d'usurpation d'identité, une fois que la délinquante se fait passer pour la personne qu'elle a hameçonnée, ou de l'infraction d'escroquerie lorsqu'elle tente, avec les informations d'une employée, pour laquelle elle se fait passer, de déterminer une autre collaboratrice de l'organisation d'effectuer un versement indu.

561 L'auteure derrière une cyberattaque peut se rendre coupable d'autres infractions du CP. Si elle agit dans un premier temps par courriel en se faisant passer pour une autorité, à l'instar de l'Office fédéral des douanes et de la sécurité des frontières (OFDF), requérant des émoluments de la part de l'organisation cible, il est possible que les éléments constitutifs du faux dans les titres de l'art. 251 CP soient réunis. Pour ce faire, il est nécessaire que le faux porte sur un titre au sens de l'art. 110 al. 4 CP, à savoir sur un titre écrit destiné et propre à prouver un fait ayant une portée juridique[1067]. Un courant doctrinal estime qu'un site Internet falsifié peut également constituer un titre s'il a une portée juridique, ce qui serait le cas si le faux matériel permet à la personne dupée d'ouvrir une session d'*e-banking*[1068]. L'auteure utilisant un rançongiciel dans un autre objectif qu'économique (par exemple pour des raisons idéologiques), peut être poursuivie pour menaces (art. 180 CP) ou contrainte (art. 181 CP) dans le cas où elle menace par exemple une autorité de ne pas lui transmettre la clé de déchiffrement contre la relaxe de détenues extrémistes. À noter toutefois que si la victime est une autorité ou la fonctionnaire d'une autorité, l'art. 285 CP (violence ou menace contre les autorités et les fonctionnaires) prime en principe les art. 180 et 181 CP[1069]. Lorsque les cybercriminelles agissent par bande de trois comparses au minimum et disposent d'une organisation effective avec division des tâches et tirant profit par exemple du partage de logiciels malveillants ou de données soustraites à leurs cibles, elles sont susceptibles de former une organisation criminelle (ou terroriste) au sens de l'art. 260*ter* CP (organisations criminelles et terroristes)[1070]. De nombreuses actrices sur le plan international cherchent, par exemple à des fins d'espionnage, à introduire dans les systèmes informatiques d'entreprises ou entités administratives des logiciels malveillants permettant d'analyser les activités et le trafic. Dans de telles situations, les art. 272 ss CP (espionnage) peuvent trouver application. Finalement, dans le cas où une auteure soustrait des données pour les vendre, la vendeuse et l'acquéreuse risquent d'être poursuivies pour blanchiment d'argent selon l'art. 305*bis* CP[1071]. En revanche, il n'existe à l'heure actuelle pas d'infraction de recel de données[1072].

1067 CR CP I-SCHUBARTH, art. 110 N 8.

1068 Dans ce cas, les éléments constitutifs de l'art. 251 CP seraient réunis, à savoir l'acte typique de création d'un faux, l'intention et l'intention de tromper autrui, cf. références citées par TEICHMANN /GERBER, *Les chevaux de Troie,* 2021, N 23.

1069 CR CP II-BOETON ENGEL, art. 285 N 58.

1070 TEICHMANN/GERBER, *Les chevaux de Troie,* 2021, N 24.

1071 TEICHMANN/GERBER, *La qualification des attaques DDoS en droit suisse,* 2021, N 34. Les infractions de blanchiment d'argent ont été commises à 82% par moyens numériques en 2021, OFS, *SPC,* 2022, p. 6.

1072 CR CP II-HENZELIN/MASSROURI, art. 160 N 7 s.

Les infractions des art. 221 ss CP peuvent également entrer en considération. 562
L'infraction d'incendie intentionnel (art. 221 CP) fait partie des dispositions adoptées à une époque où l'on considérait principalement des moyens physiques pour démarrer un feu. Aujourd'hui, l'on sait qu'une surchauffe ou un court-circuit peut créer une fumée importante et nocive potentiellement à l'origine d'un incendie ; il en va de même de la panne d'un système de refroidissement ou d'une autre composante informatique. Les cyberattaques étant susceptibles de viser de tels objectifs, il n'est pas exclu qu'une délinquante cherche à causer un incendie par des moyens numériques[1073]. L'on peut raisonner de manière analogue pour l'explosion (art. 223 CP)[1074].

Dans le cadre spécifique des attaques ciblant des infrastructures cri- 563
tiques, l'infraction d'entrave aux services d'intérêt général (art. 239 CP) peut également entrer en ligne de compte[1075]. La disposition punit par exemple les personnes mettant hors d'usage par le biais d'un moyen de communication le système informatique d'une entreprise fournissant un service à la collectivité. Cela peut typiquement se faire par la surcharge d'un réseau[1076].

Au-delà de ces infractions pouvant en principe s'appliquer de manière 564
transversale à tous les secteurs (critiques ou non), d'autres infractions visent des situations plus spécifiques ou revêtent des caractéristiques propres à certaines circonstances. C'est par exemple le cas de l'art. 142 CP, qui réprime la soustraction d'énergie. Cette disposition est applicable lorsqu'une personne cherche, par des manipulations informatiques, à soustraire de l'énergie à l'exploitante d'une installation de production, de transport ou de stockage d'énergie[1077]. Si l'auteure soustrait sans droit de l'énergie par ce biais, elle peut se rendre coupable de soustraction d'énergie. L'on peut finalement citer dans le secteur spécifique des télécommunications l'infraction d'utilisation abusive d'une installation de télécommunication (art. 179*septies* CP), lorsque

1073 À noter que la délinquante découverte par les autorités de poursuite pénale avant avoir mis son plan en exécution peut être condamnée pour des actes préparatoires délictuels en vertu de l'art. 260*bis* al. 1 litt. g CP, cf. CR CP II-PAREIN-RAYMOND/PAREIN/VUILLE, art. 321 N 33.

1074 À condition que les autres éléments constitutifs de l'infraction soient réalisés ou qu'il s'agisse d'une tentative. Cette réflexion peut s'appliquer selon nous par analogie à la majorité des art. 224 à 239 CP.

1075 Pour que l'infraction soit réalisée, il faut un service d'intérêt général et une entrave à ses prestations ; l'infraction peut être réalisée intentionnellement ou par négligence.

1076 TEICHMANN/GERBER, *La qualification des attaques DDoS en droit Suisse,* 2021, N 32. L'art. 239 CP fait également partie des dispositions intéressantes pour les actes de désinformation.

1077 CR CP II-JEANNERET, art. 142 N 5. Il convient de ne pas oublier que les motifs justificatifs peuvent toujours s'appliquer, dont l'état de nécessité de l'art. 17 CP, cf. CR CP II-JEANNERET, art. 142 N 10.

l'auteure utilise abusivement une installation de télécommunication pour inquiéter ou importuner autrui[1078].

565 Le droit pénal accessoire peut également s'appliquer à certains cercles de personnes en particulier. Tel est le cas du Code pénal militaire (CPM). Le CPM contient des dispositions spécifiques s'appliquant aux personnes listées aux art. 3 à 5 CPM. Lorsque le droit pénal militaire prévoit une infraction spécifique, il prime l'application du droit pénal ordinaire. En revanche, le droit pénal ordinaire s'applique aux personnes soumises au droit pénal militaire pour les infractions non prévues par le Code pénal militaire (art. 8 CPM). Parmi les infractions susceptibles d'être réalisées par une cyberattaque, l'art. 86 CPM réprime l'espionnage et la trahison par violation de secrets militaires, l'art. 86a la destruction et l'endommagement des installations ou choses servant à l'armée et l'art. 87 la trahison militaire. L'espionnage militaire au préjudice d'un État étranger est également réprimé à l'art. 93 CPM et la violation de secrets militaires est punie par l'art. 106 CPM.

d. Le droit pénal accessoire

566 Bien que le CP soit la source principale listant les infractions de droit suisse, des normes de droit pénal accessoire peuvent parfois s'appliquer aux cyberattaques d'importance nationale. Certaines lois ont un champ d'application personnel spécifique, comme la LTC. D'autres lois peuvent également s'appliquer à des situations particulières. C'est par exemple le cas des dispositions pénales prévues par la loi sur la concurrence déloyale ou sur la propriété intellectuelle, qui peuvent trouver application s'agissant de la répression de cas d'espionnage, fréquents entre infrastructures critiques.

567 La loi sur la concurrence déloyale (LCD) interdit certains comportements au vu de leur influence déloyale sur le marché. Par exemple, la société qui exploite le résultat du travail d'une société tierce en ayant soustrait indûment des données de cette dernière agit de façon déloyale selon l'art. 5 litt. b LCD. Il en va de même pour celle qui reprend par des procédés techniques de reproduction et sans sacrifice correspondant le résultat du travail d'autrui (art. 5 litt. c LCD). Celle qui s'introduit dans les systèmes d'une autre organisation et soustrait des données soumises au secret de fabrication ou d'affaires agit également de façon déloyale si elle les exploite ou les divulgue (art. 6 LCD). La conséquence est que la personne qui agit de manière déloyale peut se voir punir conformément à l'art. 23 al. 1 LCD, à condition que l'entreprise lésée dépose plainte (art. 9 et 10 par renvoi de l'art. 23 al. 2 LCD). Les clientes de l'entreprise lésée ont également la qualité d'agir si leurs intérêts économiques

1078 TEICHMANN/GERBER, *La qualification des attaques DDoS en droit Suisse,* 2021, N 27 s.

sont mis en danger ou lésés (art. 10 al. 1 LCD). De même, la Confédération est habilitée à déposer plainte si la réputation de la Suisse à l'étranger est menacée ou subit une atteinte et que les personnes dont les intérêts économiques sont touchés résident à l'étranger, ou si des intérêts collectifs sont menacés ou lésés (art. 10 al. 3 LCD).

568 Une attaquante qui divulgue, modifie une œuvre (au sens de l'art. 1 al. 1 de la Loi sur le droit d'auteur et les droits voisins, LDA) ou commet l'un des comportements constitutifs d'une violation du droit d'auteure est réprimée par l'art. 67 LDA. L'art. 69 LDA prévoit une répression similaire pour les droits voisins au sens des art. 33 ss LDA. L'art. 69 al. 1 litt. g ou i pourrait typiquement s'appliquer si une entreprise télévisuelle est visée par l'attaque. Lorsque l'on est dans un contexte d'application de la LDA, la personne contournant des « mesures techniques efficaces » à l'instar de contrôle d'accès ou de cryptage au sens de l'art. 39*a* avec l'intention de faire une utilisation illicite d'œuvres ou autres objets protégés peut être poursuivie sur la base de l'art. 69*a* al. 1 litt. a LDA. Il en est de même concernant la personne qui fabrique, importe ou encore met en circulation des dispositifs permettant un tel contournement (art. 69*a* al. 1 litt. b ch. 3 LDA).

569 Il existe naturellement d'autres bases légales réprimant des comportements pertinents dans ce contexte. Par exemple, une cyberattaque peut consister en l'utilisation illicite d'une invention brevetée (art. 66 litt. a et 81 al. 1 LBI). Un tel cas de figure est envisageable si l'attaquante est une concurrente de l'entreprise lésée.

2. Les mesures de lutte contre la cybercriminalité

a. Une histoire de compétences

(i) Au niveau suisse

570 Les art. 3 à 8 CP règlent le champ d'application territorial du Code pénal et, par conséquent, du Code de procédure pénale. Le droit pénal suisse s'applique aux personnes commettant un délit ou un crime en Suisse[1079].

571 Au niveau interne du pays, la question de la division des compétences entre autorités de poursuite pénale cantonales et fédérales est régie par les art. 22 ss CPP. La compétence cantonale est le principe et la compétence fédérale constitue l'exception. Les art. 23 s. CPP indiquent si l'on se trouve dans un cas de compétence fédérale. Relèvent par exemple de cette compétence des juridictions fédérales les actes pour lesquels la technologie des procédés utilisés à des fins malveillantes est particulièrement complexe, que l'affaire revêt

1079 Pour des questionnements en lien avec les problèmes liés au principe de territorialité dans les infractions informatiques, cf. notamment MÉTILLE/AESCHLIMANN, p. 287.

une composante internationale ou encore en fonction de l'ampleur sur le plan national d'une infraction et de l'importance des dommages subis par les personnes lésées. Cela concerne également la situation dans laquelle un État étranger concourt à la réalisation d'une infraction, typiquement dans un cadre d'espionnage, de menace contre les autorités et les fonctionnaires ou encore dans certains cas de criminalité organisée (art. 23 al. 1 litt. h et 24 CPP). Les compétences en matière d'importantes cyberattaques ne sont pas toujours claires et la compétence suisse peut facilement être niée. Le Tribunal pénal fédéral (TPF) a par exemple admis une compétence fédérale pour des cas d'hameçonnage en raison de la multiplication des cas de phishing en Suisse, des difficultés techniques et du fait que les personnes à l'origine d'escroquerie résident souvent à l'étranger. Le TPF a estimé pour la même affaire qu'aucune compétence fédérale ne pouvait être justifiée pour les managers financiers, ces dernières opérant le plus souvent en Suisse[1080]. Il existe des situations complexes exigeant une étroite collaboration. Le blanchiment d'argent implique souvent l'ouverture d'une procédure fédérale contre les auteures principales ainsi qu'une ou plusieurs procédures cantonales, à la suite par exemple de plaintes de victimes et de la dénonciation d'une *money mule* dans un autre canton[1081].

572 Les questions de compétences ne sont pas réglées aujourd'hui pour toutes les infractions informatiques que l'on peut rencontrer. Il existe en pratique encore bon nombre de conflits de compétence, que la jurisprudence continue à délimiter.

573 En marge de la question de la répartition des compétences entre la Confédération et les cantons, il existe d'autres questions de compétences internes à la Suisse. Certaines questions de for peuvent se poser et les art. 31 à 42 CPP permettent de désigner le canton compétent pour diligenter la procédure pénale lorsque la compétence fédérale est exclue. Ces règles revêtent naturellement un intérêt spécial dans des affaires de cybercriminalité. Le principe est celui du for de lieu de commission, qui peut s'avérer délicat à trouver lors d'une cyberattaque.

574 Il existe finalement également des questions relatives aux cybercompétences internes à chaque autorité. Toujours plus de cantons développent des compétences spécifiques pour les cas présentant une composante cyber[1082],

1080 TPF, BG.2018.15 du 29 août 2018, c. 4.2. La situation n'est pas aussi claire pour toutes les infractions de cybercriminalité.

1081 NICOLET/PEISSARD, p. 172 s.

1082 Parmi les plus importantes en pratique figurent la division cybercriminalité de la police cantonale zurichoise, la brigade Analyses et Traces Technologiques (BATT) de la police cantonale du canton de Vaud ou encore la brigade de criminalité informatique de la police judiciaire genevoise, TEICHMANN/GERBER, *La qualification pénale des attaques DDoS en droit suisse,* 2021, N 9.

mais une telle pratique n'est pas harmonisée et peut amener son lot de complications, surtout pour les cantons ne disposant pas des ressources suffisantes ou notamment en termes d'attribution de compétence.

(ii) Au niveau international

L'absence de frontières en informatique a pour conséquence que bon nombre d'infractions informatiques sont perpétrées depuis l'extérieur du pays ou revêtent du moins une composante extraterritoriale[1083]. Le principe de territorialité s'applique et a pour conséquence que les États doivent s'abstenir d'intervenir comme bon leur semble sur le territoire d'États étrangers. Ils doivent respecter la souveraineté étatique et les autorités d'un État ne peuvent pas simplement se dire compétente pour une infraction qui ne relève pas de leur compétence [1084]. 575

Une multitude de situations présentant un élément d'extranéité sont envisageables, que l'auteure d'une infraction agisse ou non depuis l'étranger. Ces éléments d'extranéité n'impliquent pas forcément la compétence de la Suisse pour la poursuite pénale, mais ils peuvent entraîner des mécanismes de coopération entre autorités de poursuite pénale ou entre autorités judiciaires. Ces mécanismes de coopération et d'entraide permettent de respecter la territorialité de chaque État, mais risquent en même temps d'entraîner des conflits de compétence extraterritoriale en droit pénal[1085]. 576

b. Tout est question de coopération

(i) La coopération en Suisse

Plusieurs instruments légaux existent afin de permettre la coopération en matière pénale au sein du pays[1086]. Le CPP comporte des dispositions permettant l'entraide entre ministères publics et tribunaux (art. 43 à 48 CPP). Entre les polices, fédérale et cantonales, il existe des ordonnances, concordats intercantonaux et règlements permettant leur collaboration, la mise en commun des forces et le partage d'informations, notamment par le biais de systèmes d'information[1087]. 577

Dans le cadre de la coopération policière, il existe des initiatives cherchant à optimiser la collaboration et l'échange d'informations entre les différentes intervenantes dans la lutte contre la cybercriminalité. Un bon exemple 578

1083 Voir par exemple NICOLET/PEISSARD, p. 170.

1084 OFJ, *Rapport sur le US CLOUD Act*, 2021, p. 16.

1085 OFJ, *Rapport sur le US CLOUD Act*, 2021, p. 16.

1086 Ce qui doit être anticipé dans la mesure du possible par le cadre légal, cf. GCSP, *Guide to Developing a National Cybersecurity Strategy*, 2021, p. 48.

1087 Voir à titre exemplatif la Convention TIP.

est celui de la Plateforme d'Information de la Criminalité Sérielle en Ligne (PICSEL), une plateforme utilisée par les cantons romands et le Tessin[1088]. L'utilisation de PICSEL repose sur le Concordat du 3 avril 2014 réglant la coopération en matière de police en Suisse romande, sur le Règlement d'application du concordat du 25 mars 2021 réglant la coopération en matière de police en Suisse romande concernant l'échange de données de police dans le domaine de la criminalité sérielle et sur la décision du 25 mars 2021 définissant les banques de données communes dans le domaine de la criminalité sérielle en application de l'article 14 du concordat réglant la coopération en matière de police en Suisse romande. En parallèle, la Convention intercantonale et interautorités du 14 juin 2019 relative à l'échange de données pour exploiter des systèmes de suivi et d'analyse de la situation dans le domaine de la délinquance sérielle sert de fondement pour un tel système auprès des polices de la Suisse du Nord-Ouest. À l'heure actuelle, ces plateformes ne sont pas utilisées dans toute la Suisse, ce qui a pour conséquence que l'échange d'informations permettant d'identifier de la criminalité sérielle en ligne sur l'entier du territoire helvétique n'est pas encore d'actualité. D'après la CSN de 2023, une base légale doit être adoptée pour permettre à PICSEL d'être utilisée sur tout le territoire helvétique[1089]. La collaboration entre la Confédération et entre les cantons doit encore être étendue[1090].

(ii) La coopération internationale

579 Les aspects internationaux de la cybercriminalité ont pour conséquence que la coopération internationale doit être efficace et la cybercriminalité dépasse souvent des territoires nationaux uniques. De nombreux sites malveillants sont hébergés à l'étranger, les auteures d'infractions passent souvent par des proxys ou des réseaux privés virtuels (*Virtual Private Networks,* VPN), et les données volées sont souvent partagées à large échelle entre délinquantes sur différentes plateformes[1091]. Les différentes autorités impliquées dans la lutte contre la cybercriminalité se doivent donc de coopérer sur le plan international, du fait des questions de souveraineté étatique et des aspects transfrontières de ce type de criminalité. Il en va principalement de l'assistance policière ainsi que de l'entraide judiciaire internationale en matière pénale.

1088 NICOLET/PEISSARD, p. 173 et 179 ; TEICHMANN/GERBER, *La qualification pénale des attaques DDoS en droit suisse,* 2021, N 9.

1089 CF, *CSN,* 2023, p. 30.

1090 CF, *CSN,* 2023, p. 29. Au sujet des entités collaboratives en Suisse dans ce contexte, cf. *supra* N 237 ss.

1091 TEICHMANN/GERBER, *Le phishing,* 2021, N 33 ; TEICHMANN/GERBER, *Les chevaux de Troie,* 2021, N 26.

Si l'on prend l'exemple de l'entraide judiciaire internationale, des instruments existent depuis longtemps, sur le plan international comme sur le plan national. Sur le plan international et de manière générale, la Suisse est liée par de nombreux traités bilatéraux et multilatéraux régissant la coopération en matière pénale avec des États étrangers. Ce réseau d'instruments de coopération se développe continuellement, avec de nouveaux traités d'assistance mutuelle avec de nouveaux États[1092]. La Convention européenne d'entraide judiciaire en matière pénale (CEEJ) et la Convention européenne d'extradition (CEExtr) sont les principaux instruments internationaux d'entraide judiciaire en matière pénale[1093]. En l'absence de traité, le droit interne, soit en particulier l'EIMP s'applique[1094]. 580

Plusieurs instruments ont été développés depuis des années afin d'augmenter l'efficacité de ces échanges. La Convention d'application du 19 juin 1990 de l'Accord de Schengen (CAAS) avait déjà permis l'entraide directe. Depuis, de nouveaux instruments, plus récents, ont été adoptés, comme la Convention sur la Cybercriminalité (CCC) et ses Protocoles additionnels[1095] ou encore, sur le plan européen, la directive *e-evidence*[1096]. La CCC est l'une des rares conventions internationales portant spécifiquement sur la lutte contre la cybercriminalité. Entrée en vigueur en Suisse il y a une dizaine d'années et ratifiée par certains États tels que les États-Unis d'Amérique (USA) ou Israël, cette convention détaille les mesures nationales matérielles et procédurales ainsi que la coopération internationale[1097]. D'une part, elle requiert des États parties 581

1092 ZIMMERMANN, N 191. Pour des exemples, voir OFJ, *Rapport d'activité 2021,* 2022, p. 22 ; OFJ, *Rapport d'activité 2022,* 2023, p. 19 ss.

1093 ZIMMERMANN, N 191. Le deuxième Protocole additionnel à la CEEJ compte des moyens d'investigation, non limités à la cybercriminalité mais permettant un bon complément à la CCC, voire une alternative pour les États non parties à la CCC, NICOLET/PEISSARD, p. 175.

1094 ZIMMERMANN, N 228.

1095 Dont son dernier protocole additionnel qui prévoit un renforcement de la coopération pour échanger des informations, notamment relatives à des noms de domaine et aux abonnées, cf. Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques (STCE nº 24), 12 mai 2022. La Suisse ne l'a ni signé ni ratifié à l'heure actuelle.

1096 À noter qu'il existe également d'autres Conventions multilatérales s'appliquant à la Suisse lorsqu'il en va de contextes ou complexes de faits spécifiques, typiquement si l'on est en présence de criminalité organisée transnationale, dans quels cas d'autres Conventions pourraient s'appliquer, comme la Convention de Palerme. Les Nations Unies sont par ailleurs en négociation au niveau international pour la conclusion d'une Convention sur la cybercriminalité, cf. UNITED NATIONS OFFICE ON DRUGS AND CRIME, *Future international convention on countering the use of information and communications technologies for criminal purposes*.

1097 Préambule CCC ; SALAMON, p. 263.

qu'ils répriment certains comportements. D'autre part, elle pose des exigences de procédure pénale afin de faciliter, entre autres, la coopération interétatique. Parmi ses dispositions principales, l'art. 29 CCC prévoit la conservation rapide des données informatiques stockées, permettant aux États parties de requérir immédiatement par le biais des autorités habilitées la conservation de données électroniques dans l'attente d'une demande d'entraide judiciaire. L'objectif poursuivi est donc d'éviter l'altération ou la suppression des données en question en raison de la demande d'entraide. L'art. 32 CCC permet l'accès transfrontière à des données stockées, soit accessibles au public soit moyennant le consentement légal et volontaire de la personne légalement autorisée à divulguer les données[1098]. L'art. 33 de la convention permet l'entraide dans la collecte en temps réel des données relatives au trafic[1099]. L'art. 18b EIMP a dû être adopté pour être en conformité avec les art. 30 et 33 CCC, prévoyant un renforcement de la coopération par la transmission à l'étranger de données relatives au trafic informatique[1100].

582 En parallèle à l'entraide judiciaire internationale en matière pénale, il existe également des instruments permettant la coopération inter polices. L'art. 355*a* CP confie à fedpol et au SRC la compétence de communiquer avec Europol, l'office européen de police qui permet de mener des actions coordonnées pour interrompre des activités délictuelles lorsque plus d'un État membre de l'UE est affecté par une forme grave de criminalité internationale[1101].

c. L'exploitabilité des moyens de preuve informatiques

583 La collecte de preuves informatiques ou numériques pose de nombreuses questions en pratique. Outre les questions techniques relatives à leur authenticité, leur traçabilité et leur conservation, les traces numériques peuvent être éphémères et les délinquantes utilisent souvent des procédés complexes susceptibles de rendre la collecte de ces traces difficile[1102]. De nombreuses infractions perpétrées aujourd'hui revêtent un caractère numérique ou informatique.

584 La cybercriminalité (en particulier les cyberattaques à l'encontre d'infrastructures critiques) a cela de particulier que l'outil servant à la réalisation

1098 NICOLET/PEISSARD, p. 174 s.

1099 ZIMMERMANN, N 156.

1100 OFJ, *Circulaire N 2 : Convention sur la cybercriminalité,* 2012, p. 1 s. ; TEICHMANN/GERBER, *Le phishing,* 2021, N 33 ; TEICHMANN/GERBER, *Les chevaux de Troie,* 2021, N 27.

1101 CR CP II-TIRELLI, art. 355*a* N 2. Voir par exemple l'action ayant permis à Europol de prendre le contrôle des infrastructures Emotet en 2021, TEICHMANN/GERBER, *Les chevaux de Troie,* 2021, N 25.

1102 NICOLET/PEISSARD, p. 167. Citant les questions d'authenticité, de traçabilité et de conservation, SALAMON, p. 135.

de l'infraction est en principe un système informatique, de même que sa cible, du moins partiellement. Partant, la majorité des moyens de preuve auxquels s'intéressent les autorités de poursuite pénale sont numériques. Les cybercriminelles utilisent régulièrement des outils techniques, comme des VPN ou des proxys, leur permettant de noyer les traces et d'empêcher le travail des autorités de poursuite pénale. Elles peuvent, typiquement par le biais de VPN, faire transiter leur connexion par des adresses IP hébergées sur le territoire d'États ne disposant pas des mêmes réglementations qu'en Suisse. Ces États constituent parfois des paradis digitaux où il est excessivement difficile voire impossible de recevoir une réponse affirmative à une demande d'entraide. En parallèle, des moteurs de recherche comme Tor permettent aux délinquantes de naviguer sur le *dark web* et rendent, grâce aux procédés d'anonymisation du moteur (et de la même façon que les VPN), l'accès à d'éventuelles traces numériques particulièrement difficile.

585 Les recherches sont souvent complexes et coûteuses dans les cas de criminalité informatique[1103]. Par ailleurs, des questions relatives à l'exploitabilité des moyens de preuve collectés se posent. Pour pouvoir être exploités dans une procédure pénale ouverte en Suisse, les moyens de preuve doivent être collectés conformément à l'art. 140 CPP par les autorités de poursuite pénale. Le cadre légal doit prévoir les questions procédurales relatives à la collecte des preuves électroniques[1104].

586 La Loi sur la surveillance de la correspondance par poste et télécommunication (LSCPT) et ses ordonnances revêtent un intérêt particulier dans la mesure où les nouvelles technologies facilitent la réalisation d'infractions. Il est nécessaire de disposer des moyens permettant d'éclaircir les infractions commises au moyen de ces technologies[1105]. Lorsque des personnes sont fortement soupçonnées d'avoir commis des infractions graves, la loi et ses ordonnances permettent aux autorités de poursuite pénale d'acquérir des informations auprès des fournisseuses de services de télécommunication. Cette acquisition d'information se fait par le biais du Service Surveillance de la correspondance par poste et télécommunication (Service SCPT)[1106]. Il est interdit en Suisse (sur la base de l'art. 13 Cst. et de l'art. 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, CEDH) de

1103 NICOLET/PEISSARD, p. 167.

1104 GCSP, *Guide to Developing a National Cybersecurity Strategy*, 2021, p. 48. Pour des aspects plus pratiques, voir notamment JAQUET-CHIFFELLE, p. 199 s. ; MÉTILLE, *Internet et droit,* p. 146 ss ; TEICHMANN/GERBER, *La qualification pénale des attaques DDoS en droit suisse,* 2021, N 11 ss.

1105 FF 2013 2379, p. 2381.

1106 BONDALLAZ, N 1783.

procéder à de la surveillance systématique des communications donc la loi pose le cadre dans lequel une telle surveillance est autorisée[1107].

587 La loi permet à certaines autorités d'obtenir des informations durant une surveillance, notamment dans le cadre d'une procédure pénale ou d'entraide (art. 1 al. 1 litt. a et b LSCPT). Les fournisseuses de services de télécommunication sont obligées de transmettre les informations des art. 21 s. LSCPT au Service SCPT, qui les met à disposition des autorités requérantes (art. 15 LSCPT) par le biais de son système d'information (art. 6 à 14*a* LSCPT)[1108].

3. D'autres mesures de lutte contre la cybercriminalité

a. L'Ordonnance sur les domaines Internet

588 L'Ordonnance sur les domaines Internet (ODI) offre la possibilité aux autorités compétentes sur le plan pénal d'intervenir lorsque des noms de domaine sont utilisés frauduleusement. L'ODI a une portée ne se limitant pas aux procédures pénales et a pour objectif de garantir en Suisse une offre de noms de domaine Internet « suffisante, avantageuse, de qualité et répondant aux besoins » (art. 1 al. 1 ODI).

589 Certaines délinquantes exploitant des noms de domaine Internet pour commettre des cyberattaques, il a été nécessaire de prévoir des possibilités de blocage des noms de domaine utilisés illicitement. L'art. 15 ODI permet au registre de bloquer un nom de domaine pour 5 jours lorsqu'il soupçonne une utilisation de celui-là pour accéder par des méthodes illicites à des données critiques, pour diffuser ou exploiter des logiciels malveillants ou pour soutenir l'une de ces activités (art. 15 al. 1 ODI)[1109]. Le blocage peut être prolongé durant 30 jours maximum si des raisons fondées font supposer que la titulaire recourt à de fausses données d'identification ou usurpe l'identité d'une personne tierce et si le blocage permet la prévention urgente de la survenance d'un préjudice imminent et difficilement réparable (art. 15 al. 2 ODI). Pour des blocages plus longs, l'intervention de l'OFCOM est nécessaire (art. 15 ODI). Les services de lutte contre la cybercriminalité reconnus par l'OFCOM peuvent également exiger un blocage de 30 jours, mais cette fois si les conditions de l'art. 15 al. 1 sont

1107 Dans le même ordre d'idées, STAIGER, p. 407. La LSCPT permet aux autorités de poursuite pénale d'obtenir des informations par le biais d'une surveillance, et des lois distinctes habilitent d'autres autorités à procéder à la surveillance malgré l'interdiction de principe de ces dernières, à l'instar de la LRens pour le SRC, cf. *infra* N 593 s.

1108 BONDALLAZ, N 1808 ss. L'OSCPT développe la procédure mise en place par la loi. Pour plus d'informations sur cette surveillance, cf. BONDALLAZ, N 1789 ss. Dans le cadre des mesures de surveillance impliquant le Service SCPT, ce dernier peut avoir accès et transmettre aux autorités de poursuite pénale des renseignements simples ou complexes, cf. SERVICE SCPT, p. 29.

1109 BENHAMOU, p. 14.

réunies (art. 15 al. 3 ODI). Parmi ces services figurent, outre le NCSC, les polices cantonales et fédérale[1110]. D'autres mesures existent, à l'instar de l'attribution d'un nom de domaine qui prête son concours à la lutte contre la cybercriminalité et la redirection à des fins d'analyse du trafic destiné ou transitant par un nom de domaine pouvant faire l'objet d'une demande d'attribution ou d'une utilisation à une fin ou d'une manière illicite (art. 15*d* ODI).

b. Des actes cantonaux et intercantonaux

Avant l'entrée en vigueur du CPP, les cantons étaient compétents pour légiférer sur la procédure pénale. Ils ont aujourd'hui des lois d'application du CPP ainsi que des lois précisant les compétences cantonales et les différentes procédures à l'échelle du canton. Les cantons demeurent compétents pour la poursuite pénale et le jugement d'une majorité d'infractions du droit pénal suisse. 590

Certaines lois cantonales revêtent un intérêt pour la poursuite pénale de la cybercriminalité. Il en va de tel pour les lois de police, qui fournissent à ces autorités des prérogatives en dehors d'une procédure pénale et donc hors cadre du CPP. Ces lois permettent aux autorités de police de procéder à des recherches préventives (voir par exemple, dans le canton de Vaud, l'art. 21a de la loi sur la police cantonale, Lpol-VD). La police cantonale peut, avant l'ouverture d'une procédure pénale et après autorisation par le Tribunal des mesures de contrainte, effectuer des recherches secrètes si elle suspecte qu'une infraction suffisamment grave a été commise[1111]. 591

C. La cyberdéfense

1. La cyberdéfense dans la protection des infrastructures critiques

a. La base légale pour le Service de renseignement de la Confédération

La cyberdéfense, troisième aspect de la protection contre les cyberrisques, est également concernée par les questions de cybersécurité des infrastructures critiques, surtout en lien avec la gestion de cyberincidents. Certaines autorités rattachées au Département fédéral de la défense, de la protection de la population et des sports (DDPS) détiennent des compétences de soutien subsidiaire lorsque les infrastructures sont visées par des cyberattaques. 592

L'art. 26 al. 1 litt. d de la Loi fédérale sur le renseignement (LRens) prévoit par exemple la possibilité pour le SRC d'infiltrer un système informatique en 593

1110 OFCOM, *Lutte contre la cybercriminalité*, 24 février 2023 (consulté le 20.3.2024).

1111 Les cantons peuvent selon le TF prévoir des mesures de surveillance secrètes si des conditions similaires à celles du CPP sont mises en place, et si l'intérêt public et la proportionnalité sont respectées, cf. notamment ATF 140 I 381, c. 4 ; TF, 1C_518/2013 du 1er octobre 2014, c. 3 (non publié à l'ATF 140 I 381).

Suisse. Son intervention doit respecter le principe de subsidiarité. Il ne doit intervenir que si une procédure pénale n'a pas abouti ou si elle ne permet pas de lutter contre une attaque mettant en péril la sûreté intérieure ou extérieure de la Suisse[1112]. Elle demeure secrète pour la personne concernée jusqu'à la fin de l'opération. La personne concernée doit ensuite être informée conformément à l'art. 33 LRens[1113]. Cette mesure permet au SRC de perturber, empêcher ou ralentir l'accès à des informations, ce qui n'est possible qu'à condition que les réseaux informatiques soient utilisés dans des attaques ayant pour cibles des infrastructures critiques (art. 26 al. 1 litt. d ch. 2 LRens)[1114]. Pour ce faire, le SRC nécessite tout d'abord, sur le plan formel, une double autorisation[1115]. Sur le fond, il faut être en présence d'une menace concrète pour la sûreté intérieure ou extérieure de la Suisse au sens de l'art. 19 al. 2 litt. a à d LRens[1116]. En outre, il faut réunir deux conditions supplémentaires pour respecter le principe de proportionnalité. Premièrement, la menace doit atteindre un seuil de gravité justifiant la mesure. Deuxièmement, il faut que la recherche d'informations non soumise à autorisation soit restée vaine et qu'à défaut de cette mesure toute autre action requière des efforts disproportionnés[1117].

594 Le SRC peut également s'introduire, sur la base de l'art. 37 LRens, dans un réseau informatique situé à l'étranger pour le perturber, en empêcher ou ralentir l'accès. À l'inverse de l'infiltration dans un réseau situé en Suisse, cette opération ne requiert pas d'autorisation judiciaire. Néanmoins, la décision doit émaner du CF pour des raisons de politique extérieure (art. 37 al. 2 LRens)[1118].

b. Les bases légales légitimant l'intervention de l'armée

595 L'armée compte parmi ses missions celle de protéger les infrastructures critiques[1119]. L'armée peut être engagée pour son service de promotion de la paix, son service d'appui et son service actif (art. 65 LAAM). Dans le cadre du service d'appui qu'elle fournit, l'armée apporte entre autres un soutien subsidiaire aux autorités civiles[1120]. Ce soutien vient en appui aux autorités civiles notamment lorsque des autorités civiles doivent faire face à des catastrophes ou à des

1112 FF 2014 2029, p. 2089.

1113 MÉTILLE, *Internet et droit*, 2017, p. 151.

1114 FF 2014 2029, p. 2089.

1115 L'autorisation doit émaner du TAF et du chef du DDPS, art. 27 ss LRens, plus précisément art. 27 al. 2 LRens et 29 s. LRens ; FF 2014 2090 ; MÉTILLE, *Internet et droit*, 2017, p. 151.

1116 FF 2014 2029, p. 2090.

1117 FF 2014 2029, p. 2091.

1118 FF 2014 2029, p. 2100 ; MÉTILLE, *Internet et droit*, 2017, p. 151.

1119 DDPS, *Stratégie Cyber VBS*, 2021, p. 31 ; FF 2014 6693, p. 6703.

1120 DDPS, *Stratégie Cyber VBS*, 2021, p. 22.

surcharges extrêmes dépassant leurs moyens (art. 67 al. 1 litt. d LAAM). Ce soutien est également apporté lorsque la protection de personnes et biens particulièrement dignes de protection, en particulier des infrastructures critiques, doit être assurée (art. 67 al. 1 litt. b LAAM). L'armée apporte donc un soutien subsidiaire à l'intervention de l'OFCS et de la police lorsque des infrastructures critiques constituent la cible d'une cyberattaque en vertu de l'art. 67 al. 1 litt. b LAAM. L'appui fourni par l'armée peut prendre la forme d'une mise à disposition de matériel et de biens d'approvisionnement, ainsi que d'un envoi de troupes ; en cas de nécessité, elle peut également faire appel à du personnel de la Confédération ou à du personnel externe à l'administration fédérale (art. 67 al. 3 LAAM).

596 En parallèle, l'armée est compétente avec le SRC pour soutenir une opération militaire. L'armée est responsable de la cyberdéfense militaire et des actions dans le cyberespace dans le cadre d'opérations militaires[1121].

2. La spécificité du domaine de la cyberdéfense

597 L'armée et l'administration militaire font partie des infrastructures considérées comme critiques en Suisse[1122]. Rattachées au DDPS, elles doivent, en parallèle de leur soutien à différentes autorités et organisations tierces, assurer leur cyberdéfense[1123]. L'Ordonnance sur la cyberdéfense militaire (OCMil) sert de base légale pour doter les autorités de compétences visant à assurer l'autoprotection et la cyberdéfense des systèmes utilisés par l'armée et l'administration militaire. Elle permet notamment (mais sans s'y limiter, ce qui pourrait également englober certaines mesures de cybersécurité) les actions dans le cyberespace visant à identifier les attaques et y acquérir des informations, protéger les ressources de l'armée ou encore perturber, entraver ou ralentir les moyens ou capacités d'un adversaire (art. 1 al. 2 OCMil).

D. Une synthèse

598 Le cadre légal pour la lutte contre la cybercriminalité se compose des infractions reconnues en droit suisse qui, lorsqu'elles sont réalisées, entraînent l'ouverture de procédures pénales. Les autorités de poursuite pénale et les autorités judiciaires sont actives dans la poursuite et la condamnation des personnes auteures d'infractions. La cybercriminalité soulève des questions

1121 DDPS, *Stratégie Cyber VBS*, 2021, p. 22 et 31. Les questions de ses compétences pour la cyberdéfense militaire sortant du cadre de la présente étude ne sont pas étudiées.

1122 FF 2018 491, p. 500.

1123 FF 2014 6693, p. 6703.

pratiques importantes en termes de compétences. Les compétences cantonales et fédérales s'entremêlent, des questions de for se posent sur le plan national comme sur le plan international. Une collaboration entre les autorités compétentes est essentielle et est renforcée par différents leviers d'action, à l'instar de l'exploitation de plateformes d'échange d'informations ou l'adoption de conventions permettant la rapidité des procédures en garantissant le respect de la souveraineté territoriale d'autres États. Outre ces questions de compétences et de collaboration, la cybercriminalité soulève des questions particulières toujours plus appréhendées par la loi, à l'instar des questions de preuve. Des développements juridiques comme pratiques doivent encore avoir lieu, dans la mesure où le droit n'appréhende aujourd'hui pas toujours correctement la cybercriminalité, comme on peut le voir avec l'échange d'informations de police, ou avec l'absence d'infractions d'hameçonnage ou de recel de données[1124].

599 Dans le domaine de la cyberdéfense, le cadre légal permet d'attribuer des compétences aux autorités principales du DDPS, qui sont le SRC et l'armée. Le SRC peut typiquement infiltrer des systèmes informatiques lorsque la sûreté intérieure ou extérieure de la Suisse est en péril. Tel peut être le cas lorsque des infrastructures critiques font l'objet de cyberattaques. L'armée est responsable de la cyberdéfense militaire, mais elle dispose également de compétences pour soutenir de façon subsidiaire les autorités civiles et les infrastructures critiques, notamment dans le cadre de cyberattaques. Ces autorités font partie de la défense. À ce titre, elles prennent des mesures de défense active et occupent en particulier un rôle important dans des contextes militaires, qui impliquent l'application de bases légales particulières et qui diffèrent des situations de paix.

600 L'examen des trois domaines juridiques composant la protection de la Suisse contre les cybermenaces permet de mieux comprendre leur complémentarité. Les trois domaines permettent d'appréhender différents aspects de la protection du pays contre les cybermenaces. Le cadre légal servant à la lutte contre la cybercriminalité cherche d'une part à créer un effet dissuasif général et à poursuivre et condamner les personnes à l'origine de cyberattaques. D'autre part, la législation sur la cybercriminalité sert de fondement pour les compétences des autorités actives dans la poursuite pénale des personnes

1124 Le manque de bases légales a été soulevé à plusieurs reprises, voir notamment CF, *Poursuites pénales en matière de cybercriminalité*, 2024, p. 22 et 36 ss. La CSN de 2023 prévoit qu'il faut vérifier les bases légales, notamment en termes de collaboration et, au besoin, en créer des nouvelles, CF, *CSN*, 2023, p. 29. Par exemple, les bases légales pour PICSEL devraient à l'avenir permettre à tous les cantons helvétiques de participer à la plateforme.

réalisant des infractions dans le cyberespace. Les bases légales pour la cyberdéfense attribuent des compétences aux autorités actives dans la défense du pays dans des contextes de paix mais surtout dans des contextes de guerres ou de conflits armés. Cette analyse met en lumière la nécessité de réglementer la cybersécurité pour un autre objectif nécessaire qui est la responsabilisation des personnes susceptibles de faire l'objet de cyberattaques. Il faut que les autorités et organisations disposent des incitations pour prévenir, détecter et réagir de la façon la plus appropriée aux cybermenaces.

III. Une conclusion au chapitre 4

La réglementation de la cybersécurité poursuit l'objectif d'inciter différents groupes cibles à améliorer leurs capacités de cybersécurité ou leur cyberrésilience face à la multitude de cybermenaces. Le cadre réglementaire pour la cybersécurité en Suisse se développe et l'objet de la présente étude porte plus particulièrement sur la cybersécurité des infrastructures critiques (I.A), en s'inspirant des différents standards internationaux acceptés par de nombreuses organisations en pratique (I.B). 601

Les infrastructures critiques sont des organisations actives dans les sous-secteurs critiques reconnus en Suisse. La réglementation de leur cybersécurité se développe de façon très sectorielle (I.C). Les organisations actives dans certains sous-secteurs critiques sont soumises à des exigences légales de cybersécurité. Il en va de la sorte en particulier pour les autorités et organisations de la Confédération ou pour les organisations actives dans l'approvisionnement en électricité. Certains sous-secteurs critiques comptent sur des normes de droit souple prévoyant certaines mesures de cybersécurité, à l'instar des secteurs de l'approvisionnement économique du pays, des établissements hospitaliers ou de certains cantons. Un flou juridique et un manque de coordination entre les instruments des autorités et du domaine privé est en effet à déplorer[1125]. D'autres sous-secteurs critiques ne disposent de quasiment aucune réglementation de cybersécurité. C'est en particulier le cas des services informatiques. 602

Des instruments réglementaires sont peu à peu adoptés en parallèle des réglementations sectorielles existantes (I.D). L'introduction d'une obligation de signaler les cyberattaques visant les infrastructures critiques est un pas particulièrement important dans ce contexte. Elle constitue la première obligation transversale et applicable à autant d'infrastructures critiques dans le 603

1125 OFCS, *Stratégie de l'OFCS*, 2023, p. 3.

domaine. D'autres instruments réglementaires contraignants et non contraignants existent et réglementent des aspects étroitement liés à la cybersécurité, à l'instar des lois de protection des données personnelles ou de la Norme minimale pour améliorer la résilience informatique de l'OFAE.

604 Cet état des lieux permet de voir les avancées qui se produisent en Suisse pour exploiter au mieux le cadre réglementaire existant pour améliorer la cybersécurité des infrastructures critiques. En revanche, des lacunes sont encore à déplorer, de la même manière qu'un manque de clarté et d'harmonisation.

605 Le domaine de la cybersécurité est connexe à ceux de la poursuite pénale de la cybercriminalité et à la cyberdéfense. La réglementation des trois domaines ne poursuit pas les mêmes objectifs. Les instruments réglementant la cybersécurité visent les mesures que peuvent mettre en place les organisations pour se protéger efficacement des cybermenaces. La lutte contre la cybercriminalité implique une législation interdisant des comportements et permettant les ressources aux autorités compétentes pour poursuivre et condamner les personnes délinquantes. Le domaine de la cyberdéfense vise la protection de la Suisse sur un plan militaire principalement. Les trois domaines de la protection contre les cybermenaces sont complémentaires.

606 Dans le domaine de la cybercriminalité, les infractions reconnues en droit pénal suisse couvrent aujourd'hui de nombreux comportements délictuels. Cependant, la répression permise par le droit de fond soulève quelques questions, par exemple liées au fait que certains comportements ne sont pas correctement appréhendés par le cadre légal, ou que certaines infractions sont poursuivies uniquement sur plainte. Sur le plan procédural et d'un point de vue pratique, des barrières existent encore. Certaines sont justifiées par le respect de garanties fondamentales et de différents droits en jeu, d'autres sont plus complexes et ont trait à des questions de coopération voire de culture. Certains accords et renforcements doivent encore être trouvés, d'un point de vue légal comme d'un point de vue pratique (II.A).

607 Le cadre légal pour la cyberdéfense sert principalement à attribuer les compétences aux autorités compétentes. Ces autorités peuvent apporter un soutien subsidiaire mais en complément à celui des autorités civiles comme l'OFCS. Elles peuvent prendre des mesures plus actives dans le soutien qu'elles apportent aux infrastructures critiques mais en dernier recours. Leurs compétences principales ayant trait à la cyberdéfense militaire, leur intervention auprès des infrastructures critiques et des autorités civiles est subsidiaire (II.B).

608 Le cadre légal pour la cybersécurité en Suisse tend peu à peu et à raison à responsabiliser les infrastructures critiques. Le cadre légal pour la cybercriminalité et pour la cyberdéfense apporte des mécanismes complémentaires

à ceux que la réglementation de la cybersécurité permet. Les trois domaines juridiques se complètent, mais la législation pour la lutte contre la cybercriminalité et pour la cyberdéfense ne dispense pas de l'adoption d'une réglementation de cybersécurité.

609 Les infrastructures critiques sont les premières responsables de leur cybersécurité. Elles font également appel à des spécialistes en cybersécurité pour les aider dans la gestion des cyberincidents auxquels elles sont confrontées. Ces spécialistes sont des prestataires de gestion de cyberincidents. Il est important d'analyser si leur activité est encadrée par la loi afin de comprendre si le cadre légal appréhende la cybersécurité de façon globale en tenant compte de toutes les intervenantes. L'examen de ce cadre légal doit porter sur tous les types de prestataires de gestion de cyberincidents, à savoir les prestataires privées externes, mais aussi les fournisseuses de prestations internes à des autorités ou à des organisations ainsi qu'à l'équipe d'intervention nationale de GovCERT intégrée à l'OFCS.

Chapitre 5 : le cadre légal pour l'activité des prestataires de gestion de cyberincidents

Préambule au chapitre 5

610 Le cadre réglementaire permettant l'introduction d'exigences minimales de cybersécurité applicables aux infrastructures critiques se développe en Suisse. La cybersécurité a comme corollaire la gestion de cyberincidents ; les cyberincidents doivent être empêchés dans la mesure du possible et il est nécessaire d'y réagir au mieux pour garantir la cybersécurité.

611 Les personnes compétentes pour prévenir, détecter les cyberincidents et y réagir disposent des compétences permettant d'assurer la cybersécurité, auprès des infrastructures critiques comme auprès d'autres organisations. Leur structure, leur nom et leurs compétences varient fortement en pratique, raison pour laquelle la présente étude utilise le terme générique de prestataires de gestion de cyberincidents.

612 L'intervention de prestataires de gestion de cyberincidents permet un rétablissement de la cybersécurité au sein d'une organisation affectée par un cyberincident (ou par une cyberattaque). Ces personnes physiques et morales détiennent aussi régulièrement des compétences de prévention et de détection. Elles se trouvent souvent au centre des échanges et des diverses

communications avec les autorités et les autres personnes concernées par des cyberincidents. Les États, comme les infrastructures critiques et les autres organisations, nécessitent aujourd'hui de bénéficier des compétences permettant d'assurer une prévention, une détection ainsi qu'une réaction aux cyberincidents. C'est dans ce cadre qu'interviennent donc les prestataires de gestion de cyberincidents[1126].

613 Auparavant, la gestion de cyberincidents était majoritairement dispersée entre plusieurs services au sein d'une organisation ou ne faisait pas l'objet d'une attention particulière. L'augmentation des cyberattaques et des cyberincidents ainsi que les nouvelles obligations légales et la pression médiatique ou sociale ont contribué à un renforcement des pratiques, processus et compétences au sein d'une multitude d'organisations. Elles sont toujours plus nombreuses à mettre en place des services compétents pour les tâches de cybersécurité et, plus précisément, de gestion opérationnelle des cyberincidents[1127]. L'utilité d'une équipe d'intervention en cas d'incident lié à la sécurité informatique (*Computer Security Incident Response Team,* CSIRT) par exemple, centre de compétence reconnu en pratique à la fin du XX^e^ siècle, ou d'une autre prestataire de gestion de cyberincidents, est maintenant établie[1128]. Son existence se fonde sur des pratiques établies internationalement et est intimement liée à la question de la réponse aux incidents.

614 Les prestataires de gestion de cyberincidents, qui font partie du sous-secteur critique des services informatiques (I.A et B), ne sont pas réglementées dans leur ensemble, bien que de nouvelles dispositions légales présentent un intérêt particulier pour leur activité. En revanche, des bases légales générales sont susceptibles de s'appliquer à leur activité en fonction du contrat les liant à leur clientèle. En outre, certaines de leurs clientes sont soumises à des exigences de cybersécurité susceptibles de se répercuter sur l'activité des prestataires de gestion de cyberincidents (I.C). Finalement, certaines lois instituant des responsabilités indépendantes des considérations susmentionnées peuvent avoir un impact sur leur pratique (I.D).

615 Bien que la pratique générale des prestataires de gestion de cyberincidents soit très variée, les équipes étatiques de gestion de cyberincidents poursuivent des missions similaires et détiennent des compétences comparables. En Suisse, l'équipe d'intervention en cas d'urgence informatique (GovCERT),

1126 Pour un rappel sur ces intervenantes, cf. *supra* N 272 ss.

1127 KILLCRECE et al., *State of Practice of CSIRT,* 2003, p. 1.

1128 NCSC, *Rapport semestriel 2022/1,* p. 7 ; DSOUZA, p. 217. Sur l'histoire des CERT, voir KILLCRECE et al., *State of Practice of CSIRT,* 2003, p. 17 ; MORGUS et al., *CSIRT Basics for Policy-Makers,* 2015, p. 7 ss.

exploitée par l'OFCS, est la prestataire de gestion de cyberincidents de la Confédération[1129]. La législation sur laquelle se fonde son activité est en plein mouvement et la cybersécurité au sein de la Confédération est en pleine réorganisation. Il est important d'analyser les conséquences qui peuvent en découler sur les compétences de l'OFCS et de son équipe technique (II.A). Les compétences de l'office fédéral dépendent de ce que la loi prévoit, dans la mesure où son activité est soumise au principe de la légalité (II.B et C). La législation doit revêtir une densité normative supérieure à celle des bases légales applicables aux autres prestataires de gestion de cyberincidents.

Les régimes légaux applicables à l'activité de l'OFCS et des autres prestataires de gestion de cyberincidents sont différents. En revanche, certaines dispositions légales leur sont communes. Il en va typiquement de la sorte pour les questions ayant trait à la responsabilité pénale des membres des différentes organisations fournissant ce type de prestations (III.A et B). 616

I. Les prestataires de gestion de cyberincidents

A. La double casquette des prestataires de gestion de cyberincidents

Les organisations qui fournissent des prestations de gestion de cyberincidents sont des infrastructures critiques. Elles font partie des fournisseuses de services numériques de sécurité qui sont des fournisseuses de services informatiques entrant dans le secteur critique de l'information et de la communication. Certains aspects de leur activité connexes à la cybersécurité sont réglementés[1130]. 617

En parallèle, ces personnes ou sociétés sont des prestataires fabriquant des produits ou fournissant des prestations de services. Leurs prestations peuvent être offertes à une organisation à laquelle elles sont intégrées ou à une clientèle externe. Lorsqu'elles sont intégrées à une organisation, c'est l'organisation qui dispose d'une personnalité juridique. Lorsqu'elles en sont externes, c'est l'entreprise qui fournit les services de gestion de cyberincidents qui a la personnalité juridique. Dans le cadre de la relation entre les expertes fournissant des prestations de cyberincidents et leur organisation ou leur clientèle externes, ces prestataires peuvent être soumises à d'autres obligations. Une diversité de bases légales est applicable à leur activité et à leurs relations, en fonction de leur structure ou de leur clientèle. Il convient de rappeler que les prestataires externes de gestion de cyberincidents peuvent 618

1129 Cf. *infra* N 212 ss et 710 s.

1130 Cf. *supra* N 470 ss.

être tant des personnes physiques que des personnes morales, comme nous allons le voir plus concrètement[1131].

B. La prestataire de gestion de cyberincidents comme infrastructure critique

1. Les bases légales principales

619 Les prestataires de gestion de cyberincidents sont des infrastructures critiques, plus spécifiquement en faisant partie des fournisseuses de services numériques de sécurité, elles-mêmes comprises dans le sous-secteur critique des services informatiques. La LSI, loi principale pour la cybersécurité en Suisse, va leur imposer une première obligation de cybersécurité. Les personnes morales ou physiques qui fournissent des prestations de gestion de cyberincidents sont soumises à l'obligation de signaler les cyberattaques en vertu des art. 74*a* ss LSI2 (plus particulièrement en vertu de l'art. 74*b* al. 1 litt. t LSI2), comme bon nombre d'autres infrastructures critiques[1132]. Le message relatif à la révision de la loi se limite à mentionner comme services numériques de sécurité les solutions de chiffrement et les moyens informatiques permettant la protection contre les cyberattaques, à l'instar de programmes antivirus ou de pare-feux[1133]. Nous avons compris que la mise à disposition de tels produits peut faire partie des prestations fournies par des prestataires de gestion de cyberincidents à leur clientèle[1134]. L'on peut en déduire que la fabrication de telles solutions est également comprise dans ces services de sécurité. Au-delà de ces exemples de compétences préventives, l'on est forcée d'admettre que la gestion de cyberincidents fait partie des services numériques de sécurité. La liste d'exemples du message de la LSI révisée n'est par ailleurs pas exhaustive.

620 Outre l'obligation de signaler les cyberattaques, comme nous l'avons vu[1135], les exigences légales leur étant applicables sont en grande partie limitées aux aspects relatifs à la LPD ainsi qu'à la LSPro et aux ordonnances la complétant. Partant, quelques considérations relatives à la sécurité pour protéger l'intégrité physique, la santé et la personnalité d'utilisatrices ou de personnes concernées existent. Toutefois, la cybersécurité n'est en grande partie pas appréhendée par le cadre légal en vigueur.

1131 Cf. *infra* N 629.

1132 Cf. *supra* N 521 ss.

1133 FF 2023 84, p. 41.

1134 Cf. *supra* N 294.

1135 Cf. *supra* N 482 ss.

2. Les spécificités pour les fabricantes

Il n'existe à notre connaissance pas d'autres obligations de cybersécurité appli- 621
cables aux prestataires de gestion de cyberincidents lorsqu'elles agissent en tant que services numériques de sécurité, sous réserve qu'elles soient également considérées comme fabricantes de matériels ou de logiciels informatiques. Certaines prestataires de gestion de cyberincidents sont considérées comme des fabricantes de matériels ou de logiciels informatiques pour une partie de leur activité. Tel est le cas lorsqu'elles développent et fournissent à leur clientèle des logiciels ou du matériel informatique. Deux conséquences légales peuvent en découler.

D'une part, elles sont susceptibles d'être soumises à l'obligation de signaler 622
les cyberattaques en vertu non pas de l'art. 74*b* al. 1 litt. t LSI2, mais de l'art. 74*b* al. 1 litt. u LSI2. Ces organisations doivent signaler la cyberattaque qui vise un matériel informatique ou un logiciel qu'elles ont fabriqué, à condition que le produit en question soit utilisé par des infrastructures critiques et, alternativement, que le produit dispose d'un accès de télémaintenance ou qu'il soit utilisé aux fins de garantie de la sécurité publique ou de commande et de surveillance de systèmes et de processus techniques (art. 74*b* al. 1 litt. u ch. 1 et 2 LSI2). Cette disposition vise les prestataires de gestion de cyberincidents qui fabriquent et mettent à disposition de leur clientèle critique des moyens informatiques permettant la communication en cas d'intervention urgente ou des systèmes pour la télémaintenance ou pour le dépannage[1136].

D'autre part et alors que l'obligation de signaler les cyberattaques concerne 623
les situations dans lesquelles la prestataire de gestion de cyberincidents est elle-même la cible d'une attaque (et non sa cliente), une autre conséquence légale peut découler de la survenance d'une cybermenace sur un matériel informatique ou sur un logiciel que la prestataire fabrique et met à disposition de sa clientèle. La prestataire de gestion de cyberincidents peut annoncer des cybermenaces, des cyberincidents ou des vulnérabilités à l'OFCS (art. 73*b* LSI2). Ces prestataires peuvent, au même titre que toute personne, annoncer ces événements. En revanche, du fait des prestations qu'elles offrent, elles sont plus à même de détecter des menaces, incidents ou vulnérabilités. Elles sont donc particulièrement aptes à être à l'origine d'un nombre important de signalements.

Plusieurs conséquences pour les fabricantes peuvent découler de l'infor- 624
mation faite à l'OFCS sur une cybermenace, un cyberincident ou une vulnérabilité. Lorsqu'une vulnérabilité est annoncée à l'OFCS, ce dernier en informe immédiatement la fabricante du matériel informatique ou du logiciel en lui

1136 FF 2023 84, p. 41 s.

fixant un délai approprié pour l'éliminer (art. 73*b* al. 3 LSI2). La décision de l'OFCS est assortie de la menace d'une sanction en vertu de l'art. 44 al. 1 litt. fbis de la Loi fédérale sur les marchés publics (nLMP). Selon l'art. 44 al. 1 litt. f*bis* nLMP, l'adjudicatrice peut exclure une soumissionnaire d'une procédure d'adjudication, la radier d'une liste ou révoquer une adjudication si cette dernière n'élimine pas une vulnérabilité dans le délai fixé par l'OFCS. Il n'existe pas d'obligation systématique d'éliminer les vulnérabilités et le droit actuel devrait déjà exclure les produits proposés lorsqu'ils comportent des vulnérabilités non éliminées[1137]. Ces sanctions se limitent aux situations dans lesquelles la prestataire de gestion de cyberincidents agit dans le cadre des marchés publics au sens de l'art. 8 LMP[1138]. L'OFCS annonce également à la fabricante que la vulnérabilité sera publiée si elle ne la corrige pas. Le cas échéant, des informations sur des vulnérabilités avec des indications sur le matériel informatique ou le logiciel concerné peuvent être publiées par l'OFCS, à condition soit que la fabricante y consente ou qu'elle n'ait pas remédié à la vulnérabilité dans le délai de l'art. 73*b* al. 3 LSI2 (art. 73*c* al. 2 LSI2)[1139].

C. Les prestataires de gestion de cyberincidents et les organisations privées

1. Une diversité de possibilité

625 Toujours plus d'organisations se dotent de prestataires de gestion de cyberincidents, bien qu'un nombre important d'infrastructures critiques notamment ne disposent pas encore de telles prestataires[1140]. Leur pratique est reconnue comme toujours plus centrale pour la protection de la Suisse contre les cybermenaces. Contrairement aux autorités nécessitant en Suisse une base légale pour agir, les entités privées ne sont pas soumises au principe de la légalité[1141]. Partant, contrairement à l'OFCS ou aux fournisseuses de prestations de gestion de cyberincidents intégrées à des autorités, les activités concrètes menées par une prestataire privée de gestion de cyberincidents n'ont pas à se fonder sur une base légale particulière. Cette dernière dispose d'une plus grande liberté d'action. Son activité étant souvent régie par le droit privé, l'autonomie des parties s'applique donc entre celle-ci et sa cliente[1142].

1137 FF 2023 84, p. 54.

1138 Sur la notion de marché public, cf. FF 2017 1695, p. 1740 s.

1139 FF 2023 84, p. 28.

1140 CF, *CSN*, 2023, p. 24.

1141 Art. 5 al. 1 Cst. ; CR Cst.-DUBEY, art. 5 N 30, 37 ; SURY, *Informatikrecht*, 2013, p. 5.

1142 La liberté contractuelle est protégée notamment par la liberté économique au sens de l'art. 27 Cst., cf. CR Cst.-MARTENET, art. 27 N 55. Au sujet de la liberté contractuelle

Les professions liées aux services numériques de sécurité ne sont pas réglementées en Suisse. L'accès et l'exercice de ces activité dépendent des pratiques contractuelles, surtout en ce qui concerne les exigences de cybersécurité à respecter dans leurs prestations. Cependant, les prestataires de gestion de cyberincidents sont susceptibles d'être soumises à des bases légales qui encadrent leur pratique, typiquement contractuelle. 626

Les prestataires privées de gestion de cyberincidents offrant leurs services à des organisations privées sont engagées sur la base d'un contrat régi par le Code des obligations (CO). Leur activité est soumise à la réglementation contractuelle s'appliquant à la relation entretenue avec l'organisation bénéficiant de leurs prestations. Cela étant, leur pratique et le niveau de cybersécurité à assurer peuvent être encadrés par la loi, en fonction notamment de leur clientèle. 627

Avant de parcourir ces différentes normes impactant la pratique de ces expertes, il est important de rappeler qu'une prestataire de gestion de cyberincidents peut être organisée de plusieurs façons. Par conséquent, elle peut entretenir des relations de différente nature avec l'organisation ou les organisations pour lesquelles elle travaille[1143]. L'on distingue principalement entre la fournisseuse interne et la prestataire externe ou commerciale. Une fournisseuse interne fournit en principe des prestations de gestion de cyberincidents à une société dont elle fait partie[1144]. Elle peut revêtir plusieurs formes. Elle peut être centralisée, à savoir localisée dans une seule zone physique ou géographique, ce qui peut typiquement être le cas pour de petites organisations[1145]. La fournisseuse peut également être distribuée, à savoir divisée entre plusieurs emplacements détenant chacun leur point de contact, avec une personne compétente pour contrôler et coordonner les activités[1146]. 628

au sens étroit, à savoir le droit d'aménager ses contrats librement : art. 19 al. 1 CO ; CR CO I-GUILLOD/STEFFEN, art. 19/20 N 48 ss ; SURY, *Digital in Law,* 2021, p. 16 et 61 s.

1143 ISO/IEC 27035-2 : 2016, p. 14 ; ANCELLE/FERDJANI, p. 135. Voir par exemple, dans une enquête effectuée par l'ElCom, que certaines infrastructures d'énergie ne disposent ni d'un CERT ni d'un SOC, que d'autres en ont, à l'interne, à l'externe ou aux deux, cf. ELCOM, *Cyber-Sicherheit 2019,* 2019, p. 30.

1144 KILLCRECE et al., *Organisational Models for CSIRT,* 2003, p. 12 ; KILLCRECE et al., *State of Practice of CSIRT,* 2003, p. 14 ; MORGUS et al., *CSIRT Basics for Policy-Makers*, 2015, p. 11.

1145 ALBERTS et al., p. 7 ; KILLCRECE et al., *Organisational Models for CSIRT,* 2003, p. 12 et 33 ss ; KILLCRECE et al., *State of Practice of CSIRT,* 2003, p. 15. Lorsqu'une prestataire interne de gestion de cyberincidents est centralisée, elle bénéficie régulièrement d'une large autorité, ce qui signifie que rares sont les décisions importantes en matière de gestion de cyberincidents prises sans son accord, cf. KILLCRECE et al., *Organisational Models for CSIRT*, 2003, p. 77.

1146 NIST, *Computer Security Incident Handling Guide*, 2012, p. 13 ; GILLIÉRON Philippe, *L'établissement d'un plan de réponse en cas de faille de sécurité* ; KILLCRECE et al., *Orga-*

Finalement, elle peut revêtir une forme combinée, entre l'organisation distribuée et l'organisation centralisée[1147].

629 À l'inverse, la prestataire externe de gestion de cyberincidents fournit en principe des prestations à un cercle extérieur de clientes qui recourt à ses compétences de gestion de cyberincidents[1148]. Ce type d'expertes peut fournir des services dans un cadre purement bilatéral ou à une communauté, à l'instar d'une CSIRT sectorielle[1149]. Les prestataires externes peuvent être des organisations qui vendent leurs solutions de services, leurs produits ou différentes prestations à leur clientèle[1150]. Les prestataires externes comptent aussi les personnes physiques telles que les «*freelancers*» agissant de façon indépendante à leur clientèle[1151]. Il existe également des CSIRT de fournisseuses (ou *vendors CSIRT*). Ce sont des fournisseuses de prestations tournées vers le public, au sein d'organisations produisant des technologies, qui offrent un soutien opérationnel dans la gestion d'incidents limité à la sécurité des produits fournis ou communément utilisés[1152].

2. La réglementation entre cocontractantes privées

a. Les contrats envisageables

(i) Les facteurs d'influence

630 Le domaine d'activité de l'organisation au sein de laquelle travaille la prestataire de gestion de cyberincidents ou la clientèle à laquelle elle fournit des prestations a un impact sur ses obligations. Des facteurs tels que ses compétences concrètes ou sa structure sont également susceptibles d'avoir un impact. Le contrat liant une prestataire à une organisation diffère selon que celle-là soit interne ou externe à l'organisation. Les prestations qu'elle fournit

nisational Models for CSIRT, 2003, p. 12, 33 s. et 57 ; KILLCRECE et al., *State of Practice of CSIRT,* 2003, p. 15.

1147 KILLCRECE et al., *Organisational Models for CSIRT,* 2003, p. 34 et 95 ss ; KILLCRECE et al., *State of Practice of CSIRT,* 2003, p. 15.

1148 AES, *Handbuch Grundschutz für «Operational Technology» in der Stromversorgung,* 2018, p. 30 ; KILLCRECE et al., *Organisational Models for CSIRT,* 2003, p. 12 ; SURY, *Digital in Law,* 2021, p. 114.

1149 Au sujet de cette tendance, voir ENISA, *How to set up CSIRT and SOC,* 2020, p. 41. À noter que si une CSIRT a une communauté, elle sera tout de même liée à chaque cliente qu'il sert individuellement. Parallèlement, elle est susceptible de se lier à l'entier de la communauté simplement par un accord de confidentialité, dans la mesure où le but de la constitution d'une communauté autour d'une CSIRT est premièrement l'échange d'informations.

1150 SURY, *Informatikrecht,* 2013, p. 10.

1151 DSOUZA, p. 217.

1152 Voir notamment DSOUZA, p. 211 ; MORGUS et al., *CSIRT Basics for Policy-Makers,* 2015, p. 11 s. ; WEST-BROWN et al., p. 62.

influencent également la qualification du contrat, par exemple si elle se limite à fournir des conseils ou si elle fournit, respectivement met à disposition de sa clientèle des logiciels de détection de cyberincidents. La qualification du contrat influe sur les obligations de la prestataire de gestion de cyberincidents, par exemple en termes de diligence ou de responsabilité.

631 Lorsqu'une organisation compte en son sein des personnes physiques compétentes pour assurer sa cybersécurité, le contrat lie l'employeuse au sein de l'organisation et ses collaboratrices. Les collaboratrices d'une organisation spécialisées pour la gestion de cyberincidents de celle-ci sont généralement considérées comme des travailleuses liées à une employeuse par le biais d'un contrat individuel de travail (art. 319 ss CO). Les prestataires externes peuvent quant à elles être liées par un contrat individuel de travail, un contrat de mandat (art. 394 ss CO), d'entreprise (art. 363 ss CO) ou un contrat innommé[1153].

(ii) Le contrat individuel de travail

632 Le contrat individuel de travail se conclut entre une employeuse et une travailleuse. L'employeuse peut être une personne physique ou morale[1154]. L'employeuse est souvent partie de l'organisation au sein de laquelle est intégrée la prestataire de gestion de cyberincidents. La travailleuse est la collaboratrice spécialisée dans la gestion de cyberincidents de l'organisation qui l'emploie[1155]. Les art. 319 ss CO s'appliquent à la relation contractuelle de travail et prévoient les droits et les obligations auxquelles sont individuellement soumises les collaboratrices.

633 À noter que les expertes peuvent être intégrées à une organisation privée, mais elles peuvent aussi l'être à une autorité publique. Dans le cas des collaboratrices engagées à l'interne par une autorité fédérale, la Loi sur le personnel de la Confédération (LPers) est applicable à la relation de travail (art. 2 LPers). Au niveau cantonal et communal, les lois cantonales trouvent application. Les art. 318 à 362 CO ne s'appliquent qu'à titre subsidiaire, en cas de renvoi exprès, pour combler une lacune ou lorsque les rapports de travail sont soumis au droit privé (voir par exemple l'art. 6 LPers pour l'administration fédérale)[1156].

1153 Pour un tableau récapitulatif des rapprochements possibles entre les contrats informatiques et les contrats nommés, voir ANCELLE/FERDJANI, p. 144.

1154 TERCIER/BIERI/CARRON, N 2753.

1155 Il est néanmoins également possible de conclure un contrat de *job sharing,* à savoir un contrat avec plusieurs travailleuses se partageant la tâche en équipe. Dans ce cas, les postes de travail, par exemple la réponse technique à un incident ou encore la mise à disposition d'une *hotline,* peuvent être réparties entre deux ou plusieurs travailleuses qui définissent la répartition des tâches entre elles, cf. ATF 122 V 169, c. 6.a.cc ; CR CO I-MEIER, art. 319 N 21 ; TERCIER/BIERI/CARRON, N 2747 et 2756.

1156 Cf. notamment ATF 138 I 232, c. 6.1 ; CR CO I-MEIER, art. 319 N 7.

634 À l'externe, certaines prestataires telles des *freelancers* endossent un rôle de travailleuse pour l'organisation qui les mandate, bien qu'elles soient en théorie indépendantes. Pour distinguer entre le statut d'indépendante et le statut de travailleuse, l'attention doit être portée sur l'exercice d'une activité régulière ou permanente de la *freelancer,* sa subordination ou son intégration à l'organisation du projet de l'employeuse, le degré de liberté de l'experte, son implication dans la gestion de projets, la partie supportant le risque économique, le compte de la personne au nom de qui la collecte est effectuée ou encore la perception de cotisations sociales par l'employeuse[1157].

(iii) Les autres contrats pour la prestataire externe

635 Lorsqu'une organisation fait appel en tant que cliente à une entreprise externe lui offrant des prestations de cybersécurité, le contrat liant une prestataire de gestion de cyberincidents à sa cliente relève rarement du contrat de travail individuel, lorsque la prestataire est une personne morale (en dehors du cas de la personne physique externe, à l'instar de la *freelancer*). En outre, il existe rarement un rapport de subordination entre la prestataire externe et sa cliente[1158]. Elles sont souvent liées par des contrats d'entreprise, des contrats de mandat ou des contrats innommés. Des contrats de licence sur des outils informatiques peuvent exister en sus ou en parallèle. Les prestations concrètes permettent de qualifier le contrat.

636 À titre d'exemple, le développement d'outils ou logiciels de sécurité individualisés[1159], à l'instar de systèmes de détection d'incidents, peut facilement être constitutif d'une prestation soumise au contrat d'entreprise[1160]. Le développement et la mise à disposition d'un logiciel revêtent dans tous les cas une part de prestations proches du contrat d'entreprise. Toutefois, le contrat ne

1157 Au sujet des personnes analogues aux travailleuses *(arbeitnehmerähnliche Personen)* et des fausses-indépendantes *(Scheinselbständige),* cf. notamment ATF 118 II 157, c. 2c et 4a.bb ; CR CO I-MEIER, art. 319 N 27 ; SURY, *Digital in Law,* 2021, p. 95 s. ; WYLER/HEINZER, p. 25 s.

1158 MÜLLER, N 1840.

1159 Les logiciels individualisés ou spécifiques sont conçus pour résoudre le problème spécifique d'une cliente. Ils sont à distinguer des logiciels standards destinés à une pluralité d'utilisatrices ainsi que des formes intermédiaires pour lesquelles une fournisseuse adapte un logiciel standard aux nécessités spécifiques d'une cliente, cf. TF, 4A_372/2022 du 11 juillet 2023, c. 4.2.1.

1160 Un ouvrage immatériel qui se matérialise lorsqu'il est enregistré de manière perceptible sur un support électronique de données, cf. MÜLLER, N 1821 s. ; STRAUB, *Gewährleistung und Haftung aus IT-Verträgen,* 2009, p. 250 ; STRAUB, *Verantwortung für Informationstechnologie,* 2008, p. 51. La simple fourniture du logiciel sans sa conception ferait pencher le contrat vers la vente. Par ailleurs, d'autres questions sont susceptibles de se poser en lien avec ces contrats notamment concernant le droit d'auteure, cf. TF, 4A_372/2022 du 11 juillet 2023, c. 4.2.

doit pas systématiquement être qualifié comme tel. L'entreprise de sécurité informatique qui limite son activité à prodiguer des conseils techniques ou politiques en qualité de conseillère ou consultante fournit des prestations relevant davantage du contrat de mandat[1161].

637 Contrairement à ces prestations, il n'est pas aisé de déterminer si l'activité spécifique de réponse à un cyberincident *(containment, eradication and recovery)*[1162] constitue une obligation de résultat ou de moyens. La qualification du contrat diffère selon que la partie contractante a une obligation de moyens ou une obligation de résultat. La délimitation est délicate à opérer entre l'obligation de résultat, caractéristique d'un contrat d'entreprise, et l'obligation de moyens, qui relève plus du contrat de mandat. Bien qu'il semble exigeant de considérer ce type de prestations comme une obligation de résultat et qu'il soit plus probable que la prestation consiste en une obligation de moyens, cette qualification dépend des circonstances concrètes, du contenu du contrat et de la volonté des parties[1163]. La liberté contractuelle implique une liberté s'agissant du choix du type de contrat à conclure.

638 Les diverses prestations offertes par une prestataire peuvent constituer une unité ou être indépendantes les unes des autres[1164]. Le choix des parties peut conduire à la conclusion d'un contrat innommé[1165]. Le contrat innommé peut consister en un contrat mixte, plus précisément combiné, qui contient des éléments du contrat de mandat ainsi que du contrat d'entreprise, ou se composer d'un contrat de mandat et d'un contrat d'entreprise distincts sous la forme d'un contrat composé[1166]. Tel serait par exemple le cas d'une organisation confiant à une prestataire externe de gestion de cyberincidents d'une part la tâche proactive de fournir un outil de détection des incidents

1161 Dans la mesure où il s'agit davantage d'une obligation de moyens que de résultats, cf. MÜLLER, N 2596 ; SURY, *Digital in Law,* 2021, p. 97. Il en irait de même pour l'accompagnement d'une cliente dans la migration de données sur une nouvelle plateforme informatique, à condition que la prestataire ne se soit pas engagée à atteindre un résultat objectivement vérifiable, cf. JACCARD/ROBERT, p. 99.

1162 Sur ces notions, cf. *supra* N 90 et 99 ss.

1163 À noter que la question de l'ouvrage se pose également dans ce contexte. Concrètement, la question est de savoir si l'on peut considérer comme un ouvrage le système informatique remis à une cliente dans un état sûr, par exemple après l'éradication complète d'un virus, le nettoyage des systèmes informatiques ainsi que la sauvegarde et la restauration des informations compromises.

1164 STRAUB, *Gewährleistung und Haftung aus IT-Verträgen,* 2009, p. 239 ; STRAUB, *Verantwortung für Informationstechnologie,* 2008, p. 21.

1165 CR CO I-GUILLOD/STEFFEN, art. 19/20 CO N 50 s.

1166 Sur les contrats composés et les contrats mixtes, cf. MÜLLER, N 3930 ss. Ces contrats sont récurrents dans les pratiques informatiques. Pour une comparaison, les contrats de solutions infonuagiques sont souvent des contrats mixtes de durée mêlant des éléments du contrat d'entreprise, de maintenance, de mandat et de licence, cf. JOTTERAND, p. 10.

(qui serait soumise, du moins en partie, aux dispositions du contrat d'entreprise, voire du contrat de vente si le logiciel ou le programme est vendu « clé en main »)[1167] et d'autre part celle de fournir des conseils techniques ou politiques (prestation qui serait soumise au contrat de mandat). Le contrat innommé peut également être un contrat *sui generis,* à l'instar de contrats d'*outsourcing* ou de maintenance[1168]. Le choix d'un contrat innommé implique des différences substantielles du droit applicable[1169].

639 Ces différences peuvent résulter d'autres formes d'engagement dans ce contexte de contrats innommés, par exemple si une entreprise de placement loue des travailleuses à une locataire[1170]. Dans un tel cas de figure, la Loi sur le service de l'emploi et la location de services (LSE) trouve application, emportant des conséquences, notamment contractuelles ou de responsabilités[1171]. Un contrat de travail classique est conclu entre la travailleuse et l'employeuse. En revanche, la bailleresse de services est liée à la locataire de services par un contrat innommé *sui generis*. Ce contrat comporte des éléments du contrat de mandat et il est réglé essentiellement par l'art. 22 LSE[1172]. En outre, la bailleresse n'a en principe qu'une obligation de moyens et c'est donc la locataire de services qui supporte le risque en cas de mauvaise exécution du contrat ; elle dispose de nombreuses limitations de responsabilité[1173]. La distinction entre le contrat de location de services et les contrats de mandat ou d'entreprise est donc importante en pratique[1174].

1167 L'établissement d'un programme ou logiciel individualisé peut être soumis aux règles du contrat d'entreprise, cf. TERCIER/BIERI/CARRON, N 3525, qu'il résulte d'un projet classique ou agile, cf. EGLI, N 49, et bien que cette solution n'exclue pas d'autres alternatives, cf. STRAUB, *Verträge für agil geführte Projekte,* 2015, N 77 ss. Le contrat d'entreprise peut être préféré au contrat de vente dans le cadre de la gestion de cyberincidents, le contrat de vente concernant davantage un rapport unique d'échange et étant par conséquent moins adapté aux relations juridiques s'établissant sur la durée et aux prestations récurrentes cf. ATF 124 III 456, c. 4b et bb ; JACCARD/ROBERT, p. 100 s.

1168 Au sujet des contrats de sous-traitance informatique, cf. notamment JOTTERAND, p. 12 ; STRAUB, *Verantwortung für Informationstechnologie,* 2008, p. 129 ; SURY, *Digital in Law,* p. 85. Pour les contrats de maintenance, voir notamment CJ/GE, arrêt ACJC/585/2018 du 24 avril 2018, c. 4.1 ; BRINER, p. 131 s. ; JOTTERAND, p. 12 ; MORAND, p. 129 ss ; STRAUB, *Gewährleistung und Haftung aus IT-Verträgen,* 2009, p. 272 ss ; STRAUB, *Verantwortung für Informationstechnologie,* 2008, p. 118 s.

1169 MÜLLER, N 3942 ss.

1170 ANCELLE/FERDJANI, p. 147.

1171 Pour des considérations sur la location de services, cf. notamment FÉLIX, p. 780 ss ; SUBILIA-BIGLER, p. 554 ss.

1172 FÉLIX, p. 782 s.

1173 FÉLIX, p. 791 ss.

1174 Sur la distinction entre contrat de location de services d'une part et les contrats d'entreprise et de mandat d'autre part, cf. FÉLIX, p. 793 ss.

(iv) Une réalité pratique

Il est difficile de définir un cadre juridique uniforme pour les contrats informatiques, compte tenu de la liberté contractuelle et dans la mesure où il existe un large éventail de prestations (les mêmes prestations pouvant faire l'objet de différents contrats en fonction des circonstances, des modalités contractuelles et de la volonté des parties)[1175]. Les diverses parties se lient régulièrement par le biais de conventions complexes et préformulées. Elles peuvent utiliser des contrats-types, des contrats-cadres contenant des projets individuels ou des contrats de services et accords de niveau de service (*service level agreement,* SLA)[1176]. Le contrat-cadre sert à déterminer l'objet du contrat, définir les notions générales qui seront reprises dans les contrats qui en découleront, les bases de rémunération, le droit applicable ou encore la procédure de modification de la relation. Si le contrat-cadre ne règle pas le droit contractuel applicable, il convient de déterminer le contrat nommé auquel rattacher chaque contrat, ce qui dépendra des prestations concrètes[1177]. Des modèles de contrats ont été élaborés par divers organismes mais il n'existe pas de règles globalement acceptées dans le domaine de la sécurité informatique, à l'inverse d'autres domaines comme celui de la construction[1178]. 640

Il ne serait pas opportun d'approfondir ici toutes les éventualités contractuelles, dans la mesure où la liberté contractuelle domine ces relations et que la loi est muette s'agissant des professions concernées par la gestion de cyberincidents. Il convient cependant de rappeler que la prestataire de gestion d'incidents doit respecter ses engagements contractuels ainsi que les limites posées par la loi (art. 19 al. 1 CO)[1179]. 641

D'autres exigences légales trouvent à s'appliquer à ces contrats. Les questions de protection des données doivent être réglées en amont (par exemple par un contrat de sous-traitance lorsqu'il doit être conclu en vertu de l'art. 9 LPD). Il en va de même des questions relatives au droit d'auteure lorsqu'une prestataire exploite un logiciel développé par une autre entreprise dans le cadre de ses activités, et d'autant plus si un logiciel est mis à disposition de la cliente par la prestataire de gestion de cyberincidents. Les questions de cession de 642

1175 JACCARD/ROBERT, p. 98 ; STRAUB, *Gewährleistung und Haftung aus IT-Verträgen,* 2009, p. 239 ; STRAUB, *Verantwortung für Informationstechnologie,* 2008, p. 19.

1176 CR CO I-CHAIX, art. 363 N 45 ; ANCELLE/FERDJANI, p. 142 ; GUROVITS KOHLI, p. 273 ; NEUENSCHWANDER, p. 129 ss.

1177 Sur l'application des dispositions du contrat d'entreprise aux contrats informatiques, cf. SURY, *Digital in Law,* 2021, p. 69.

1178 JACCARD/ROBERT, p. 124. Voir notamment les modèles de contrats élaborés par SWICO ou la Conférence suisse sur l'informatique (CSI) ; SURY, *Digital in Law,* 2021, p. 70.

1179 CR CO I-GUILLOD/STEFFEN, art. 19/20 N 4 ss, 30 ss et 60 ss ; MÜLLER, N 3943.

droit d'utilisation doivent être contractuellement réglées[1180]. Si les personnes œuvrant au sein d'une prestataire de gestion de cyberincidents sont transférées dans d'autres États, l'application de la LDét entraînera d'autres spécificités[1181]. Ces réflexions s'ajoutent au caractère déjà complexe de ce type de contrats.

643 En parallèle des contrats conclus avec leur clientèle, les prestataires de gestion de cyberincidents sont amenées en pratique à conclure des contrats avec d'autres partenaires, comme des prestataires analogues. Les contrats entre différentes prestataires de gestion de cyberincidents peuvent revêtir diverses formes. Il peut s'agir de simples contrats d'échange d'informations avec des clauses de responsabilité en cas de violations. Il peut également s'agir de contrats de licence, typiquement dans le cas où une prestataire de gestion de cyberincidents met à disposition d'autres prestataires analogues un logiciel tel un système de détection et de prévention d'intrusion (*intrusion detection and prevention system,* IDPS)[1182]. Par ailleurs, il s'agit dans ces cas de licence portant sur un droit immatériel absolument protégé par la loi ou sur un droit de propriété immatérielle proprement dit, dans la mesure où un logiciel est considéré comme une œuvre protégée par le droit d'auteure et fait régulièrement l'objet de licences (art. 2 al. 3 LDA)[1183].

b. Les conséquences

(i) Les impacts de la qualification du contrat

644 Lorsqu'une organisation souhaite organiser des compétences de gestion de cyberincidents, elle doit s'attarder sur quelques considérations qui dépendent du contrat la liant aux personnes compétentes. Audelà des considérations ayant trait à la rémunération, au pouvoir décisionnel ou aux risques, les régimes de responsabilités sont distincts. Les responsabilités doivent par exemple être délimitées et justifiées[1184].

645 Contrairement à une mandataire qui agit de manière indépendante et sous sa responsabilité, la travailleuse est au service de l'employeuse. Les organisations supportent plus de responsabilités et de coûts lorsqu'elles concluent un contrat individuel de travail. Partant, elles peuvent être tentées de privilégier une relation contractuelle avec une personne morale, avec laquelle il est impossible de contracter un contrat individuel de travail[1185].

1180 TF, 4A_372/2022 du 11 juillet 2023, c. 4.2.

1181 Pour plus d'informations et certaines difficultés sur ce sujet, cf. WYLER/HEINZER, p. 1157 ss.

1182 Au sujet des obligations découlant du contrat de licence, cf. ANCELLE/FERDJANI, p. 139 et 142 ; MÜLLER, N 4035 ss.

1183 ATF 125 III 263, c. 4a ; MÜLLER, N 4008.

1184 MÜLLER, N 1842 ; NIST, *Computer Security Incident Handling Guide,* 2012, p. 15.

1185 SURY, *Digital in Law,* 2021, p. 96.

(ii) Un exemple de responsabilité contractuelle

La responsabilité contractuelle d'une partie est engagée lorsqu'il y a une mauvaise exécution du contrat de laquelle découle un dommage pour la partenaire contractuelle[1186]. Principalement réglementée à l'art. 97 CO, la responsabilité contractuelle est précisée pour chaque contrat nommé. Une prestataire de gestion de cyberincidents peut être liée à sa cliente par différents contrats, en fonction notamment des prestations qu'elle offre. De plus, une distinction peut être opérée entre la fournisseuse interne de prestations de gestion de cyberincidents, dont on a vu qu'elle était généralement liée par un contrat de travail, et la prestataire externe de gestion de cyberincidents régulièrement liée par un contrat de mandat, un contrat d'entreprise ou un contrat innommé. Les différents contrats imposent une diversité d'obligations, variant d'une forme à l'autre, sont susceptibles d'engager la responsabilité de la prestataire ou d'une de ses expertes qui violerait ses obligations. 646

Concrètement, imaginons la situation dans laquelle une prestataire (interne ou externe) de gestion de cyberincidents est engagée par une organisation pour prévenir et détecter les cyberincidents subis par l'organisation ainsi qu'y réagir. L'organisation fait l'objet d'une cyberattaque par laquelle une personne malveillante de chiffrer ses informations. La prestataire de gestion de cyberincidents disposait d'une sauvegarde mais l'attaquante la chiffre. L'organisation peut-elle se retourner contre la prestataire de gestion de cyberincidents ? La réponse dépend d'une multitude d'éléments relatifs au cas d'espèce mais le contrat conclu entre la prestataire et l'organisation est susceptible d'influencer la réponse à donner, dans la mesure où le niveau de diligence attendu diffère selon le type de contrat conclu[1187]. 647

L'experte en cybersécurité engagée par un contrat de travail peut voir sa responsabilité auprès de son employeuse engagée sur la base de l'art. 321*e* CO. L'art. 321*e* al. 1 CO prévoit qu'elle répond du dommage qu'elle cause à l'employeuse intentionnellement ou par négligence. Pour que la responsabilité de la travailleuse soit engagée, les conditions usuelles de la responsabilité contractuelle doivent être remplies (dommage, violation contractuelle, causalité et faute)[1188]. 648

1186 SURY, *Digital in Law,* 2021, p. 121.

1187 Il s'agit ici d'un exemple général mais il va de soi que les prestations concrètes attendues de la prestataire de gestion de cyberincidents dans un cas d'espèce varient selon qu'il s'agisse par exemple d'un contrat de mandat ou d'un contrat d'entreprise.

1188 WYLER/HEINZER, p. 161 s.

649 La faute est un élément important d'appréciation de l'étendue de la réparation qu'il est possible d'exiger d'une travailleuse ; sans faute de sa part elle n'engage pas sa responsabilité sur le plan contractuel. Seules les fautes intentionnelles ou causées par négligence grave peuvent conduire à une réparation complète du dommage[1189]. L'étendue de la diligence attendue de la travailleuse se détermine notamment par le contrat, le risque professionnel, l'instruction, les connaissances techniques nécessaires pour accomplir le travail ainsi que les qualités et les aptitudes de la travailleuse que l'employeuse aurait dû connaître (art. 321*e* al. 2 CO). Les connaissances que l'on peut attendre de la travailleuse doivent souvent être les connaissances usuelles pour l'activité considérée ; seules des circonstances particulières permettent d'exiger de la travailleuse des capacités exceptionnelles[1190]. Il peut être difficile de détecter toutes les vulnérabilités exploitables et très difficile de prévoir les nouvelles techniques d'attaques. Il n'est en effet pas rare que des attaquantes maîtrisent de nouveaux logiciels malveillants qui ne sont pas encore connus de la communauté scientifique[1191]. Dans une pareille situation, il est difficile d'exiger qu'une experte en cybersécurité parvienne, même avec une réponse rapide et efficace, à conserver par exemple un contrôle sur toutes les données en danger en fonction de l'attaque visant l'organisation qui l'occupe. La travailleuse ne doit en tout cas pas supporter le risque d'entreprise lorsqu'il se produit en l'absence de faute de sa part. Elle est effectivement soumise à une obligation de moyens et non de résultat[1192]. Il est envisageable qu'une experte en cybersécurité employée pour gérer des cyberincidents ne parvienne pas à éviter tout dommage causé par un cyberincident mais sans faute de sa part. Dans un tel cas, elle n'engage pas sa responsabilité sur le plan contractuel. À noter que l'art. 321*e* CO n'exclut pas les mesures disciplinaires[1193].

650 Dans le cas où les règles d'un autre contrat seraient applicables (typiquement dans le cas de la prestataire externe de gestion de cyberincidents répondant aux règles du contrat de mandat ou du contrat d'entreprise), le niveau de la diligence est plus élevé malgré qu'il soit renvoyé à celui de la travailleuse[1194]. Les mandataires ou les entrepreneuses sont en principe engagées

1189 WYLER/HEINZER, p. 163.

1190 Pour un exemple, cf. ATF 110 II 344, c. 6.ee ; CR CO I-WITZIG, art. 321*e* N 2.

1191 STRAUB, *Verantwortung für Informationstechnologie,* p. 146 s

1192 CR CO I-WITZIG, art. 321*e* N 3.

1193 À ce sujet, cf. CR CO I-WITZIG, art. 321*e* N 9 ss ; ATF 119 II 162, c. 2 ; ATF 144 III 327, c. 5.5.2 ; WYLER/HEINZER, p. 169.

1194 CR CO I-CHAIX, art. 364 N 3 ; MÜLLER, N 2008 ; STRAUB, *Gewährleistung und Haftung aus IT-Verträgen,* 2009, p. 266 ; STRAUB, *Verantwortung für Informationstechnologie,* 2009, p. 90. Certaines questions se posent dans l'examen de la diligence de la travailleuse

en qualité de spécialistes, disposent de plus d'expertise que l'organisation qui requiert leurs compétences et effectuent leurs tâches de manière autonome, contrairement à une travailleuse[1195].

La diligence exigée par un contrat de mandat se distingue de celle du contrat d'entreprise, dans la mesure où le contrat de mandat ne requiert pas la réalisation d'un résultat, mais seulement un effort diligent de la part de la mandataire[1196]. La mandataire est liée par l'étendue du mandat fixée à l'avance[1197]. À défaut d'une convention, elle est liée par la nature de l'affaire, découlant du but du contrat, à savoir en tout cas la gestion de cyberincidents[1198]. Elle a un devoir de diligence, qui dépend des particularités du cas concret, de ses qualités ainsi que des difficultés qu'elle peut rencontrer[1199]. Dans tous les cas, la mandataire engage sa responsabilité non pas parce qu'elle n'atteint pas, du fait de sa faute ou non, le résultat souhaité (comme l'entrepreneuse), mais uniquement lorsqu'elle commet une faute, à savoir lorsqu'elle ne se comporte pas de la façon dont on pouvait l'attendre d'après les règles de l'art et de façon similaire à la situation d'une travailleuse[1200]. 651

Des règles contractuelles spécifiques peuvent également s'appliquer, par exemple en cas de transfert d'un système de détection de cyberincidents à une cliente. Il se peut que le contrat liant la prestataire de gestion de cyberincidents ou la fabricante à une cliente couvre le développement d'un logiciel individualisé pour détecter les cyberincidents et que celui-ci soit entaché d'un défaut. La notion de défaut est particulièrement importante dans le contrat d'entreprise et elle peut être complexe à appréhender dans le domaine informatique, dans la mesure où un logiciel ne peut être complètement exempt de dysfonctionnements ou vulnérabilités[1201]. 652

dans le domaine informatique, notamment en lien avec le risque qui est variable, cf. STRAUB, *Verantwortung für Informationstechnologie,* 2008, p. 146 s.

1195 Par exemple pour les mandataires, cf. STRAUB, *Verantwortung für Informationstechnologie,* 2008, p. 91.

1196 Le niveau attendu dépend de critères tels que le degré de spécialisation de la mandataire, CR CO I-WERRO, art. 394 N 7, art. 398 N 14 ; MÜLLER, N 2731 ; STRAUB, *Gewährleistung und Haftung aus IT-Verträgen,* 2009, p. 266. La mandataire étant en principe plus spécialisée que la travailleuse, sa responsabilité diffère en principe également, cf. STRAUB, *Gewährleistung und Haftung aus IT-Verträgen,* 2009, p. 266 ; STRAUB, *Verantwortung für Informationstechnologie,* 2008, p. 90.

1197 CR CO I-WERRO, art. 396 N 3.

1198 Sur la nature de l'affaire, cf. CR CO I-WERRO, art. 396 N 4.

1199 CR CO I-WERRO, art. 396 N 4 ; STRAUB, *Verantwortung für Informationstechnologie,* p. 90 s.

1200 TERCIER/BIERI/CARRON, N 4339.

1201 JACCARD/ROBERT, p. 109.

(iii) Quelques autres aspects de la responsabilité contractuelle

653 La débitrice de l'obligation répond du dommage causé par ses collaboratrices en cas d'inexécution d'obligations contractuelles (art. 101 CO)[1202]. À titre d'exemple, il se peut qu'un établissement bancaire comptant une fournisseuse interne de prestations de gestion de cyberincidents engage sa responsabilité vis-à-vis d'une cliente qui se voit imputer des achats en ligne effectués sans droit par une personne tierce qui aurait détourné ses données par une intrusion dans les systèmes informatiques de la banque[1203]. Par ailleurs, si la gestion de cyberincidents est déléguée à une prestataire externe, l'établissement bancaire risque tout de même d'engager sa responsabilité pour le fait de son auxiliaire au sens de l'art. 101 CO, dans la mesure où la notion d'auxiliaire est large et qu'un lien de subordination n'est pas nécessaire[1204]. À noter que la question du recours récursoire contre la collaboratrice de la prestataire de gestion de cyberincidents dépend de la relation contractuelle entre cette dernière et la débitrice. En pratique, des exclusions de responsabilité peuvent exister[1205]. Typiquement, lorsqu'une prestataire de gestion de cyberincidents est interne à une organisation, il peut être difficile pour cette dernière de choisir, instruire et (surtout) contrôler les prestations rendues par cette première, particulièrement lorsqu'elle ne dispose pas de connaissances spécifiques en cybersécurité. La prestataire est réputée disposer de compétences souvent plus spécifiques. Partant, si les travailleuses possèdent les compétences professionnelles nécessaires et qu'elles ont été suffisamment instruites, le juge prend ces considérations en compte dans la détermination de la faute de celles-ci. Cette prise en compte peut permettre aux employeuses de répondre dans une moindre mesure des fautes des travailleuses disposant de compétences plus poussées, selon ce que le juge décide[1206].

654 Lorsque les parties à un contrat prévoient des clauses annexes comme des SLA ou des accords de confidentialité (*non-disclosure agreements,* NDA) elles peuvent prévoir dans ces clauses des peines conventionnelles, pénalités ou autres conséquences pour violation, inexécution ou mauvaise exécution des obligations y figurant[1207]. Contrairement aux secrets légaux auxquels la loi attache des sanctions définies, la responsabilité en cas de violation d'un

1202 CR CO I-THÉVENOZ, art. 101 N 3 ; CR CO I-WERRO/PERRITAZ, art. 55 N 32.

1203 Exemple basé sur MEIER, N 1783. L'engagement de la responsabilité dépendrait naturellement des circonstances concrètes.

1204 CR CO I-THÉVENOZ, art. 101 N 11.

1205 À ce sujet, CR CO I-THÉVENOZ, art. 101 N 34 et 37 ss ; STRAUB, *Gewährleistung und Haftung aus IT-Verträgen,* 2009, p. 280 ss ; SURY, *Digital in Law,* 2021, p. 99.

1206 SURY, *Digital in Law,* 2021, p. 99.

1207 Pour les SLA, voir GUROVITIS KOHLI, p. 280.

secret conventionnel doit typiquement être analysée sous l'angle des violations contractuelles[1208].

Dans des circonstances présentant une composante extraterritoriale, d'autres instruments légaux sont susceptibles de s'appliquer, comme la Loi fédérale sur le droit international privé (LDIP) ou encore la Convention de Lugano (CL)[1209]. 655

Finalement, dans des circonstances plus complexes, par exemple en cas de location de services, plusieurs types de responsabilité pourraient trouver à s'appliquer. La locataire de service peut notamment agir contre la bailleresse sur la base de l'art. 97 CO (en faisant attention à ses exclusions de responsabilité), qui pourra exclure sa responsabilité, respectivement se retourner contre sa travailleuse fautive sur la base de l'art. 101 CO. La locataire peut en outre se retourner sur la base de l'art. 41 CO contre la travailleuse avec qui elle n'a pas de relation contractuelle[1210]. 656

D. Entre prestataire privée et cliente critique

1. Les fournisseuses internes aux infrastructures critiques

Les prestataires de gestion de cyberincidents offrent des prestations à une variété d'organisations, parmi lesquelles figurent de nombreuses infrastructures critiques. La réglementation de la cybersécurité au sein des différents secteurs critiques est dispersée et les compétences spécifiques des prestataires de gestion de cyberincidents varient en fonction du domaine d'activité de leur clientèle[1211]. 657

Lorsqu'une infrastructure critique soumise à des exigences minimales de cybersécurité compte en son sein une prestataire de gestion de cyberincidents ou plus largement une fournisseuse de service numérique de sécurité, l'activité de la prestataire est soumise aux exigences minimales applicables à l'infrastructure critique. 658

Les fournisseuses internes aux autorités et organisations soumises à la LSI vont devoir respecter les exigences de la loi[1212]. Pour un autre exemple, l'on peut par exemple trouver des exigences minimales de cybersécurité dans 659

1208 EPINEY/FASNACHT, N 48.

1209 Voir par exemple dans le domaine de la protection des données personnelles MEIER, N 1848.

1210 L'étendue de la réparation doit cependant être fixée en fonction de la gravité de la faute de la travailleuse et des circonstances en vertu de l'art. 43 CO, cf. WYLER/HEINZER, p. 166 s. Sur la responsabilité civile, cf. *infra* N 679 ss.

1211 CF, *CSN*, 2023, p. 24.

1212 Il en irait typiquement de la sorte pour la MilCERT, la CERT de l'armée.

la LApEl révisée et concrétisée par la OApEl. Le futur art. 5a al. 1 OApEl, découlant du nouvel art. 8*a* LApEl donne un caractère contraignant à la Norme minimale pour améliorer la résilience informatique de l'OFAE pour les organisations de l'art. 5*a* al. 2 OApEl[1213]. La prestataire de gestion de cyberincidents interne à une de ces organisations doit être impliquée dans les différentes étapes et mesures pour assurer la cybersécurité au sein de l'organisation conformément à ce qui est attendu dans l'annexe 1*a* OApEl[1214]. Elle est donc garante, du moins en partie, du respect des exigences minimales contraignantes en termes de prévention, de détection et de réaction (dans la limite de ses compétences) par l'organisation au sein de laquelle elle œuvre.

660 En parallèle de ce type d'exigences, il n'est pas exclu que les fournisseuses internes de prestations de gestion de cyberincidents soient chargées du respect des obligations d'annonce, surtout pour l'obligation de signaler les cyberattaques à l'OFCS en vertu des art. 74*a* ss LSI2. Cette compétence peut revenir à la prestataire de gestion de cyberincidents, surtout si elle compte en son sein une ou plusieurs juristes. Dans les cas où une cyberattaque au sens de l'art. 74*d* LSI2 se produit et que la prestataire de gestion de cyberincidents est compétente pour transmettre l'annonce à l'OFCS, le signalement peut, mais ne doit pas, être transmis électroniquement par le biais d'un formulaire établi par l'OFCS mais pas obligatoirement (art. 74*f* LSI2)[1215]. Le système sécurisé devant permettre les annonces à différentes autorités (art. 74*f* al. 2 et 3 LSI2), les organisations doivent organiser leurs compétences internes pour remplir les diverses obligations d'annoncer[1216].

661 Certaines normes mentionnent des structures de prestataires de gestion de cyberincidents à l'instar du *Security Operation Center* (SOC) et de la CSIRT, en soulignant leur importance pratique[1217].

1213 Cf. *supra* N 414 ss.

1214 Cf. 1 Annexe 1*a* OApEl pour le niveau de protection selon l'organisation : le niveau attendu dépend de l'importance de l'organisation ; le niveau de protection A prévoit des exigences plus strictes pour les entreprises pour l'approvisionnement en électricité les plus importantes et les niveaux B et C comportent des exigences moins élevées pour les organisations respectivement de taille moyenne ou de petite taille, cf. DETEC, *Rapport explicatif concernant l'avant-projet relatif à la révision de mai 2024 de l'ordonnance sur l'approvisionnement en électricité,* 2023, p. 5. Cf. 2 Annexe 1*a* OApEl pour les valeurs minimales à atteindre en fonction des mesures et du niveau de protection. Pour les mesures de la norme, cf. OFAE, *Norme minimale pour améliorer la résilience informatique,* 2023, p. 15 ss.

1215 FF 2023 84, p. 45 s. ; NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques,* 2022, p. 21 s.

1216 Pour plus d'informations sur les obligations d'annonce dont l'obligation de signaler les cyberattaques, cf. *supra* N 521 ss.

1217 Cf. par exemple AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung,* 2018, p. 24 ss.

2. Les prestataires externes de gestion de cyberincidents

a. Le cas particulier de la cliente étatique

(i) Le cadre légal

Les contrats entre une prestataire de gestion de cyberincidents privée et ses clientes privées sont largement régis par le CO et par des lois précisant certains types de contrats. Lorsque la prestataire agit pour une autorité ou une organisation étatique, la situation peut différer et d'autres lois peuvent entrer en ligne de compte. Des bases légales prévoient en outre que les exigences en termes de cybersécurité ou de sécurité de l'information et de sécurité informatique doivent être reprises dans les contrats avec des organisations tierces. 662

Lorsque la bénéficiaire des prestations est une autorité fédérale, la législation sur les marchés publics revêt un intérêt particulier. « Un marché public est un contrat conclu entre un adjudicateur et un soumissionnaire en vue de l'exécution d'une tâche publique », caractérisé par l'échange de prestations et de contre-prestations ; la prestation caractéristique est fournie par la soumissionnaire (art. 8 al. 1 LMP)[1218]. Les marchés publics portent notamment sur les projets informatiques (cf. notamment[1219] art. 8 al. 2 litt. c LMP)[1220]. Les procédures varient en fonction de la valeur seuil et peuvent consister en une procédure ouverte, une procédure sélective, une procédure sur invitation ou une procédure de gré à gré (art. 17 à 21 LMP)[1221]. 663

La prestataire de gestion de cyberincidents qui conclut avec l'État, typiquement à l'issue d'une procédure d'adjudication, est susceptible d'être soumise aux exigences qui s'appliquent à l'autorité contractante. C'est le cas pour la prestataire de gestion de cyberincidents qui conclut avec une unité administrative de la Confédération ou avec une autre autorité ou organisation de la Confédération au sens de l'art. 2 LSI[1222]. 664

La LSI régit spécifiquement la question des marchés publics, dans la mesure où il s'agit de fournisseuses de services numériques de sécurité contractant avec une autorité étatique. L'art. 9 LSI prévoit que les autorités et 665

1218 ZUFFEREY, p. 6. La LMP est prise ici comme exemple dans la mesure où la présente étude met un accent sur le droit fédéral ; elle est applicable aux autorités fédérales.

1219 D'autres lois, typiquement cantonales, peuvent s'appliquer en fonction des autorités concernées.

1220 FF 2017 1695, p. 1741.

1221 Les contrats de prestations informatiques sont souvent attribués de gré à gré, VOGT Reto, *IT-Sicherheit? Die meisten IT-Dienstleister schweigen*. Ces contrats sont souvent des contrats de durée qui peuvent soulever certaines questions dans le domaine informatique, cf. art. 15 al. 4 LMP ; FF 2017 1695, p. 1765.

1222 Cf. *supra* N 382 ss pour les autorités et organisations de la Confédération visées par l'art. 2 LSI.

organisations soumises à la loi doivent reprendre les exigences et mesures prévues par la LSI dans les contrats qu'elles concluent avec les organisations avec lesquelles elles collaborent (art. 9 al. 1 LSI). Les prestataires pour la cybersécurité des autorités et organisations soumises à la LSI doivent donc respecter les exigences et les mesures de la LSI et de l'OSI[1223]. Elles doivent à ce titre détecter les incidents liés à la sécurité de l'information et y réagir (art. 10 LSI) ou encore être actives dans la sensibilisation de leurs collaboratrices (art. 11 OSI). En outre, les cocontractantes ne devraient être habilitées à accéder aux informations ou aux moyens informatiques de la Confédération qu'une fois les mesures de sécurité nécessaires mises en œuvre[1224].

666 L'art. 10 OSI concrétise la disposition légale. L'ordonnance impose la responsabilité aux unités administratives par rapport aux risques relatifs à leurs objets à protéger ainsi qu'à leur potentielle dépendance vis-à-vis des organisations avec lesquelles elles collaborent (art. 10 al. 1 OSI). Le service spécialisé de la Confédération pour la sécurité de l'information émet, après consultation de l'OFCS et de la Conférence des achats de la Confédération (art. 24 Org-OMP), des recommandations quant aux dispositions de sécurité de l'information devant figurer dans tous les contrats d'acquisition ou de prestation de la Confédération (art. 10 al. 3 OSI). À la suite de la cyberattaque visant la société de services informatiques Xplain, le SEPOS est chargé d'élaborer en 2024 les clauses contractuelles standards pour la sécurité de l'information conformément à l'art. 19 al. 3 OSI[1225].

667 Finalement, d'autres dispositions légales prévoient quelques aspects pertinents lorsqu'une fournisseuse de prestations informatiques contracte avec une autorité fédérale[1226]. Par exemple, l'art. 11 OTNI prévoit que les fournisseuses externes de prestations informatiques ne peuvent avoir accès à des données non librement accessibles que si l'accès est nécessaire pour la prestation fournie, si l'autorité responsable des données a donnée par écrit son accord et que des mesures contractuelles, techniques et organisationnelles

1223 OA, *Enquête administrative « Fuite de données »*, 2024, N 301.

1224 FF 2017 1765, p. 2831. À noter également que ces tierces doivent être choisies avec soin, être identifiées en fonction de la sensibilité de l'activité concernée, être tenue au maintien du secret et recevoir une formation adaptée (art. 20 LSI), cf. OA, *Enquête administrative « Fuite de données »*, 2024, N 305.

1225 Il doit également élaborer dans ce délai des directives de sécurité pour la collaboration avec des fournisseuses, cf. SERVICE SPÉCIALISÉ DE LA CONFÉDÉRATION POUR LA SÉCURITÉ DE L'INFORMATION, *Train de mesures pour éviter de nouvelles fuites de données*, 2024, p. 2.

1226 Ces dispositions sont susceptibles de s'appliquer à l'activité d'une prestataire de gestion de cyberincidents.

appropriées ont été prises pour éviter que les données soient accessibles à des personnes tierces (art. 11 OTNI)[1227]. L'ordonnance ne fixe pas de mesures de sécurité que la prestataire doit prendre, mais elle prévoit que des mesures appropriées doivent être prises pour que la confidentialité des données soit garantie lorsqu'il s'agit de donner l'accès à la prestataire l'accès à des données non accessibles au public (art. 11 al. 1 litt. c OTNI). L'art. 11 OTNI n'apporte pas plus de précisions quant à de potentielles exigences de sécurité auxquelles la prestataire externe devrait se conformer. En parallèle, l'art. 7 OTUIC impose aux personnes chargées de travaux techniques sur l'infrastructure électronique de la Confédération des conditions à respecter pour accéder aux données de l'infrastructure électronique de la Confédération, cette fois expressément lorsqu'il en va de données personnelles ou de personnes morales (art. 7 al. 1 OTUIC). En revanche, elle impose aux prestataires externes une obligation de sécurité des données dans ce contexte[1228].

(ii) Les conditions générales et clauses types

668 Il existe une diversité de clauses contractuelles types dans le contexte de fourniture de prestations informatiques aux autorités de la Confédération[1229]. La Conférence des achats de la Confédération avait chargé le Centre de compétence des marchés publics de la Confédération de réviser les conditions générales (CG) de la Confédération pour les prestations informatiques. Depuis le 1er janvier 2024, de nouvelles CG s'appliquent notamment pour l'achat et la maintenance de matériel informatique, pour l'acquisition et la maintenance de logiciels standards, pour les contrats d'entreprise dans le domaine informatique et pour la maintenance de logiciels individuels, ainsi que pour les services informatiques. Les modifications des CG pour les services informatiques devraient décrire plus précisément et systématiquement l'étendue de la responsabilité dans ce cadre, afin d'éviter des interprétations divergentes ou des ambiguïtés. Ces modifications cherchent également à préciser que les informations devant être protégées et dont la sécurité doit être assurées ne sont pas uniquement les informations produites dans le cadre de l'exécution du contrat, mais également celles mises à disposition pour l'exécution concrète ou celles créées par une des parties au contrat[1230]. Ces CG prévoient que les

1227 Il peut typiquement s'agir d'informations couvertes par des secrets.

1228 L'art. 7 al. 2 OTUIC reprend l'art. 8 LPD qui s'applique aux sous-traitantes.

1229 SPÉCIALISÉ DE LA CONFÉDÉRATION POUR LA SÉCURITÉ DE L'INFORMATION, *Train de mesures pour éviter de nouvelles fuites de données,* 2024, p. 1 s.

1230 CCMP, *Révision des CG au 1er janvier 2024,* 2023, p. 4 s.

différentes prestataires doivent respecter toutes les dispositions légales pour garantir la « protection et [la] sécurité des données », à l'instar de la LSI[1231].

669 Il n'existe ni contrat type ni CG spécifiques pour les contrats de gestion de cyberincidents, mais ce type de prestataire est susceptible d'effectuer des prestations devant être couvertes par les CG et contrats types existants. Qui plus est, une nouvelle clause contractuelle type existe pour que les partenaires contractuelles contribuent à la protection des informations de la Confédération ainsi que des systèmes informatiques, en particulier dans le cadre d'activités sensibles de sécurité. La clause type, destinée à toutes les bénéficiaires de prestations au sein de l'administration fédérale et à leurs prestataires informatiques, prévoit que la fournisseuse de prestations doit protéger les moyens informatiques contre les cyberattaques et implémenter les mesures de prévention et d'élimination des dangers et des vulnérabilités ; la fournisseuse doit respecter les bases légales et les directives pertinentes. L'obligation de signaler les cyberattaques doit être prévue par le contrat, la prestataire doit prouver sa cybersécurité et autoriser la bénéficiaire à effectuer des audits. Le contrat doit également, selon la clause contractuelle type, prévoir une réglementation des peines conventionnelles, une clause de responsabilité et la souscription d'une assurance responsabilité civile[1232].

670 En cas de violations des exigences susmentionnées, la prestataire est susceptible d'être sanctionnée sous l'angle des marchés publics (art. 44 LMP). La LSI2 prévoit par ailleurs que la fabricante de matériel informatique ou de logiciel qui n'élimine pas une vulnérabilité dans le délai fixé par l'OFCS peut être exclue par une soumissionnaire de la procédure d'adjudication, radiée d'une liste ou voir son adjudication révoquée (art. 44 al. 1 lit. f*bis* nLMP)[1233]. En parallèle et en cas d'inexécution ou d'exécution imparfaite du contrat, les règles applicables sont celles des art. 97 ss CO[1234]. Lorsque l'autorité ou l'organisation de la Confédération est liée à la prestataire de gestion de cyberincidents par le biais d'un contrat de location de services, elle peut agir contre la bailleresse de services sur la base de l'art. 97 CO et contre la travailleuse sur la base de l'art. 41 CO[1235].

1231 Voir par exemple CCMP, *Conditions générales pour l'acquisition et la maintenance de logiciels standard,* 2023, ch. 25.1 et référence citée ; CCMP, *Conditions générales pour les services informatiques,* 2023, ch. 17.1 et référence citée.

1232 CA, *Clause contractuelle type de la CA pour les cyberattaques,* 2024, p. 2 ss. À noter que d'autres CG existent pour les relations contractuelles avec des prestataires informatiques, cf. *supra* N 491.

1233 FF 2023 84, p. 54.

1234 DUBEY/ZUFFEREY, N 1125.

1235 Cf. *supra* N 646 ss et 679 ss.

b. L'exemple de l'approvisionnement en électricité

La modification de la législation pour l'approvisionnement en électricité a pour conséquence que les organisations soumises aux exigences minimales de la Norme minimale pour améliorer la résilience informatique de l'OFAE doivent s'assurer que leurs prestataires externes respectent certaines exigences de cybersécurité. Il en va typiquement de la sorte pour la gestion de risques liés à la chaîne d'approvisionnement. Toutes les organisations de l'art. 5*a* OApEl doivent, indépendamment de leur niveau de protection, atteindre une valeur Tier 3 pour la mesure ID.SC-3[1236]. Cette valeur minimale à atteindre implique que les organisations doivent exiger contractuellement que leurs fournisseuses et prestataires de service développent et mettent en œuvre des mesures appropriées pour atteindre les objectifs du processus de gestion de risques liés à la chaîne d'approvisionnement[1237]. 671

D'autres exigences ont un impact sur le rôle et la responsabilité tout en demeurant générales. Par exemple, la mesure ID.AM-6 impose que les rôles et responsabilités des intervenantes externes soient établies[1238]. 672

3. Une conclusion sur l'influence sectorielle

En conclusion, l'activité des prestataires de gestion de cyberincidents est susceptible d'être conditionnée au respect d'exigences minimales de cybersécurité. Ces exigences varient en fonction des bases légales, des normes sectorielles et des contrats qui lient ces prestataires à leurs clientes. 673

La prestataire de gestion de cyberincidents interne à une infrastructure critique participe et partage les responsabilités pour assurer la cybersécurité dans les pratiques de l'organisation lorsque cette dernière est soumise à des 674

1236 Le Tier 3 est qualifié de « reproductible », à savoir que les plans sont validés, les risques informatiques sont répertoriés, les directives sont mises à jour, la pratique de l'organisation tient compte de ses nouveaux besoins, que des méthodes standardisées existent et que l'organisation sait qu'elle est tributaire de ses partenaires externes et partage des informations lui permettant de prendre des décisions, cf. OFAE, *Norme minimale pour améliorer la résilience informatique,* 2023, p. 38. Pour l'échelle des valeurs Tier, cf. *supra* N 370.

1237 OFAE, *Norme minimale pour améliorer la résilience informatique,* 2023, p. 20.

1238 OFAE, *Norme minimale pour améliorer la résilience informatique,* 2023, p. 15. Les organisations de niveau de protection A doivent atteindre la valeur de 4 (dynamique), contrairement aux organisations de niveau de protection B ou C qui doivent atteindre une valeur de 3 (reproductible). Sur ces valeurs, cf. *supra* N 416. Il conviendra de voir, une fois le cadre NIST mis à jour, comment l'OFAE en tient compte dans sa norme minimale, dans la mesure où cette mise à jour pourrait avoir une incidence sur le niveau de cybersécurité à assurer et le rôle des organisations tierces dans ce contexte, cf. NIST, *Public Draft : The NIST Cybersecurity Framework 2.0,* 2023, p. 26 s. ; NIST, *The NIST Cybersecurity Framework (CSF) 2.0,* 2024, p. 18.

exigences minimales de cybersécurité. Lorsque la prestataire de gestion de cyberincidents est externe, la loi peut imposer qu'elle se conforme aux mêmes exigences que l'organisation à laquelle elle fournit ses prestations. Autrement, elle peut être contractuellement obligée de respecter les exigences minimales de cybersécurité imposées à sa cliente. Les clauses types et les exigences auxquelles une prestataire offre des services informatiques à une autorité fédérale ont été considérées comme manquant de clarté. La situation est toujours opaque, avec une multitude d'instruments, et il est important que la situation soit rapidement clarifiée pour que des exigences et des responsabilités claires existent.

E. Les responsabilités indépendantes du contrat

1. Une remarque introductive

675 Les prestataires de gestion de cyberincidents peuvent engager leur responsabilité également hors du contrat. Si les agissements des personnes physiques ou morales expertes causent un dommage à une personne tierce, elles sont susceptibles d'engager leur responsabilité civile pour acte illicite. L'employeuse est en principe tenue pour responsable des agissements de ses collaboratrices.

676 En parallèle, les prestataires de gestion de cyberincidents peuvent engager leur responsabilité en vertu d'autres lois selon les prestations qu'elles fournissent. Elles peuvent typiquement être responsables de la violation d'une obligation de la Loi fédérale sur la responsabilité du fait des produits (LRFP) ou de la LDA.

677 Elles peuvent aussi engager leur responsabilité administrative ou pénale si elles violent des exigences légales applicables en raison de leur qualité d'infrastructure critique, d'exigences légales sectorielles de sécurité ou sur la base de la LSPro en fonction des produits qu'elles fabriquent[1239].

678 La responsabilité civile au sens des art. 41 et 55 CO concerne la personne physique indépendante qui fournit ses prestations à une cliente, l'entreprise externe ou l'infrastructure critique privée. La responsabilité de la fournisseuse interne de prestations de gestion de cyberincidents est couverte par la Loi sur la responsabilité LRCF au niveau fédéral et par les lois cantonales de responsabilité de l'État pour les autorités cantonales[1240].

1239 La responsabilité pénale des prestataires de gestion de cyberincidents ainsi que la responsabilité pour violations d'obligations de protection des données et pour violations d'obligations de garder le secret seront analysées plus tard, cf. *infra* N 928 ss et 976 ss.

1240 La LRCF sera abordée plus tard dans l'analyse de l'OFCS, cf. *infra* N 765 ss.

2. La responsabilité civile pour acte illicite

a. La responsabilité civile

679 La responsabilité extracontractuelle ne se fonde pas sur un rapport direct régi par des règles contractuelles[1241]. La responsabilité civile peut relever de différents chefs de responsabilité, et découle de l'art. 41 CO si un acte illicite est commis, ou dans un contexte de location de services. D'autres lois spécifiques comme la LSPro ou la législation applicable en matière de propriété intellectuelle prévoient des situations de responsabilité civile.

680 Pour que l'art. 41 CO s'applique dans ce contexte, il faut un dommage, une faute de la part d'une personne active au sein de la prestataire de gestion de cyberincidents, un acte illicite (à savoir un acte commis en violation d'une norme) et un lien de causalité entre l'acte illicite et le dommage[1242]. Des questions peuvent se poser en lien avec les dommages directs ou indirects. Les prestataires de gestion de cyberincidents peuvent plus régulièrement être à l'origine de dommages indirects. La question se pose typiquement dans le cas où la prestataire de gestion de cyberincidents commet un acte illicite entraînant un dommage supplémentaire à celui causé par une cyberattaque à la santé des patients d'un hôpital. L'analyse du lien de causalité peut au même titre être délicate[1243]. Il faut systématiquement analyser si c'est bien le fait d'une collaboratrice de la prestataire qui est à l'origine d'un dommage. Cela pourrait typiquement être le cas si, dans la gestion d'un incident auprès d'un établissement bancaire, la CSIRT n'isole pas un serveur compromis par une attaque et que l'attaquante peut accéder et soustraire des montants de comptes clientes[1244]. Lors de l'examen de ce chef de responsabilité, il est nécessaire d'être dans un cas où un acte illicite est commis par une collaboratrice de la prestataire de gestion de cyberincidents, par exemple s'il y a la réalisation d'une infraction pénale, à l'instar d'un accès indu à un système informatique au sens de l'art. 143*bis* CP. D'autres questions peuvent se poser dans ce contexte, notamment en rapport avec le lien de causalité (notamment par rapport à l'invocation de la force majeure).

681 La personne dont les données sont traitées illicitement peut attaquer la personne physique ou morale fournissant des prestations de gestion de cyberincidents qui réunirait les conditions de l'art. 41 CO en utilisant un moyen

1241 STRAUB, *Verantwortung für Informationstechnologie,* 2008, p. 173.

1242 SURY, *Digital in Law,* 2021, p. 122 s.

1243 STRAUB, *Verantwortung für Informationstechnologie,* 2008, p. 178.

1244 Sur les différents dommages, cf. notamment STRAUB, *Verantwortung für Informationstechnologie,* 2008, p. 177 s. ; SURY, *Digital in Law,* 2021, p. 124.

réparateur (et outre les moyens d'action basés sur les art. 30 ss LPD et 28 ss du Code civil, CC). Concrètement, imaginons le cas d'une prestataire de gestion de cyberincidents active auprès d'un établissement hospitalier, qui déconnecte par erreur des systèmes informatiques non compromis sur lesquels sont stockés les dossiers de la patientèle. Cette action a pour conséquence la perte de données de patientèle et une patiente se voit administrer de la pénicilline alors qu'elle y est allergique, information figurant dans son dossier. L'administration de pénicilline a pour conséquence de fortes réactions de la patiente qui doit être prise en charge. La nouvelle prise en charge de la patiente occasionne à cette dernière d'importants frais médicaux supplémentaires. Si le lien de causalité entre les agissements de la collaboratrice de la prestataire de gestion de cyberincidents et les frais médicaux supplémentaires peut être prouvé par la patiente lésée, l'experte en sécurité informatique est susceptible de devoir des dommages-intérêts à la patiente sur la base des art. 41 ss CO. La patiente peut dans ce genre de cas potentiellement prétendre également à des indemnités de tort moral, si l'atteinte revêt un certain degré de gravité (art. 49 CO)[1245].

682 À noter déjà ici que l'art. 55 CO, primant l'art. 41 CO, permettrait à la patiente de se tourner vers l'employeuse, à savoir l'entreprise employant l'experte à l'origine de l'erreur[1246]. Si la prestataire de gestion de cyberincidents est interne à l'hôpital, il est plus vraisemblable que ce dédommagement passe par la relation contractuelle, dans la mesure où les patientes se situent dans une relation contractuelle avec l'établissement.

b. La responsabilité de l'employeuse

683 La collaboratrice à l'origine d'une responsabilité au sens de l'art. 41 CO peut œuvrer comme collaboratrice interne à une organisation ou au sein d'une prestataire externe. Dans tous les cas, son employeuse est en principe responsable de ses actes commis dans l'exercice de ses fonctions selon l'art. 55 al. 1 CO[1247], sous réserve que l'employeuse prouve avoir pris tous les soins commandés pour éviter le dommage ou que sa diligence n'aurait pas modifié la situation advenue. L'art. 55 CO constitue une *lex specialis* par rapport à l'art. 41 CO[1248].

684 Si un dommage est causé de façon illicite par la collaboratrice dans l'accomplissement de son travail, son employeuse en répond auprès des personnes tierces, sous réserve qu'elle prouve qu'elle a fait preuve de toute la

1245 MEIER, N 1785.

1246 CR CO I-WERRO/PERRITAZ, art. 55 N 6 ss.

1247 Au sujet de l'exception, cf. STRAUB, *Verantwortung für Informationstechnologie*, 2008, p. 188 ss.

1248 CR CO I-WERRO/PERRITAZ, art. 55 N 28.

diligence que l'on pouvait objectivement attendre d'elle[1249]. L'employeuse a ensuite un recours récursoire contre l'employée responsable du dommage (art. 55 al. 2 CO). Le lien de subordination fait foi. Par conséquent, la *freelancer* peut, selon les circonstances, être considérée comme une de « ses autres auxiliaires » selon l'art. 55 al. 1 CO[1250].

c. La responsabilité du fait des produits

L'organisation responsable du développement d'un logiciel peut répondre des défauts de ses produits sur la base de la LRFP. L'application de cette loi est limitée lorsqu'il en va des produits qu'une prestataire de gestion de cyberincidents peut mettre à disposition de sa clientèle. Pour qu'une responsabilité soit envisageable, il faut tout d'abord être en présence d'un « produit » au sens de la loi. Un logiciel en tant que tel n'étant pas une chose mobilière, il faut considérer le logiciel, qui fait partie d'une chose, comme un système de mesure intelligent d'une machine permettant de commander et contrôler des accès à distance[1251]. 685

Une délimitation doit être faite entre les organisations qui développent et fabriquent les différentes pièces d'un produit. En outre, la personne physique ou morale utilisant le produit doit être distinguée de la personne ayant créé le logiciel (si ce n'est pas la prestataire de gestion de cyberincidents) pour savoir qui est à l'origine de la faute ou qui doit engager sa responsabilité[1252]. Finalement, il n'est pas exclu qu'une fabricante bénéficie d'une exception et n'engage pas sa responsabilité si le produit défectueux est entaché d'un défaut dont l'existence ne pouvait pas être décelée lors de la mise en circulation du produit selon l'état des connaissances scientifiques et techniques (art. 5 al. 1 litt. e LRFP). 686

Ensuite, la loi institue une responsabilité uniquement lorsqu'un produit défectueux cause la mort ou des lésions corporelles, ce qui est rare dans le contexte qui nous occupe, ou qu'il cause un endommagement ou une destruction d'une chose habituellement utilisée pour la consommation privée et que c'est à cette fin qu'elle était utilisée (art. 1 al. 1 LRFP). Cela implique que les dommages industriels ne sont pas couverts par la loi, ce qui est susceptible de se produire de façon bien plus fréquente dans l'activité de CSIRT auprès d'infrastructures critiques. Pour ces cas, l'art. 55 CO et le droit général de la responsabilité délictuelle s'appliquent sans réserve[1253]. 687

1249 À noter qu'en pratique les entreprises de sécurité informatique peuvent souscrire à des assurances de responsabilité civile professionnelle pour leur activité.

1250 STRAUB, *Verantwortung für Informationstechnologie,* 2008, p. 187.

1251 STRAUB, *Verantwortung für Informationstechnologie,* 2008, p. 194 s. ; SURY, *Digital in Law,* 2021, p. 127.

1252 STRAUB, *Verantwortung für Informationstechnologie,* 2008, p. 174.

1253 CR CO I-THÉVENOZ, art. 101 N 39.

688 Il est rare qu'une personne puisse se prévaloir de la LRFP lorsque des prestations de gestion de cyberincidents sont offertes à des infrastructures critiques, dès lors que la LRFP s'applique lorsqu'un dommage est causé à une chose habituellement utilisée pour la consommation privée. En outre, les prétentions basées sur la responsabilité pour le fait des produits se périment dix ans après la mise en circulation du produit (art. 10 al. 1 LRFP), ce qui en pratique peut amener la personne lésée à fonder ses prétentions sur d'autres bases pour s'assurer une protection[1254].

d. La responsabilité pour violation du droit d'auteure

689 La LDA permet plusieurs leviers d'action. Sur le plan civil notamment, elle permet à la personne qui risque de subir une violation de son droit d'auteure ou d'un droit voisin d'interdire, de faire cesser ou d'exiger de la partie défenderesse l'indication de la provenance et de la quantité des objets en sa possession, confectionnés ou mis en circulation illicitement (ainsi que la quantité d'objets qui ont été remis à des acheteurs commerciaux) conformément à l'art. 62 al. 1 LDA. Cette voie est ouverte en cas de risques pour les droits d'auteure ou les droits voisins selon les art. 39*a* al. 1 et 3, 39*c* al. 1 et 3 et 39*d* de la loi (par renvoi de l'art. 62 al. 1*bis* LDA).

690 Par exemple, la prestataire de gestion de cyberincidents qui utilise le logiciel d'une autre organisation en contournant les mesures techniques efficaces au sens de l'art. 39a al. 2 LDA pour la protection du logiciel, ou qui supprime les informations sur le régime des droits d'auteure au sens de l'art. 39*c* al. 1 LDA. Dans ce contexte, elle peut engager sa responsabilité sur le plan civil face à la titulaire des droits. À noter que l'art. 62 de la loi réserve les actions relevant du CO tendant au paiement de dommages-intérêts, à la réparation du tort moral ou à la remise du gain en gestion d'affaires (art. 62 al. 2 LDA)[1255].

3. La responsabilité pour violation d'obligations de sécurité

691 Une infrastructure critique et ses collaboratrices compétentes pour la gestion de cyberincidents peuvent engager leur responsabilité sur le plan administratif si elles ne répondent pas à leurs obligations de sécurité. Des sanctions ou autres mesures sont en pratique aujourd'hui rares, comme on peut le voir avec l'art. 8 al. 5 LApEl qui attribue au CF la compétence de prévoir des sanctions en cas de violations des prescriptions concernant un approvisionnement électrique sûr, compétence dont il n'a, à notre connaissance, pas encore fait usage.

1254 CR CO I-THÉVENOZ, art. 101 N 38.

1255 Pour plus d'informations sur l'action en exécution d'une prestation au sens de l'art. 62 LDA, cf. EGLOFF/HEINZMANN, p. 457 ss.

Outre ces rares situations, une prestataire externe de gestion de cyberincidents peut, en fonction de ses prestations, engager sa responsabilité sur d'autres fondements administratifs. Il en va de la sorte si elle met en circulation des logiciels soumis à la LSPro. La loi pose des exigences pour la mise en circulation de produits. Elle se limite cependant à protéger la sécurité physique et la santé des humains, ce qui limite son applicabilité aux prestataires de gestion de cyberincidents[1256]. Une prestataire de gestion de cyberincidents peut se voir contrôler et infliger une mesure administrative en vertu de l'art. 10 LSPro si elle produit ou importe un produit sans respecter les exigences techniques de mise en circulation, sans contrôler le produit mis en circulation ou en violant d'autres obligations lui incombant en vertu de la loi (art. 3 ss LSPro)[1257]. 692

4. La responsabilité pour violation d'obligations de signaler

En parallèle des manquements de sécurité, plusieurs lois imposent diverses obligations de signaler des attaques, incidents, événements importants et autres problèmes auxquels une prestataire de gestion de cyberincidents peut être confrontée. De telles obligations peuvent découler soit de son statut d'infrastructure critique (en vertu des art. 74*a* ss LSI2) ou du secteur dans lequel est active l'organisation au sein de laquelle œuvre la prestataire de gestion de cyberincidents (par exemple pour les organisations soumises à une obligation de signaler les cyberattaques à la FINMA). Les infrastructures critiques sont libres dans leur organisation interne, raison pour laquelle il est possible que la prestataire de gestion de cyberincidents soit compétente pour effectuer les différents signalements. La prestataire interne à un établissement financier devrait par conséquent annoncer les cyberattaques à la FINMA, de même pour la prestataire interne à une entreprise de transport public ou au corps de sapeurs-pompiers à la centrale CENAL. Les compétences liées à d'autres signalements que celui des art. 74*a* ss LSI2 étant fortement susceptibles d'incomber à d'autres personnes, seule la responsabilité en cas de violation de l'obligation de signaler les cyberattaques est parcourue. 693

La fournisseuses (en particulier interne) de prestations de gestion de cyberincidents d'une infrastructure critique peut être compétente pour transmettre les signalements de cyberattaques à l'OFCS[1258]. Si c'est le cas et qu'elle ne remplit pas son obligation dans les cas de l'art. 74*d* LSI2, l'OFCS 694

1256 Au sujet de l'application de la LSPro aux entreprises fournissant des services informatiques, cf. *supra* N 483 s.

1257 Elle peut également engager sa responsabilité pénale, cf. *infra* N 793 ss.

1258 Lorsqu'il en va de l'annonce de violations de la sécurité des données à la PFPDT, on part du principe qu'il s'agit au sein d'infrastructures critiques d'autres services des organisations.

l'informe de la nécessité de se conformer à l'obligation en lui fixant un délai approprié pour s'acquitter de son obligation (art. 74*g* al. 1 LSI2). Si l'infrastructure critique, par le biais de sa prestataire de gestion de cyberincidents, ne fournit toujours pas les informations requises par la loi, l'OFCS rend une décision sur cette obligation et fixe un nouveau délai avec la menace d'une amende (art. 74*g* al. 2 LSI2). Si l'obligation n'est toujours pas respectée, l'OFCS saisit les autorités de poursuite pénale (art. 74*h* LSI2). La personne qui ne se conforme pas intentionnellement à la décision de l'OFCS s'expose aux risques d'engager sa responsabilité pénale et de payer une amende de 100 000 francs au plus[1259]. L'entreprise peut être poursuivie sur la base de la Loi fédérale sur le droit pénal administratif (DPA) en vertu de l'art. 74*h* al. 2 LSI2. La DPA permet de rendre la cheffe d'entreprise responsable en vertu de l'art. 6 al. 2 DPA, à la manière de l'art. 29 CP. Il est donc possible d'attribuer une responsabilité pénale à la direction de l'entreprise[1260].

F. Une conclusion

695 Les prestataires de gestion de cyberincidents font partie des infrastructures critiques. En fonction des prestations qu'elles fournissent à leur clientèle, certaines obligations peuvent trouver application et elles peuvent revêtir un rôle particulier. En revanche et contrairement à ce qui prévaut pour d'autres soussecteurs critiques, elles ne sont pas soumises à des exigences minimales de cybersécurité, ni pour leurs systèmes informatiques ni dans le cadre de leurs activités.

696 La gestion de cyberincidents n'est pas une profession réglementée et il n'existe pas d'exigences relatives à la cybersécurité pour leurs activités. Des bases légales applicables à de nombreux domaines sont susceptibles de s'appliquer aux expertes compétentes, notamment lorsqu'il en va de leurs relations contractuelles. Une place importante est toutefois laissée à la pratique et la qualification du contrat liant une prestataire de gestion de cyberincidents et ses membres à sa clientèle entraîne des conséquences notamment en termes de responsabilité contractuelle.

697 Une prestataire de gestion de cyberincidents peut être soumise à des exigences si elle est interne à une infrastructure critique soumise elle-même à des exigences de cybersécurité. Si elle lui est externe, les exigences minimales de certains sous-secteurs critiques doivent être reprises afin que la prestataire

1259 FF 2023 84, p. 46 ss ; MEYER/MÉTILLE, *Loi fédérale sur la sécurité de l'information : version 2.0,* 2022, N 57.

1260 FF 2023 84, p. 47.

respecte les exigences auxquelles est soumise sa cliente. Les exemples les plus parlants pour ces pratiques sont ceux des autorités et organisations de la Confédération ou des organisations actives dans l'approvisionnement en électricité.

698 En dehors de ce cadre contractuel, les prestataires de gestion de cyberincidents et leurs membres peuvent engager leur responsabilité en cas d'acte illicite. Les art. 41 CO et 55 CO s'appliquent dans ces situations, ou, de façon plus spécifique, des lois spéciales telles que la LDA ou la LRFP. En fonction de leur secteur d'activité ou des prestations qu'elles fournissent, elles sont susceptibles d'engager leur responsabilité administrative en cas de manquements à des obligations légales. Elles sont dans tous les cas soumises à l'obligation de signaler les cyberattaques à l'OFCS. En cas de violation de cette obligation, elles peuvent engager leur responsabilité pénale. D'autres lois sont susceptibles d'imputer une responsabilité aux prestataires de gestion de cyberincidents, à l'instar de la LPD, qui sera analysée plus tard[1261].

699 Bien que certaines bases légales existent et s'appliquent à l'activité des prestataires de gestion de cyberincidents, l'on peut voir que seules peu d'organisations fournissant ce type de prestations sont soumises à des exigences de cybersécurité pour leurs activités. En outre, les bases légales applicables sont à nouveau très dispersées, dépendent des prestations concrètes, de la clientèle, du contrat et d'autres critères similaires. En revanche, les bases légales permettent dans de nombreux cas d'agir, mais uniquement *a posteriori*.

II. L'Office fédéral de la cybersécurité

A. Un contexte en mouvement

1. Le développement des fondements légaux

700 L'OFCS est l'autorité principale pour la cybersécurité en Suisse et exploite GovCERT, la CERT nationale suisse[1262]. L'activité de l'office est gouvernée par le principe de la légalité (art. 5 al. 1 Cst.)[1263]. Plusieurs dispositions constitutionnelles servent de fondements aux lois et ordonnances régissant l'activité de l'OFCS, à l'instar des art. 54 et 101 Cst. pour les affaires étrangères, art. 57 Cst. pour la sécurité, ou art. 102 al. 1 Cst. pour l'approvisionnement du pays[1264].

1261 Cf. *infra* N 843 ss, en particulier 927 ss.

1262 Au sujet de l'organisation de l'OFCS, de l'ancien NCSC et de GovCERT, cf. *supra* N 207 ss.

1263 Cf. *infra* N 1378 ss.

1264 CR Cst.-BLEICKER, art. 57 N 17 s. ; WEBER/WILLI, p. 146. La sécurité extérieure du pays se trouve notamment dans un rapport étroit avec les affaires étrangères et l'approvisionnement du pays, cf. CR Cst.-BLEICKER, art. 57 N 19. L'art. 104 Cst. prévoit spécifiquement,

701 Avant même la transformation du NCSC en OFCS, le NCSC hébergeait GovCERT, qui constituait déjà le service d'intervention en cas d'urgence informatique (art. 12 al. 1 litt. c aOPCy). L'aOPCy a servi de fondement à la création du NCSC et à la définition de son service, GovCERT. L'Ordonnance se basait d'une part sur la Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI), dont l'art. 30 prévoit que le CF est chargé d'édicter les dispositions d'exécution de la loi. D'autre part, l'aOPCy se fondait sur les art. 43 al. 2, 47 al. 3 et 55 de la Loi fédérale sur l'organisation du gouvernement et de l'administration (LOGA). L'aOPCy est entrée en vigueur en juillet 2020 et poursuivait notamment un objectif de centralisation des compétences, en prévoyant notamment la création du NCSC. Elle servait de fondement juridique à la création et au développement du NCSC tout en réglant les compétences et structures des autorités impliquées dans la protection de la Suisse contre les cyberrisques[1265].

702 La loi sur laquelle se fondent les activités de l'OFCS est maintenant la LSI, qui se fonde elle-même sur les art. 54 al. 1, 60 al. 1, 101, 102 al. 1 et 173 al. 1 et 2 Cst.[1266]. La LSI et ses ordonnances ont en partie repris et abrogé l'aOPCy (art. 50 OSI, Annexe 2 I OSI). Elles servent de bases légales pour l'activité du nouvel OFCS qui remplace le NCSC (art. 15a al. 1 Org-DDPS). Le nouvel art. 15*a* al. 2 litt. f Org-DDPS a été adopté avec la LSI. Il prévoit que l'OFCS gère l'équipe d'intervention pour aider les infrastructures critiques à se protéger contre les cybermenaces.

2. L'Office fédéral de la cybersécurité et son service technique

a. Les compétences générales pour la cybersécurité

703 L'OFCS, créé en janvier 2024, est l'autorité principale pour la cybersécurité. C'est à lui que revient les compétences de CERT nationale, qu'il exerce par le biais de son service technique, GovCERT. Les compétences de l'OFCS et de son unité technique étaient prévues de 2020 à 2023 à l'art. 12 aOPCy. Depuis janvier 2024, ces compétences sont prévues par l'art. 15*a* Org-DDPS, ainsi que par les art. 73*a* ss LSI2 dès que ces derniers entreront en vigueur[1267]. L'adoption de

dans le secteur de l'agriculture, la sécurité de l'approvisionnement, cf. art. 104 al. 1 litt. a Cst.

1265 DFF, *Erläuterungen zur Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung*, 2020, p. 2.

1266 Pour une analyse et une critique des fondements constitutionnels pour la LSI, cf. *infra*, N 1153 ss.

1267 L'OCyS devrait concrétiser la LSI2 et devrait entrer en vigueur en 2025 comme la seconde version de la loi.

bases légales était nécessaire, dans la mesure où une nouvelle unité administrative ne peut pas s'appuyer sur du droit en vigueur[1268].

L'art. 15*a* al. 1 Org-DDPS indique que l'OFCS est le NCSC. On peut y voir un manque de clarté juridique et de cohérence. On peut néanmoins comprendre l'intention derrière cette formulation, qui était de simplifier la rédaction de la loi[1269]. Partant, les art. 73*a* ss LSI2 qui mentionnent expressément le NCSC s'appliquent au nouvel OFCS[1270]. 704

L'OFCS constitue l'une des actrices techniques et opérationnelles tenues d'analyser les cybermenaces et de traiter les cyberincidents[1271]. Il analyse les logiciels malveillants et fournit les résultats. L'office publie des informations sur la situation de la cybermenace en Suisse, tient des statistiques à ce sujet et fournit des recommandations dans des cas concrets aux unités administratives, aux infrastructures critiques ainsi qu'aux entreprises et aux citoyennes confrontées à des cyberincidents (notamment art. 73*a* al. 2 litt. a et c LSI2)[1272]. L'OFCS informe également spécifiquement les infrastructures critiques pour les aider à mettre en place une protection appropriée de leurs systèmes et les sensibilise au sujet des cyberrisques (plus particulièrement art. 74 al. 2 litt. b et c LSI2)[1273]. En outre, il constitue un point de contact et de collaboration sur le plan national et sur le plan international[1274]. Son activité générale se concentre exclusivement sur la partie civile du réseau de la Confédération, à savoir sur les infrastructures critiques, les entreprises, la population et les autorités et organisations de l'administration[1275]. 705

Les art. 73*a* ss LSI2 confèrent à l'OFCS la mission d'exploiter le « guichet unique » suisse en matière de cyberrisques[1276]. Ce faisant, il réceptionne et traite les signalements concernant les différentes cybermenaces, y compris les cyberincidents, les vulnérabilités et les cyberattaques (art. 73*a* al. 2 litt. d, 706

1268 CF, *Plan de mise en œuvre de la SNPC 2018-2022*, 2019, p. 40.

1269 À ce sujet, cf. *infra* N 1381 ss.

1270 C'est pour cette raison que la présente étude se réfère à l'OFCS lorsqu'il est fait mention des art. 73*a* ss LSI2 et ce bien que la loi mentionne uniquement le NCSC.

1271 NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques*, 2022, p. 14 ; UPIC, *Rapport « évaluation de l'efficacité de la stratégie nationale de protection contre les cyberrisques (SNPC) »*, 2016, p. 29.

1272 Ce qui fait de lui un maillon particulièrement important pouvant fournir des informations cruciales pour la cybersécurité.

1273 FF 2017 2765, p. 2801.

1274 DDPS, *SNPC*, 2012, p. 16 ; SKOPIK/SETTANNI/FIEDLER, p. 156.

1275 SG-DDPS, *Législation d'exécution relative à la LSI, Explications*, 2023, p. 5 s.

1276 FF 2023 84, p. 26 ; CF, *Plan de mise en œuvre de la SNPC 2018-2022*, 2019, p. 40 ; compétence détenue auparavant par MELANI.

73*b* al. 1, 74a al. 1 LSI2 et art. 15*a* al. 2 litt. c Org-DDPS). Alors que les signalements de cybermenaces telles que les vulnérabilités et les cyberincidents (ainsi que les cyberattaques lorsqu'elles ne sont pas communiquées par des infrastructures critiques de l'art. 74*b* LSI2) peuvent être transmis par toute personne physique ou morale sur une base volontaire, le signalement des cyberattaques par les infrastructures critiques, faisant partie de la liste de l'art. 74*b* al. 1 LSI2, constitue une obligation imposée par la loi[1277].

707 L'office fédéral se tient, en pratique, à disposition de l'administration fédérale, des infrastructures critiques, des PME ainsi que de la population. Néanmoins, ses compétences ne sont pas les mêmes selon la destinataire de ses prestations. Les compétences de l'OFCS sont moindres lorsqu'il en va de la cybersécurité directe des PME ou de la population. Il collabore plus étroitement avec le réseau suisse d'infrastructures critiques, comprenant les membres du groupe fermé de clientes d'anciennement MELANI[1278]. Il les soutient dans leur protection contre les cybermenaces (art. 15*a* al. 2 litt. f Org-DDPS). Ce choix a d'ailleurs été critiqué politiquement et certaines personnes estiment que la Confédération devrait apporter un soutien plus étendu aux communes et aux PME, de la même manière que pour les infrastructures critiques[1279]. Le CF était contre une mainmise de la Confédération sur ces entités, partant du principe que la souveraineté cantonale serait gravement atteinte par une telle décision, de même que le principe de la responsabilité propre[1280].

708 L'OFCS est donc chargé d'apporter un soutien aux infrastructures critiques (art. 73*a* litt. e et 74 al. 1 LSI2)[1281]. Ce soutien est apporté par la mise à disposition d'un système de communication permettant l'échange sécurisé d'informations, d'informations techniques utiles de façon générale aux infrastructures critiques sur les cybermenaces en cours et de recommandations sur les mesures de prévention, ainsi que d'outils techniques et instructions de détection de cyberincidents (art. 74 al. 2 LSI2). En outre, il peut les conseiller et leur fournir de l'aide dans la gestion de cyberincidents et dans l'élimination de

1277 FF 2023 84, p. 26 et 32 ; NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques,* 2022, p. 14 ; RNS, *Recommandations de mise en œuvre des organisations cantonales pour la cybersécurité,* 2021, p. 14.

1278 Cf. *supra* N 210 s.

1279 Voir à ce sujet la Motion 21.4187 « Protéger nos PME et nos administrations publiques » déposée par Johanna Gapany le 30 septembre 2021.

1280 Voir l'avis du CF en réponse à la Motion 21.4187 « Protéger nos PME et nos administrations publiques contre les cyberattaques » déposée par Johanna Gapany le 30 septembre 2021.

1281 Art. 12 al. 1 litt. b aOPCy ; FF 2023 84, p. 30 s. ; GCSCC, *Cybersecurity Capacity Review,* p. 27.

vulnérabilités lorsque ces cybermenaces mettent en péril le fonctionnement de l'infrastructure critique (et, s'il s'agit d'une exploitante privée, qu'elle ne peut pas obtenir un soutien équivalent sur le marché assez rapidement) (art. 74 al. 3 LSI2)[1282]. Finalement, lorsqu'il prend connaissance d'une cyberattaque contre une infrastructure critique par le biais d'un signalement dûment effectué en vertu de l'art. 74a LSI2, l'OFCS doit aider l'infrastructure critique touchée à gérer une cyberattaque ; l'infrastructure critique soumise à l'obligation de signaler a droit au soutien de l'OFCS dans la gestion de la cyberattaque annoncée (art. 74a al. 3 LSI2). L'obligation de signaler les cyberattaques permet à l'OFCS d'avertir les potentielles lésées et leur recommander les mesures préventives et réactives s'imposant (art. 74*a* al. 4 LSI2)[1283]. Le soutien qu'il apporte aux infrastructures critiques passe en grande partie par son service, GovCERT (art. 15*a* al. 2 litt. f Org-DDPS).

709 Globalement, la loi octroie d'autres tâches à l'OFCS pour protéger la Suisse contre les cybermenaces, dont, conformément à l'art. 73*a* LSI2 et à l'art. 15*a* al. 2 Org-DDPS :

— la sensibilisation et l'alerte du public au sujet des cybermenaces ;
— l'alerte des autorités, des organisations et des personnes concernées lors de cybermenaces immédiates ou de cyberattaques en cours ;
— la mise en garde générale contre les cyberrisques et vulnérabilités pouvant impacter les moyens informatiques ;
— la publication d'informations et instructions en matière de cybersécurité et de protection contre les cyberrisques pouvant être intégrés aux dispositifs de protection individuels préexistants des entreprises ;
— les analyses techniques permettant d'évaluer et écarter les cybermenaces dans le cadre de la protection de la Suisse contre les cybermenaces[1284] ;
— la coordination des travaux de la Confédération dans le domaine de la cybersécurité ; et
— l'élaboration de la CSN à l'intention du CF et la coordination de sa mise en œuvre.

1282 FF 2023 84, p. 31.

1283 FF 2023 84, p. 33 ; NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques,* 2022, p. 9 ; MEYER/MÉTILLE, *Loi fédérale sur la sécurité de l'information : version 2.0,* 2022, N 38.

1284 NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques,* 2022, p. 16 ; MEYER/MÉTILLE, *Loi fédérale sur la sécurité de l'information : version 2.0,* 2022, N 35 ss. La liste de l'art. 73*a* n'est pas exhaustive, cf. FF 2023 84, p. 26.

b. Le service technique de l'office fédéral

710 L'aOPCy définissait GovCERT, son rôle et son rattachement au NCSC. Désormais, GovCERT et son rôle dans le soutien aux infrastructures critiques sont définis à l'art. 15*a* al. 2 litt. f Org-DDPS. L'art. 12 al. 1 litt. c aOPCy donnait une définition plus large de GovCERT que ce qui est maintenant prévu à l'art. 15*a* al. 2 litt. f Org-DDPS. L'aOPCy le définissait comme « le service spécialisé national pour la gestion technique des cyberincidents, l'analyse des questions techniques, l'évaluation technique des menaces et l'appui technique au guichet unique suisse ». L'Org-DDPS est moins exhaustive et se limite à prévoir que GovCERT est « l'équipe d'intervention en cas d'urgence informatique » gérée par l'OFCS lorsqu'elle aide les infrastructures critiques à se protéger contre les cybermenaces[1285]. Dans tous les cas, les compétences prévues à l'art. 12 al. 2 litt. c aOPCy sont conservées par l'OFCS. GovCERT constitue dans tous les cas un service de l'OFCS et seul ce dernier voit à l'heure actuelle son rôle concrétisé dans le cadre légal. Dans la mesure où l'OFCS a un pouvoir décisionnel (contrairement à GovCERT) et que GovCERT ne regroupe que les expertes techniques de l'OFCS, ce sont en réalité les compétences de l'OFCS qui nous intéressent ici, avec un accent sur la cybersécurité des infrastructures critiques et la gestion de cyberincidents les impactant[1286]. Dans ce contexte, l'OFCS détient des compétences importantes et, à l'interne de l'office, les collaboratrices de GovCERT, l'équipe d'intervention de l'OFCS, disposent de compétences pour le compte de l'OFCS en ce qui concerne les aspects techniques des missions de ce dernier.

711 L'OFCS dispose de nombreuses compétences, dont des compétences techniques. Les collaboratrices de son équipe, GovCERT, l'appuient dans ses tâches techniques, bien que ni la loi ni l'ordonnance ne le spécifient. GovCERT dispose de compétences techniques typiquement pour la mise à disposition d'instruments techniques et d'informations techniques auprès des infrastructures critiques (art. 74 al. 2 litt. b et c LSI2) ou encore dans le cadre du soutien fourni à ces dernières dans la gestion de cyberattaques ou de cyberincidents (respectivement art. 74a al. 3 LSI2 et 74 al. 3 LSI2).

1285 L'art. 7 P-OCyS prévoit les compétences de GovCERT, ce qui devrait aboutir à une définition à nouveau plus claire des compétences du service technique, OFCS, *Commentaire concernant l'OCyS*, 2024, p. 11.

1286 La présente étude ne va donc pas approfondir les questions relatives à d'autres compétences de l'OFCS, à l'instar de ses compétences de sensibilisation du grand public par des informations générales et non spécialement techniques sur les cybermenaces (art. 73*a* LSI2).

c. Les compétences liées à la sécurité de l'information

En parallèle des compétences prévues aux art. 73*a* ss LSI2, l'ordonnance relative à la première version de la loi prévoit les compétences du nouvel OFCS lorsque ses « clientes » sont des autorités ou des organisations de la Confédération. Tout d'abord, l'art. 43 OSI prévoit que l'OFCS fournit des conseils techniques et peut rechercher des menaces[1287]. Ensuite, l'OFCS conserve des compétences du NCSC jusqu'à ce que le service spécialisé de la Confédération pour la sécurité de l'information reprenne ces fonctions en 2025 (art. 51 al. 6 OSI). Il en va typiquement des compétences d'édicter des directives pour la sécurité des moyens informatiques ou pour la sécurité de l'information (art. 15, art. 27 al. 7 ou art. 29 al. 1 OSI). 712

L'OFCS devrait continuer d'assumer ces tâches d'autoprotection de la Confédération jusqu'en 2025, date à laquelle le service spécialisé de la Confédération pour la sécurité de l'information sera opérationnel[1288]. Certaines de ces tâches revenant à partir de 2025 au service spécialisé de la Confédération pour la sécurité de l'information comportent une dimension technique importante. 713

Nous allons développer les compétences de l'OFCS selon un fonctionnement similaire à celui utilisé pour les autres prestataires de gestion de cyberincidents. Une distinction sera d'abord opérée entre les compétences proactives et réactives. En parallèle, ses compétences de gestion de la qualité de la sécurité et de gestion des vulnérabilités seront parcourues. 714

B. L'office fédéral et la cybersécurité des infrastructures critiques

1. Ses compétences préventives et de gestion de la qualité de la sécurité

Une CERT nationale peut être amenée à fournir des prestations préventives comme des compétences de gestion de la qualité de la sécurité. Certaines de ces prestations peuvent revêtir tant un caractère préventif que de gestion de la qualité de la sécurité. À ce titre, l'OFCS (en partie par son unité, GovCERT) sensibilise sa communauté de clientes. La sensibilisation permet la préparation de sa communauté à des attaques et incidents, et l'amélioration de la qualité de la sécurité générale de celle-ci. La sensibilisation du grand public au sujet des cybermenaces (art. 73*a* al. 2 litt. a LSI2) fait partie des compétences incombant à l'OFCS, de même que la publication d'informations sur la cybersécurité et d'instructions sur les mesures à prendre pour se protéger de façon préventive et réactive contre les cybermenaces (art. 73*a* litt. c LSI2). 715

1287 SG-DDPS, *Législation d'exécution relative à la LSI, Explications*, 2023, p. 25.

1288 SG-DDPS, *Législation d'exécution relative à la LSI, Explications*, 2023, p. 6.

716 Outre ces annonces, l'OFCS peut effectuer des veilles technologiques. L'OFCS veille à l'évolution de la science, des menaces et des politiques ainsi que des réglementations[1289]. L'autorité procède à des analyses techniques des cybermenaces afin de partager avec différents groupes cibles des informations relatives à la cybersécurité. Ces informations permettent de donner des avertissements anticipés sur des cybermenaces à sa communauté. L'unité technique, GovCERT, publiait déjà, avant la création de l'OFCS, des informations à l'instar de statistiques et de tendances à l'attention. Ces informations sont toujours accessibles, en particulier pour les professionnelles de cybersécurité[1290].

717 En principe, la détection de cyberincidents ne se fait pas par l'OFCS, mais les cyberincidents sont portés à sa connaissance par la suite. Certaines CERT nationales développent et utilisent des outils de détection. L'OFCS pourrait, à la lecture de son mandat, détenir de telles compétences, en tout cas pour les infrastructures critiques (art. 74 al. 2 litt. c LSI2)[1291].

2. Ses compétences réactives

a. Une remarque introductive

718 La gestion de cyberincidents représente le cœur de l'activité des autres CERT et CSIRT[1292]. L'OFCS détient une multitude de compétences différentes, dont des compétences de gestion de cyberincidents dans lesquelles il est épaulé par son équipe technique, GovCERT. De la même façon que pour les CSIRT, la réponse stricte aux incidents débute avec la réception du rapport d'incident. L'OFCS comptant en son sein le guichet unique suisse en matière de cybermenaces, c'est une fois une notification parvenue qu'il peut fournir son soutien technique. À noter qu'un canal plus spécifique existe pour permettre aux expertes en cybersécurité de signaler directement à GovCERT des cyberincidents[1293]. Dans ce cadre, GovCERT est ensuite amenée à analyser, pour le

1289 Sur ce type de tâches, cf. KILLCRECE et al., *Organisational Models for CSIRT,* 2003, p. 20 et 120.

1290 Concernant la diffusion d'informations relatives à la sécurité, cf. GOVCERT, *Blog and White papers* ; KILLCRECE et al., *Organisational Models for CSIRT,* 2003, p. 120 ; WESTBROWN et al., p. 32. Au sujet de la circonscription de CERT nationales ou gouvernementales, voir ENISA, *Baseline Capabilities of National/Governmental CERT, Part 2,* 2010, p. 33. Parmi les informations partagées par GovCERT peut également figurer de la documentation basée sur des attaques passées, voir par exemple MELANI/GovCERT, *APT Case RUAG,* 2016, où GovCERT publie des recommandations basées sur les leçons tirées d'une attaque ayant affecté RUAG.

1291 MORGUS et al., *National CSIRT and Their Role in Computer Security Incident Response,* 2015, p. 18.

1292 Pour des explications générales sur les compétences réactives des prestataires de gestion de cyberincidents, cf. *supra* N 296 ss.

1293 Voir notamment GOVCERT, *Contacts, Reports on cyberincidents from critical infrastructures* ; KILLCRECE et al., *Organisational Models for CSIRT,* 2003, p. 116.

compte de l'OFCS, les incidents, des artéfacts ou des nouveaux logiciels malveillants[1294]. Au-delà de la réponse aux cyberincidents et comme nous le verrons, l'OFCS et son service technique peuvent être amenés à analyser des vulnérabilités également (comme découlant implicitement de l'art. 73*b* LSI2)[1295].

b. Les recherches passives

(i) Après le signalement d'un cyberincident ou d'une cyberattaque

Lorsqu'un cyberincident est signalé à l'OFCS, il l'analyse afin de déterminer son importance pour la protection de la Suisse contre les cybermenaces. Si la personne effectuant le signalement le demande, il peut émettre une recommandation relative aux mesures à prendre, pour autant que la situation ne nécessite pas d'analyses ou de clarifications supplémentaires (art. 73*b* al. 2 LSI2)[1296]. Cette formulation n'étant pas parfaitement claire, il est difficile de savoir dans quels cas l'OFCS émet ou non une recommandation, même si l'on peut supposer qu'il s'agit en tout cas d'une réserve lui permettant d'agir compte tenu de ses ressources. L'office peut en parallèle publier les informations aux conditions de l'art. 73*d* LSI2[1297]. 719

Contrairement à la suite donnée aux signalements de cyberincidents émanant de PME ou de la population, l'OFCS fournit des conseils et de l'aide dans la gestion technique de cyberincidents signalés par une infrastructure critique si le cyberincident en question met en péril le fonctionnement de l'infrastructure concernée. En outre, si l'infrastructure critique est une organisation privée, l'office n'intervient que s'il est impossible d'obtenir un soutien équivalent sur le marché en temps utile (art. 74 al. 3 LSI2). Son soutien est donc subsidiaire, surtout lorsqu'il est apporté à une organisation privée[1298]. 720

Lorsqu'une infrastructure critique signale une cyberattaque conformément à son obligation des art. 74*a* ss LSI2, elle a droit au soutien de l'OFCS et de ses services (art. 74*a* al. 3 LSI2)[1299]. Lorsqu'une cyberattaque est signalée par une infrastructure critique de l'art. 74*b* LSI2 à l'OFCS, l'OFCS cherche à en avertir les victimes potentielles, recommande des mesures de prévention et 721

1294 ENISA, *Baseline Capabilities of National/Governmental CERT, Part 2,* 2010, p. 22. Pour la définition des artéfacts, cf. *supra* N 303.

1295 Cf. notamment GOVCERT, *Exchange Vulnerability 2021* ; ENISA, *Baseline Capabilities of National/Governmental CERT, Part 2,* 2010, p. 22 ; KILLCRECE et al., *Organisational Models for CSIRT,* 2003, p. 120.

1296 FF 2023 84, p. 26 s.

1297 FF 2023 84, p. 27 s.

1298 FF 2023 84, p. 31 ; NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques*, 2022, p. 16.

1299 FF 2023 84, p. 31 s.

de défense qui s'imposent et, surtout, tente d'identifier des modes opératoires (art. 74*a* al. 4 LSI2). Cette formulation nous laisse penser que ses compétences ne se limitent pas à fournir des conseils à l'organisation, mais elles consistent en réalité aussi en l'apport d'un soutien technique concret[1300]. La responsabilité propre des infrastructures critiques doit être respectée, ce qui implique que l'OFCS ne leur apporte qu'un soutien subsidiaire (surtout lorsqu'il s'agit d'une organisation privée). Il ne peut pas être le permier responsable de la réaction à un incident et du rétablissement du bon fonctionnement des opérations, bien qu'il fournisse un soutien pour maintenir et rétablir la sécurité de l'information après un incident[1301]. L'aide concrète fournie dépend des capacités de l'entité affectée.

(ii) Les mesures concrètes

722 L'OFCS peut, à la suite des signalements de cyberincidents ou de cyberattaques par des infrastructures critiques, effectuer des analyses. Il peut émettre une recommandation en vertu de l'art. 73*b* al. 2 LSI2 pour un cyberincident et de l'art. 74*a* al. 4 LSI2 pour une cyberattaque.

723 Parfois, les analyses et les mesures de soutien technique entreprises par l'OFCS vont plus loin. Son soutien va plus loin lorsqu'un cyberincident touche une infrastructure critique et met en danger le fonctionnement de cette dernière (art. 74 al. 3 LSI2). Si l'infrastructure critique est une organisation privée, il faut en outre qu'elle ne puisse pas obtenir un soutien équivalent sur le marché en temps utile (art. 74 al. 3 in fine LSI2). Dans ce cas de figure, le soutien, notamment technique, apporté par l'OFCS, ne constitue qu'une mesure d'urgence. Les mesures plus étendues, visant notamment à rétablir la cybersécurité en général, restent du ressort de l'infrastructure concernée[1302]. L'OFCS peut également aller plus loin dans son soutien à une infrastructure critique lui signalant une cyberattaque conformément à son obligation des art. 74*a* ss LSI2, cas dans lequel cette dernière a droit au soutien technique (art. 74*a* al. 3 LSI2)[1303].

724 L'aide concrète fournie par l'OFCS dépend des capacités de l'entité affectée et elle est fournie principalement lorsque l'organisation signalant la cyber-

1300 La protection des infrastructures d'information critiques peut effectivement faire partie de ses responsabilités, cf. ENISA, *Baseline Capabilities of National/Governmental CERT, Part 2,* 2010, p. 21.

1301 FF 2017 2765, p. 2870 ; FF 2023 84, p. 31 ; CF, *Rapport « La politique de sécurité de la Suisse »,* 2021, p. 26.

1302 FF 2023 84, p. 31.

1303 Lorsque les capacités et les ressources de l'OFCS sont limitées, il fournit son soutien en priorité à l'infrastructure critique confrontée à une cyberattaque devant être signalée, cf. FF 2023 84, p. 33.

attaque dispose de ressources limitées[1304]. Il peut par exemple procéder à l'analyse d'un logiciel malveillant et d'artéfacts ou à des analyses forensiques, puis fournir des recommandations sur les mesures techniques concrètes à prendre afin de prévenir des dangers ou détecter des cyberincidents[1305]. L'analyse effectuée par l'office est en principe plus superficielle que celle menée par la prestataire de gestion de cyberincidents de l'organisation affectée. Son soutien est effectivement subsidiaire et l'autonomie des infrastructures critiques doit être garantie, ce qui implique que le nouvel office ne devrait pas être la première personne responsable de la réaction à un cyberincident et du rétablissement du bon fonctionnement des opérations, bien qu'elle fournisse un soutien pour maintenir et rétablir la sécurité à la suite d'un cyberincident.

Pour donner quelques exemples d'analyses, les spécialistes techniques 725
engagées par l'OFCS peuvent utiliser des techniques de rétro-ingénierie pour tenter de comprendre le fonctionnement d'un logiciel malveillant, son développement ou la stratégie et les étapes de l'intrusion d'une personne dans un système. L'autorité peut aussi simuler sur des ressources des moyens informatiques vulnérables *(honeypots*[1306]*)* pour comprendre et analyser les comportements des logiciels malveillants et des auteures de cyberattaque, mais aussi pour améliorer leurs connaissances et neutraliser une attaquante[1307]. Elle peut mettre en place un gouffre DNS *(DNS sinkhole)*[1308] et requérir du registre que ce dernier redirige le trafic Internet vers un outil d'analyse ou vers une page d'informations (art. 15*a* al. 1 ODI). Ce faisant, l'OFCS peut collecter et analyser les données pour les noms de domaine suisses, identifier les appareils infectés et en informer les propriétaires par l'intermédiaire de leur fournisseuse d'accès (art. 15 al. 2 ODI)[1309]. À noter que les analyses de l'office visent souvent la corrélation entre les informations provenant de diverses sources au sein du cercle d'organisations qu'elle sert[1310].

L'OFCS ne dispose en pratique pas de la même autorité envers toutes les 726
infrastructures critiques. Alors qu'il semble détenir une autorité partagée avec

1304 FF 2017 2765, p. 2870 ; CF, *Rapport « La politique de sécurité de la Suisse »*, 2021, p. 26.

1305 FF 2017 2765, p. 2869 ; KILLCRECE et al., *Organisational Models for CSIRT,* 2003, p. 118. Sur l'analyse forensique, d'incidents et d'artéfacts, cf. *supra* N 300 ss.

1306 Les *honeypots* et autres leurres sont mis en place pour attirer des auteures malveillantes et détourner leurs attaques contre les systèmes de l'organisation. Une attention doit être portée sur l'isolation utilisée avec ceux-ci pour éviter que le code malveillant dévié n'infecte les systèmes informatiques de l'organisation, NIST, 800-53, rev. 5, SC-26, p. 316 ; ILG et al., p. 2 ss.

1307 FF 2017 2765, p. 2869.

1308 Sur cette méthode, cf. ENISA, *DNS Sinkhole*.

1309 NCSC, *Rapport semestriel 2021/1,* 2021, p. 21 s.

1310 KILLCRECE et al., *Organisational Models for CSIRT,* 2003, p. 117.

l'administration fédérale, tel n'est pas le cas en rapport avec les autres infrastructures critiques, avec lesquelles ses compétences sont plus limitées. Outre les conseils de cybersécurité que l'office peut apporter aux unités administratives et aux départements qui se confrontent à un incident ou à une faille de sécurité (art. 12 al. 3 OSI)[1311], il est susceptible d'aller plus loin avec ces autorités dans certains cas. Lorsqu'une autorité de la Confédération est affectée par un cyberincident critique (art. 12 al. 5 OSI), le service spécialisé de la Confédération pour la sécurité de l'information peut diriger les opérations de gestion de cyberincidents ou en déléguer la direction à l'OFCS, tout cela avec l'accord de l'unité administrative ou du département (art. 12 al. 7 OSI). Dans ce cas, l'OFCS peut ordonner la prise de mesures immédiates (art. 12 al. 7 litt. b OSI)[1312]. Il peut typiquement ordonner l'arrêt d'un système. Néanmoins, il est probable que cette situation soit en pratique évitée afin de conserver l'intégrité des relations de confiance liant l'office à l'administration fédérale. Si une infrastructure critique affectée est externe à l'administration fédérale, l'OFCS se limiterait à conseiller l'arrêt du système.

727 Outre les analyses et recommandations de l'OFCS et de son équipe technique de gestion de cyberincidents, le nouvel office a d'autres possibilités d'action prévues légalement[1313]. Dans certains cas concrets, des bases légales spéciales servent de fondement aux compétences réactives de l'ancien NCSC et, partant, du nouvel OFCS. Ce dernier peut par exemple détenir des compétences découlant de l'Ordonnance sur les domaines Internet (ODI), qui régit les noms de domaine suisse[1314]. L'ODI confère notamment à l'OFCOM certaines compétences générales en ce qui concerne ces noms de domaine (art. 4 al. 1 ODI). Parmi ses compétences, l'OFCOM peut prendre plusieurs mesures en cas de soupçon d'abus, dont fait partie le blocage d'un nom de domaine. Les services de lutte contre la cybercriminalité reconnus par l'OFCOM, dont le NCSC, peuvent également exiger un tel blocage (art. 15 al. 3 ODI). L'OFCS devrait donc pouvoir, en tant qu'unité reconnue de lutte contre la cybercriminalité et sur la base de l'art. 15 al. 3 ODI, requérir du registre le blocage technique et administratif pendant 30 jours d'un nom de domaine, s'il existe des soupçons portant sur une utilisation abusive d'un nom de domaine[1315]. Par

1311 SG-DDPS, *Législation d'exécution relative à la LSI, Explications,* 2023, p. 14.

1312 SG-DDPS, *Législation d'exécution relative à la LSI, Explications,* 2023, p. 14 s.

1313 En tant que service d'une autorité, la loi peut lui attribuer d'autres compétences en comparaison avec une équipe privée de gestion de cyberincidents.

1314 MÉTILLE, *Internet et droit,* 2017, p. 31 s.

1315 MEYER/MÉTILLE, *Computer security incident response teams : are they legally regulated ? The Swiss example,* 2022, p. 52 ; OFCOM, *Lutte contre la cybercriminalité* pour les services reconnus de lutte contre la cybercriminalité selon l'art. 15 al. 3 ODI.

utilisation abusive, l'on entend notamment l'utilisation d'un nom de domaine pour accéder par des moyens illicites à des données critiques ou la diffusion de logiciels malveillants[1316]. Si le NCSC, devenu l'OFCS, le requiert, le domaine doit être bloqué, mesure qui consiste en la « déconnection » d'un domaine Internet, ainsi que de tous les sites rattachés et qui mettent le réseau en danger[1317]. La nature provisoire de cette mesure se justifie par le fait que l'intervention ne se fonde que sur un soupçon du service compétent et reconnu et que ce dernier n'a pas de compétence décisionnelle en vertu de la loi. Les cas dans lesquels les services de lutte contre la cybercriminalité reconnus peuvent agir sont limités, comme pour les autres services spécialisés[1318].

L'OFCS détient finalement aussi des compétences post-cyberincidents. 728
Il en va typiquement du partage de bonnes pratiques ou de leçons tirées de la gestion d'incidents. L'autorité publie en effet des documents dans ce cadre[1319].

c. Une surveillance active ?

La question de la surveillance active revient à poser celle du contre-hacking, 729
du *hack back* ou *counterhacking,* impliquant une intrusion dans le système de la personne s'étant initialement infiltrée indûment. La pratique du *hack back* soulève plusieurs questions juridiques. Pour répondre à la question de son utilité pour l'OFCS, il convient de survoler les objectifs poursuivis par celui-ci et faire un parallèle avec les intérêts d'autres autorités. L'OFCS a comme mission de protéger des réseaux et des systèmes ainsi que de rétablir au plus vite une situation sûre[1320]. En théorie, le fait de pouvoir s'introduire chez une intruse pour perturber le fonctionnement de sa machine et ainsi la neutraliser pourrait sembler être une démarche intéressante. Il n'en demeure pas moins qu'il s'agit là d'une démarche difficile, longue et fastidieuse. Partant et dans la mesure où l'office fédéral cherche à répondre au plus vite, à savoir dans les premières heures, à un incident, le contre-hacking n'est que rarement et à raison une solution à privilégier par cette autorité, en raison notamment du temps que cette pratique nécessite[1321]. En outre, ce type de compétence ne vise pas en premier lieu le rétablissement d'une situation sûre, mais la perturbation

1316 OFCOM, *Révision de l'ODI,* 2017, p. 2.

1317 MÉTILLE, *Internet et droit,* 2017, p. 34.

1318 OFCOM, *Révision de l'ODI,* 2017, p. 20.

1319 Cf. notamment MELANI/GovCERT, *APT Case RUAG*, 2016.

1320 Cf. notamment MORGUS et al., *National CSIRT and Their Role in Computer Security Incident Response,* 2015, p. 13.

1321 Elle pourrait en revanche être intéressante dans le cas où une attaque n'a pas encore été perpétrée.

du système de l'attaquante. Ces compétences sont davantage susceptibles de tomber dans la sphère de compétence d'autorités telles que le SRC[1322].

3. L'office fédéral comme point de contact

a. Les flux de données généraux

730 L'OFCS, exploitant la CERT gouvernementale, détient des compétences de coordination, car son cercle de bénéficiaires est étendu et diversifié[1323]. Ses compétences de point de contact dépassent la réponse proprement dite aux cyberincidents[1324]. En dehors des échanges dans le cadre des cyberincidents et des cyberattaques visant les infrastructures critiques, l'office reçoit des signalements au sujet de cyberincidents en provenance des PME et de la population (art. 73*a* litt. d et 73*b* al. 1 LSI2)[1325]. L'OFCS participe également à la sensibilisation du grand public (art. 73*a* al. 2 litt. a LSI2). Finalement, il sert de point de contact en collaborant sur le plan national et sur le plan international, en étant l'autorité la mieux placée pour, par exemple, échanger des informations avec des CERT et CSIRT de l'étranger[1326].

731 Beaucoup d'organisations, dont des infrastructures critiques, disposent aujourd'hui de prestataires de gestion de cyberincidents propres[1327]. L'OFCS n'est donc pas systématiquement contactée pour tout cyberincident. En outre, les cyberattaques qui ne réunissent pas les conditions de l'art. 74*d* LSI2 ne seront probablement pas toutes portées à la connaissance du nouvel office. Lorsque l'OFCS en prend connaissance, il collecte et enregistre des données pour les diffuser au sein de sa communauté, permettant ainsi de mieux identifier les cybermenaces, faciliter un échange sûr d'informations et d'interactions pour la réponse aux cyberincidents, mieux identifier ces derniers, mieux cerner de nouvelles menaces et élaborer des stratégies plus adaptées

1322 Cf. *supra* N 243 ss et 592 ss ; CF, *CSN*, 2023, p. 27. Dans la mesure où le SRC détient déjà certaines compétences de défense active, il n'est pas certain qu'un développement de cette activité soit réellement souhaitable, à défaut d'une étude traitant spécifiquement de la question.

1323 ENISA, *NCSS Good Practice Guide*, 2016, p. 32 ; KILLCRECE et al., *Organisational Models for CSIRT*, 2003, p. 114.

1324 À titre d'exemple de compétences de coordination hors réponse aux incidents, GovCERT peut être amenée à coordonner la gestion de vulnérabilités ou d'artéfacts, cf. KILLCRECE et al., *Organisational Models for CSIRT*, 2003, p. 119 ; WESTBROWN et al., p. 62.

1325 NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques*, 2022, p. 14.

1326 ENISA, *Baseline Capabilities of National/Governmental CERT, Part 2*, 2010, p. 20.

1327 CF, *CSN*, 2023, p. 24.

à celles-ci (notamment dans le cadre de ses compétences figurant aux art. 73*b* al. 2 et art. 74 LSI2)[1328]. Il constitue un point de contact à privilégier pour échanger sur les bonnes stratégies de réponse au sein de sa communauté. Il permet aux infrastructures critiques d'échanger en toute sécurité par le biais d'une plate-forme sûre d'échange d'informations (art. 74 al. 2 litt. a LSI2)[1329]. En effet, les dangers, menaces et vulnérabilités représentent souvent un objectif commun à plusieurs secteurs critiques, si ce n'est à tous[1330]. L'OFCS détient parmi ses compétences celle d'encourager l'échange d'informations entre les infrastructures critiques[1331]. Au-delà des échanges entre l'office et la communauté qu'il sert, ce dernier échange également avec d'autres actrices, à l'instar des autorités d'application de la loi, avec lesquelles la coopération est censée être bidirectionnelle[1332]. Il collabore aussi avec des services disposant de compétences similaires aux siennes, sur le plan national comme international, et avec d'autres autorités et organisations.

b. Le partage d'informations avec les infrastructures critiques

Il est naturel que l'OFCS échange avec les infrastructures critiques qu'il soutient, par la diffusion d'informations proactives, par des échanges d'informations à la suite de la détection d'un incident ou par le partage d'informations générales diffusées pour sensibiliser[1333]. Les organisations soutenues par l'OFCS disposant souvent d'une prestataire de gestion de cyberincidents, en externe ou en interne, c'est souvent cette dernière qui sert d'interlocutrice privilégiée à l'office et à son équipe technique[1334]. 732

Dans le cadre du soutien apporté aux infrastructures critiques (art. 73*a* litt. f et 74 LSI2), l'OFCS transmet aux infrastructures critiques des informations ayant une portée préventive. Pour ce faire, il partage avec elles des informations techniques sur les cybermenaces et sur les vulnérabilités connues, ainsi que des recommandations sur les mesures de prévention (art. 74 al. 2 litt. b LSI2). Il est important que l'office fédéral puisse transmettre des alertes ou avertissements à ses clientes lorsqu'une menace lui est connue[1335]. Cette 733

1328 KILLCRECE et al., *Organisational Models for CSIRT,* 2003, p. 118.

1329 FF 2017 2765, p. 2780 ; FF 2023 84, p. 30 ; KILLCRECE et al., *Organisational Models for CSIRT,* 2003, p. 118 s. Voir, par exemple, MELANI-NET, cf. *infra* N 338.

1330 FF 2017 2765, p. 2870.

1331 Voir les art. 12 al. 1 litt. b aOPCy et 74 al. 4 LSI2.

1332 ENISA, *Baseline Capabilities of National/Governmental CERT, Part 2,* 2010, p. 35.

1333 À ce sujet, voir ENISA, *Baseline Capabilities of National/Governmental CERT, Part 2,* 2010, p. 33.

1334 KILLCRECE et al., *Organisational Models for CSIRT,* 2003, p. 118.

1335 KILLCRECE et al., *Organisational Models for CSIRT,* 2003, p. 117.

information se limite toutefois aux éléments susceptibles d'être utiles aux infrastructures critiques en général et ne consiste pas en des conseils personnalisés destinés aux entreprises[1336]. Il transmet également des informations relatives aux mesures réactives à prendre ainsi que des outils techniques et des instructions de détection de cyberincidents adaptées aux besoins des infrastructures critiques (art. 74 al. 2 litt. b et c LSI2)[1337]. Ces instruments sont conçus soit pour l'ensemble des infrastructures critiques, soit pour certains groupes plus spécifiques[1338].

734 Des échanges d'informations ont naturellement lieu dans le contexte des signalements de cyberincidents[1339]. Tout d'abord et par le signalement d'une cyberattaque, l'organisation affectée fournit les informations de l'art. 74*e* al. 2 LSI2 à l'OFCS par l'intermédiaire du guichet unique suisse en matière de cybermenaces[1340]. Les informations partagées portent sur l'infrastructure critique visée par la cyberattaque, sur le type de cyberattaque subie, sur son déroulement et ses conséquences ainsi que sur les mesures que prend ou compte prendre l'organisation (art. 74*e* al. 2 LSI2), informations qu'elle peut, si nécessaire, transmettre de façon échelonnée en vertu de l'art. 74*e* al. 3 LSI2[1341].

735 Lorsqu'une infrastructure critique est confrontée à un cyberincident et qu'elle y autorise l'OFCS, ce dernier peut accéder aux informations et aux moyens informatiques de l'organisation pour analyser l'incident, le gérer ou limiter les dommages (art. 74 al. 4 LSI2). Dans ce contexte, l'autorité émet à l'attention des spécialistes informatiques de l'infrastructure critique concernée des recommandations sur les indicateurs à rechercher au sein des systèmes[1342]. Les infrastructures critiques peuvent transmettre à l'OFCS les données personnelles utiles à leur protection contre les cybermenaces (art. 76

1336 FF 2023 84, p. 30 s. ; NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques*, 2022, p. 16.

1337 L'OCyS devrait préciser les échanges d'informations permis par les systèmes exploités par l'OFCS, cf. art. 11 ss P-OCyS.

1338 FF 2023 84, p. 31 ; NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques*, 2022, p. 16.

1339 MEYER/MÉTILLE, *Computer security incident response teams : are they legally regulated ? The Swiss example*, 2022, p. 52.

1340 FF 2023 84, p. 26.

1341 FF 2023 84, p. 44 ; NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques*, 2022, p. 21. À noter qu'en vertu de l'art. 74*e* al. 3 LSI2, la personne qui assume l'obligation de signaler n'est pas tenue de fournir des informations qui l'exposent à des poursuites pénales.

1342 FF 2023 84, p. 31 s.

al. 2 LSI2)[1343]. Ces données sont souvent liées aux cybermenaces, aux cyberincidents aux services qu'elles fournissent ainsi qu'à leurs activités[1344].

736 L'office transmet aux infrastructures critiques des informations par le biais de son soutien technique ainsi que des recommandations qu'elle peut émettre en général ou dans des situations de cyberincidents et de cyberattaques. Dans ces situations, il indique aux infrastructures critiques affectées les mesures qui s'imposent (art. 74*a* al. 4 LSI2). Il est habilité, comme les infrastructures critiques, à communiquer à ces dernières les données personnelles lorsque cela s'avère nécessaire pour la protection contre les cybermenaces (art. 76 al. 1 LSI2)[1345].

737 Une particularité dans les communications entre l'OFCS et sa communauté concerne les fournisseuses de services de télécommunication. Ces dernières détiennent une double casquette. La première est celle d'infrastructure critique et la seconde est liée à leur activité. Les services d'accès à Internet (*Internet service providers,* ISPs) sont inclus dans le sous-secteur critique des télécommunications et détiennent un rôle supplémentaire en rapport aux cyberincidents, dans la mesure où la quasi-totalité des autres infrastructures critiques repose sur leur bon fonctionnement. Leur coopération est essentielle pour que les cyberincidents puissent être gérés au niveau national[1346]. Dans le cadre de cette coopération, des données personnelles et des ressources d'adressage peuvent être communiquées entre les fournisseuses de services de télécommunication et l'office fédéral pour la cybersécurité, à condition que la communication soit « nécessaire à la protection contre les cybermenaces » (art. 76 al. 2 LSI2)[1347]. Par exemple, si un serveur de commande grâce auquel un réseau de machines zombies est exploité est découvert, des fichiers

1343 Selon la LSI dans sa première version actuellement en vigueur, les infrastructures critiques peuvent communiquer à l'OFCS des données, notamment personnelles, liées à des incidents (art. 76 al. 3 LSI).

1344 FF 2017 2765, p. 2872 s. ; FF 2023 84, p. 50.

1345 La première version de la LSI prévoit que des services comme l'OFCS peuvent communiquer des informations dont des données personnelles aux infrastructures critiques si ces communications sont nécessaires à la sécurité de celles-ci (art. 76 al. 2 LSI).

1346 FF 2018 491, p. 499 ; ENISA, *Baseline Capabilities of National/Governmental CERT, Part 2,* 2010, p. 34 ; OAS, *Best Practices National CSIRT,* 2016, p. 18 s. ; WEST-BROWN et al., p. 62.

1347 Jusqu'à l'entrée en vigueur de la LSI révisée, l'OFCS peut leur communiquer les informations « utile à la sécurité de l'information » (art. 76 al. 2 LSI). Les fournisseuses de services de télécommunication peuvent lui communiquer des informations, notamment des données personnelles en vertu de l'art. 76 al. 3 LSI, qui ne précise pas de motif et est donc plus large que l'art. 76 al. 2 LSI2. En outre, l'actuel art. 76 al. 2 et 3 LSI prévoit que les communications peuvent se faire non pas uniquement entre l'OFCS et les fournisseuses de services de télécommunication, mais également avec les « fournisseurs de services informatiques ».

journaux contenant les adresses IP des ordinateurs infectés pourraient être transmis par l'hébergeuse à l'OFCS, qui pourrait alors les remettre aux fournisseuses de services de télécommunication pour que ces dernières avertissent leurs clientes. L'hébergeuse pourrait également livrer à l'office les données de configuration des modèles de communication du serveur de commande pour éventuellement trouver d'autres réseaux de machines zombies[1348].

738 Finalement, l'OFCS met à disposition de sa communauté d'infrastructures critiques un système de communication permettant l'échange sécurisé d'informations (art. 74 al. 2 litt. a LSI2). Ce système sert à l'échange d'informations (constituant potentiellement des données personnelles) principalement sur les menaces et dangers, sur des consignes concernant l'identification et la réponse techniques aux incidents, sur l'analyse d'incidents ou de vulnérabilités, et sur des recommandations[1349]. Il est crucial que la collaboration entre infrastructures critiques se poursuive[1350].

c. La collaboration avec les autorités de poursuite pénale

739 Alors que l'OFCS a notamment pour missions de prévenir les cyberincidents et, lorsque ceux-ci ont lieu, de les analyser et de prendre les bonnes mesures pour les éradiquer, les autorités de poursuite pénale ont des compétences différentes. Elles doivent investiguer lorsqu'elles suspectent la réalisation d'infractions pénales, identifier les individus à l'origine d'attaques et réduire le nombre d'attaques réussies. L'OFCS, lui, priorise le rétablissement de systèmes et l'amélioration de leur résilience, alors que l'autorité de poursuite pénale cherche principalement l'attribution des attaques et la poursuite pénale des délinquantes[1351]. Les cyberincidents n'impliquent pas toujours un caractère pénal, mais si c'est le cas, l'office pour la cybersécurité peut faire partie des premières entités à intervenir et elle est susceptible d'analyser les systèmes affectés et de partager les informations, notamment avec les autorités de poursuite pénale[1352].

740 La question de la collaboration est bidirectionnelle. La collaboration devrait servir à la transmission d'informations de l'OFCS aux autorités de

1348 FF 2017 2765, p. 2873 ; MEYER/MÉTILLE, *Computer security incident response teams : are they legally regulated ? The Swiss example,* 2022, p. 53.

1349 FF 2023 84, p. 30 ss.

1350 CF, *Rapport « La politique de sécurité de la Suisse »,* 2021, p. 36. Ce système de coopération avait selon le NCSC bien fait ses preuves via MELANI, NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques,* 2022, p. 16.

1351 MORGUS et al., *National CSIRT and Their Role in Computer Security Incident Response,* 2015, p. 13.

1352 ENISA, *Baseline Capabilities of National/Governmental CERT, Part 2,* 2010, p. 35 ; ENISA, *Roadmap on the cooperation between CSIRT and LE,* 2019, p. 19.

poursuite pénale et inversement. Les autorités de poursuite pénale peuvent bénéficier de certaines informations précieuses détenues par l'office grâce à son activité[1353]. En outre, ce dernier peut être à l'origine, dans certaines circonstances, d'une saisie des autorités de poursuite pénale compétentes lorsque des activités délictuelles sont mêlées à un cyberincident dont elle a connaissance.

741 L'OFCS dispose d'informations particulièrement utiles aux missions des autorités de poursuite pénale. Il leur octroie, par le biais d'une procédure d'appel, l'accès aux informations renseignant sur l'identité et le mode opératoire des auteures de cyberattaques à celles-ci (art. 76*a* al. 3 LSI2). Il leur met à disposition les informations au sujet des délinquantes et de leurs méthodes. Il peut s'agir de données purement techniques, ayant notamment trait aux modes opératoires ou aux valeurs de hachage des logiciels malveillants, ou de données personnelles, comme des ressources d'adressage (comme l'adresse IP) ou des informations relatives à des transactions financières (à l'instar d'un numéro de compte bancaire) permettant d'établir un lien avec des personnes spécifiques[1354].

742 Lorsque des informations sont obtenues dans le cadre de signalements, les collaboratrices de l'OFCS, ne sont pas soumises à l'obligation de dénoncer de l'art. 22*a* de la Loi sur le personnel de la Confédération (LPers). Cette obligation entrerait en conflit avec le principe du traitement confidentiel du signalement. Les collaboratrices de l'office doivent en revanche rapporter au directeur de l'OFCS, qui peut exceptionnellement dénoncer la possible infraction aux autorités de poursuite pénale si sa gravité le justifie (art. 73*d* al. 3 LSI2)[1355]. L'OFCS ne transmet donc le signalement aux autorités de poursuite pénale que si une telle dénonciation lui semble indiquée sur la base de la mise en balance de l'intérêt de l'État à une poursuite pénale et de l'intérêt à la confidentialité de la personne à l'origine du signalement[1356]. Tel pourrait typiquement être le cas si les membres de l'autorité découvrent du matériel pédopornographique visionné sur des systèmes informatiques d'une organisation ayant signalé un cyberincident[1357].

1353 ENISA, *Baseline Capabilities of National/Governmental CERT, Part 2,* 2010, p. 35.

1354 FF 2023 84, p. 51 ; NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques,* 2022, p. 25.

1355 FF 2023 84, p. 51.

1356 NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques,* 2022, p. 15 ; MEYER/MÉTILLE, *Computer security incident response teams : are they legally regulated ? The Swiss example,* 2022, p. 54.

1357 FF 2023 84, p. 29.

743 Dans le sens inverse et en raison du caractère confidentiel de la poursuite pénale, il est plus délicat pour l'autorité de poursuite pénale de partager des informations avec l'OFCS[1358]. Néanmoins, il est toujours possible que les autorités de poursuite pénale se retrouvent à requérir l'aide de l'office, notamment grâce aux compétences techniques de ce dernier et typiquement dans des cas de grande envergure[1359].

744 La relation entre autorités de poursuite pénale et l'OFCS implique une certaine attention de la part de ce dernier lorsqu'il intervient sur un système. Bien qu'il arrive en pratique que les autorités de poursuite pénale travaillent en même temps que l'OFCS sur les systèmes d'une infrastructure affectée par une cyberattaque, il se peut que celui-ci arrive en première position sur « le lieu du crime ». Il est en pratique important que l'office demeure attentif à ne pas compromettre les traces. Concrètement, l'office fédéral cherche à remédier à un dommage et à rétablir un système. Il doit, durant sa mission, demeurer attentif à ne pas détruire les moyens de preuves pertinents pour l'autorité de poursuite pénale qui, comme le service de renseignement, peut avoir besoin de ceux-ci et les exploiter[1360]. Pour éviter la destruction des preuves durant le rétablissement d'un système affecté, le travail simultané et en étroite collaboration entre les forces de police et l'OFCS est important.

745 Si une autorité de poursuite pénale étrangère (ou une autorité administrative) requiert des informations dans le cadre de sa procédure, les dispositions applicables en matière d'entraide judiciaire (ou d'assistance administrative) s'appliquent à la coopération de l'autorité concernée et l'OFCS (art. 77 al. 3 LSI)[1361].

d. Les échanges avec le Service de renseignement de la Confédération

746 Le SRC étant également susceptible de détenir des compétences de soutien aux infrastructures critiques, il peut être amené à coopérer avec l'OFCS. Dans ce cadre, la LRens sert de cadre permettant au SRC de soutenir les infrastructures

1358 Ce qui n'est pas spécifique à la Suisse, mais se retrouve ailleurs également, cf. ENISA, *Baseline Capabilities of National/Governmental CERT, Part 2,* 2010, p. 35 ; ENISA, *National/governmental CERT,* 2014, p. 28.

1359 Les capacités techniques des CERT nationales ou gouvernementales sont effectivement reconnues comme susceptibles d'aider les forces de police, cf. ENISA, *Baseline Capabilities of National/Governmental CERT, Part 2,* 2010, p. 35.

1360 MORGUS et al., *National CSIRT and Their Role in Computer Security Incident Response,* 2015, p. 13 s. À noter que la même attention doit être accordée par les autres équipes de gestion de cyberincidents, aussi susceptibles de travailler de manière coordonnée avec les autorités d'application de la loi, cf. MORGUS et al., *National CSIRT and Their Role in Computer Security Incident Response,* 2015, p. 20.

1361 FF 2017 2765, p. 2874.

critiques en cas de cyberattaques[1362]. La SNPC 2012-2017 précisait déjà que le Cyber SRC transmettait des informations nationales et internationales à MELANI, au même titre que le NCSC lui transmettait des informations techniques. L'*Operation Information Center* (OIC) MELANI sert en pratique d'interlocutrice pour les informations sur les cyberattaques et c'est ce centre qui exploite le service d'alerte précoce prévu à l'art. 6 al. 5 LRens[1363].

L'OFCS peut, dans un système semblable à celui qui régit ses échanges avec 747
les autorités de poursuite pénale, transmettre des informations au SRC lors du signalement d'un cyberincident en vertu de l'art. 73*d* al. 2 LSI2. En outre, elle lui octroie l'accès à certaines informations en vertu de l'art. 76*a* al. 1 LSI2.

L'OFCS transmet ces informations au SRC en vertu de l'art. 73*d* LSI2 si le 748
signalement d'un cyberincident ou son analyse révèle des informations utiles pour la détection précoce et la prévention des menaces pour la sûreté intérieure ou extérieure, dans l'évaluation de la menace et dans le service d'alerte en matière de renseignement pour la protection des infrastructures critiques (art. 6 al. 1 litt. a, al. 2 et 5 LRens). Cette communication se limite aux informations nécessaires à ces fins[1364].

En parallèle, l'OFCS et ses unités apportent leur soutien au SRC dans la 749
réalisation des objectifs de l'art. 6 al. 1 litt. a, al. 2 et 5 LRens. Pour ce faire, l'OFCS réalise des analyses techniques des cyberrisques et des évaluations spécifiques des cyberattaques relativement à leur nombre, leur type et leur ampleur (art. 76*a* al. 1 LSI2)[1365].

Aujourd'hui, un travail de collaboration étroite est mené entre le Cyber 750
SRC, l'OFCS, l'armée et les autorités de poursuite pénale, notamment afin d'analyser la situation de la cybermenace en Suisse[1366] ou en ce qui concerne les prestations fournies par l'OFCS aux infrastructures critiques[1367]. Dans le

1362 CF, *Rapport sur l'avancement des travaux concernant la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022,* 2020, p. 23 ; CF, *Plan de mise en œuvre de la SNPC 2018-2022,* 2019, p. 56 et 58.

1363 FF 2014 2029, p. 2068 ; UPIC, *Rapport « évaluation de l'efficacité de la stratégie nationale de protection contre les cyberrisques (SNPC) »,* 2016, p. 41.

1364 FF 2023 84, p. 29 ; NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques,* 2022, p. 15 ; MEYER/MÉTILLE, *Computer security incident response teams : are they legally regulated ? The Swiss example,* 2022, p. 53 s.

1365 FF 2023 84, p. 51 ; NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques,* 2022, p. 25.

1366 CF, *Plan de mise en œuvre de la SNPC 2018-2022,* 2019, p. 21 et 23.

1367 Le SRC détient également des compétences en rapport avec les cybermenaces pesant contre les infrastructures critiques, raison pour laquelle il est normal qu'il collabore avec l'OFCS pour ces questions, cf. CF, *Plan de mise en œuvre de la SNPC 2018-2022,* 2019, p. 39 ss.

cadre de la relation entre l'office fédéral pour la cybersécurité et le SRC, l'office devrait demander en pratique à la fournisseuse d'informations si elle peut les partager avec le SRC. Dans l'autre sens, il semblerait que le SRC pourrait communiquer des informations, à l'instar d'indicateurs de compromission (*indicators of compromise,* IOCs), à l'OFCS par le biais de MELANI OIC[1368]. Il convient en tout cas de soulever la question des conflits d'intérêts dans lesquels l'office fédéral peut se trouver, dans la mesure où les situations dans lesquelles il doit apporter des informations au SRC ne sont pas claires au vu de l'art. 6 LRens qui comprend de nombreuses situations. L'OFCS peut se trouver dans une position inconfortable en devant transmettre au SRC des informations, brisant ainsi la confiance portée par ses interlocutrices. Une telle pratique risque à terme d'impacter négativement la confiance et la collaboration efficace entre l'OFCS et ses autres partenaires. Ce potentiel conflit risque par ailleurs d'être exacerbé par le nouveau rattachement de l'ancien NCSC au DDPS.

751 Un dernier point mérite d'attirer l'attention de l'OFCS et du SRC dans le cadre de leur activité. L'objectif poursuivi par le SRC, à savoir la collecte et l'analyse d'informations principalement pour la sécurité nationale, pour la défense et pour les affaires étrangères, diffère de celui de l'office pour la cybersécurité. En pratique, le SRC peut par exemple avoir un intérêt à laisser subsister une vulnérabilité pour éventuellement l'exploiter plus tard, par le biais notamment de ses attributions aux art. 26 et 37 LRens, alors que l'OFCS chercherait tendanciellement davantage à l'éradiquer pour rétablir le fonctionnement sûr d'un réseau[1369].

e. Les échanges avec d'autres autorités

752 l'OFCS collabore par exemple avec la PFPDT, à qui certaines violations de la sécurité des données doivent être annoncées par les responsables du traitement (art. 24 LPD)[1370]. Lorsqu'une responsable du traitement doit annoncer une violation en vertu de l'art. 24 LPD, la PFPDT peut, avec l'accord de la personne tenue d'annoncer, transmettre le signalement à l'OFCS à des fins d'analyses de la violation. Le signalement transmis à l'OFCS peut contenir des données personnelles, y compris sensibles si relatives à des poursuites ou à des sanctions pénales ou administratives visant la personne tenue d'annoncer

1368 Concernant MELANI OIC, cf. *supra* N 250 ; au sujet de la transmission d'indicateurs de compromis par le Cyber SRC au NCSC, OBERHOLZER, *Bericht der Administrativuntersuchung – Auszug aus den Empfehlungen und der rechtlichen Beurteilung des Schlussberichts*, 2022, p. 3.

1369 MORGUS et al., *National CSIRT and Their Role in Computer Security Incident Response,* 2015, p. 13 s.

1370 Cf. *supra* N 525 ss.

(art. 24 al. 5*bis* nLPD). La PFPDT peut donc faire appel aux spécialistes techniques de GovCERT lorsqu'elle nécessite son expertise technique pour élucider les circonstances d'un incident, et lui communiquer à cette fin les données prévues à l'art. 15 al. 1 OPDo, toujours à la lumière du principe de proportionnalité (art. 24 al. 5*bis* nLPD)[1371].

753 En parallèle, lorsqu'une infrastructure critique est tenue de signaler à l'OFCS une cyberattaque en vertu des art. 74*a* ss LSI2, il se peut qu'elle soit soumise en parallèle à une obligation d'annoncer une violation de la sécurité des données à la PFPDT ou à une autre obligation sectorielle d'annoncer un événement à une autorité de surveillance spécifique. Il existe effectivement, selon les secteurs critiques, des possibilités ou obligations d'annoncer des incidents ou autres événements importants[1372]. L'OFCS met à disposition un système électronique sécurisé qui permet à l'exploitante désirant passer par ce biais de communiquer simultanément à l'OFCS ainsi qu'à d'autres autorités et services tout ou partie du signalement d'une cyberattaque ou de ses conséquences (art. 74*f* LSI2). Ce système a pour vocation de soulager le travail à fournir par les infrastructures critiques, mais elles ne sont pas obligées de procéder de la sorte et peuvent communiquer leurs signalements (du moins à l'OFCS) d'une autre manière. Néanmoins, au-delà de ce mécanisme, ni l'OFCS ni son service technique de GovCERT ne transmettent de communications aux autres autorités et services, au-delà des échanges susmentionnés avec le SRC et les autorités de poursuite pénale[1373].

f. La collaboration avec d'autres prestataires analogues

754 L'OFCS collabore sur le plan national avec les services cantonaux chargés de la cybersécurité. Elle doit veiller à maintenir une relation de confiance avec les autres prestataires de gestion de cyberincidents, par exemple sectorielles et locales de ses clientes pour pouvoir optimiser la gestion d'incidents et la protection contre les cybermenaces. L'office héberge également de point de contact sur le plan international pour communiquer avec des autorités disposant de compétences similaires.

755 L'OFCS donne l'accès aux informations nécessaires à la protection contre les cybermenaces aux services cantonaux chargés de la cybersécurité

1371 OFJ, *Rapport explicatif OPDo*, 2022, p. 45 ; NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques*, 2022, p. 27 ; BSK DSG-MATHYS/THOMANN, art. 24 N 112 s.

1372 Ces obligations sectorielles sont définies plus loin.

1373 NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques*, p. 21 s.

(art. 76*a* al. 4 LSI2). Il s'agit régulièrement de données techniques, à l'instar de modes opératoires. Il peut également s'agir de données personnelles, par exemple de ressources d'adressage ou de transactions financières[1374].

756 L'office fédéral pour la cybersécurité peut transmettre des informations aux organisations actives dans le domaine de la cybersécurité (art. 73*d* al. 1 LSI2). Ces informations proviennent des signalements et elles ne peuvent être transmises qu'à condition qu'elles soient utiles aux spécialistes auxquelles elles sont destinées dans le contexte de la protection contre les cybermenaces. En outre, la communication ne peut porter sur des données personnelles qu'à condition que la personne concernée y consente[1375].

757 Comme l'OFCS et son équipe de GovCERT pour la Suisse, bon nombre d'autres États ont leur CERT nationale ou gouvernementale. Les échanges d'informations entre ces différentes autorités sont utiles, voire nécessaires, pour appréhender au mieux les cybermenaces, qui peuvent impacter différents pays. Les mêmes logiciels malveillants sont par ailleurs régulièrement utilisés à travers différents États, en raison du caractère transfrontière d'Internet. L'art. 77 LSI2 habilite l'office et ses collaboratrices à échanger des informations sur l'identité ou le mode opératoire des auteures de cyberattaques avec des services étrangers ou internationaux chargés de la cybersécurité si ces derniers en ont besoin pour accomplir des tâches similaires à celles du nouvel OFCS). Une garantie de la part du service étranger doit être fournie, selon laquelle les informations seront utilisées conformément aux fins prévues (art. 77 al. 2 LSI2). Le protocole *Traffic Light Protocol* (TLP) est par ailleurs régulièrement appliqué en pratique, notamment par les autorités. Le TLP est un modèle internationalement reconnu permettant la catégorisation des informations confidentielles. Il détermine les conditions d'utilisation et de transmission des informations pour les différents niveaux de protection qu'il prévoit[1376]. Finalement, si des données personnelles viennent à être communiquées, les art. 16 s. LPD sont applicables (art. 77 al. 1 LSI2).

758 Pour pouvoir créer des stratégies et répondre au mieux aux incidents, plusieurs types de coopération existent pour permettre aux CSIRT (non seulement gouvernementales ou nationales) de partager des informations[1377]. D'une part, elles peuvent tout d'abord coopérer de manière bilatérale ou multilatérale, à savoir sur la base d'accords bilatéraux ou multilatéraux entre

1374 FF 2023 84, p. 51.

1375 FF 2023 84, p. 29.

1376 Cf. *infra* N 1014 ss ; FF 2017 2765, p. 2873 ; FF 2023 84, p. 52. Il ne s'agit en revanche pas d'une classification contraignante ou d'une solution universelle applicable à tous les échanges d'informations.

1377 ENISA, *Baseline Capabilities of National/Governmental CERT, Part 2,* 2010, p. 37.

parties. L'accord peut être formel comme informel[1378]. D'autre part, l'OFCS échange par le biais de son équipe technique, GovCERT, avec des CSIRT dans le cadre de communautés ou d'associations, à l'instar du *Forum of Incident Response and Security Teams* (FIRST), de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) ou encore du groupe des CERT des gouvernements européens (*European Government CERT group,* EGC). Ces communautés permettent de faciliter l'établissement d'une confiance mutuelle entre de nombreuses prestataires de gestion de cyberincidents, pour échanger au sujet notamment de leurs services, communautés clientes ou secteurs en commun[1379]. Ces échanges sont en principe fondés sur une base volontaire et de confiance. GovCERT est désignée implicitement comme étant le service de l'autorité compétente pour ces échanges sur la base de l'art. 77 al. 1 LSI. Elle a la capacité de refuser des échanges de données dans chaque cas d'espèce, par exemple si les art. 16 ss LPD ou le principe de proportionnalité risqueraient d'être violés.

4. La gestion de vulnérabilités

En sus de ses compétences dans la gestion de cyberattaques ou de cyberincidents, l'OFCS est actif dans le suivi de vulnérabilités. Les vulnérabilités de moyens informatiques peuvent, de la même manière que les cyberincidents, être signalées par toute personne au guichet unique (art. 73*b* al. 1 LSI2). Le NCSC disposait d'une unité spécialement compétente pour la gestion des vulnérabilités que l'OFCS conserve dans son service de cybersécurité opérationnelle. Ce service est compétent pour l'analyse des vulnérabilités afin de déterminer leur importance pour la protection de la Suisse contre les cybermenaces. L'OFCS émet des recommandations à la suite de ces analyses, si la situation ne nécessite pas d'analyses ou de clarifications supplémentaires (art. 73*b* al. 2 LSI2). 759

L'OFCS joue également un rôle dans la divulgation coordonnée des vulnérabilités par laquelle passe l'autorité pour informer la fabricante[1380]. Sur la base du signalement et de l'analyse des prestataires compétentes, l'OFCS informe immédiatement la fabricante des vulnérabilités signalées et lui fixe un délai adéquat pour y remédier (art. 73*b* al. 3 LSI2). À défaut de remédiation de la part de la fabricante, l'OFCS publie la vulnérabilité en indiquant le matériel ou le logiciel concerné si une telle manœuvre contribue à la protection de la 760

1378 ENISA, *Baseline Capabilities of National/Governmental CERT, Part 2,* 2010, p. 32.

1379 ENISA, *Baseline Capabilities of National/Governmental CERT, Part 2,* 2010, p. 32 et 38 s. Sur les principaux rassemblements de CERT, cf. *supra* N 341 ss.

1380 FF 2023 84, p. 27 ; OFCS, *Rapport semestriel 2023/II,* 2024, p. 12 s.

Suisse contre les cybermenaces (art. 73*c* LSI2)[1381]. Il s'agit dans ce cadre principalement de compétences d'analyses permettant le partage d'informations sur des vulnérabilités et la correction de ces dernières. L'OFCS fait partie du réseau mondial qui a la compétence de gérer les vulnérabilités des systèmes informatiques. Il peut à ce titre attribuer un numéro d'identification unique aux vulnérabilités qui lui sont signalées, conformément au système de référence international. Ce numéro permet d'identifier, de définir et de cataloguer les vulnérabilités rendues publiques. L'OFCS gère également ces numéros en vue d'échanges internationaux[1382].

5. L'activité du secteur privé comme limite

761 Il est important que l'OFCS n'empiète pas sur l'activité des prestataires privées de gestion de cyberincidents. L'État, plus particulièrement l'OFCS, doit se limiter à apporter un soutien subsidiaire[1383]. En plus de respecter la responsabilité individuelle de toute personne, les autorités étatiques doivent s'abstenir d'entraver la liberté économique et y déroger uniquement moyennant le respect de l'art. 94 al. 4 Cst. La portée de cette disposition implique que l'État doit en principe s'abstenir de concurrencer l'économie privée lorsqu'elle répond de manière satisfaisante à une demande, afin d'éviter de procéder à une conduite contre-productive et de décourager l'initiative privée. Cela étant, une certaine action de l'État peut néanmoins s'avérer nécessaire[1384]. Lorsque c'est le cas, l'État peut compléter et guider l'action du secteur privé.

762 Dans le cadre de la gestion de cyberincidents, tant l'État que des actrices privées disposent de compétences et fournissent des prestations. L'OFCS fournit notamment une assistance aux infrastructures critiques dans la gestion de cyberincidents (art. 15*a* al. 2 litt. f Org-DDPS). L'autorité et son équipe d'intervention sont susceptibles d'accomplir des prestations proches de celles offertes par les prestataires privées de gestion de cyberincidents sur le marché.

1381 GovCERT publiait déjà avant l'entrée en vigueur de la LSI des informations au sujet des vulnérabilités découvertes et analysées, voir par exemple GOVCERT, *Exchange Vulnerability*. Pour plus d'informations sur le processus, cf. FF 2023 84, p. 27 s.

1382 OFCS, *Le NCSC fait désormais partie du réseau mondial gérant les vulnérabilités des systèmes informatiques*.

1383 C'est d'ailleurs l'un des principes guidant la CSN et déjà la SNPC auparavant, cf. CF, *CSN*, 2023, p. 12 ; CF, *Plan de mise en œuvre de la SNPC 2018-2022,* 2019, p. 4 s., qui se concrétise p. 41. Pour une autre expression du principe de subsidiarité, cf. OFEN, *Bases pour l'introduction de systèmes de mesure intelligents auprès du consommateur final en Suisse,* 2014, p. 10, qui prévoit que le principe de subsidiarité implique que l'État ne fixe des exigences minimales que lorsque son intervention promet des gains d'efficacité économiques ou si l'intérêt public le justifie.

1384 CR Cst.-MARTENET, art. 94 N 45.

Partant, il est nécessaire de s'assurer que la liberté économique et la libre concurrence sont assurées (art. 94 al. 1 Cst.)[1385].

763 Toutes les mesures doivent être prises pour éviter de risquer une distorsion de la concurrence et un évincement des actrices privées[1386]. C'est pourquoi l'art. 74 al. 3 in fine LSI2 prévoit que l'OFCS ne peut apporter un soutien dans la gestion de cyberincidents affectant une infrastructure critique privée que lorsqu'il existe un danger pour le fonctionnement de l'infrastructure concernée et, surtout, qu'il est impossible d'obtenir un soutien équivalent sur le marché en temps utile. Son soutien est donc subsidiaire à celui fourni par les prestataires de services informatiques disponibles sur le marché[1387]. En outre, l'office fédéral n'agit pas dans les mêmes conditions et ne dispose pas des mêmes prérogatives que les prestataires privées. Le rétablissement d'une situation sûre figure dans les objectifs poursuivis par l'OFCS dans le contexte de l'art. 74 LSI2. Son intervention doit être limitée aux mesures urgentes pour respecter le principe de subsidiarité. Le soutien apporté par l'État ne vise donc pas les mesures plus étendues, visant par exemple à rétablir la cybersécurité en général. Ce type de mesures demeure du ressort de l'infrastructure critique et elles ne font pas partie des prestations offertes par l'office fédéral[1388].

764 Les autres compétences générales de l'OFCS visant le soutien des infrastructures critiques s'adressent en pratique aux fournisseuses, typiquement internes, de prestations de gestion de cyberincidents qui sont les interlocutrices principales de l'office, et particulièrement de son équipe technique, GovCERT. En outre, les diverses mesures entreprises par l'OFCS poursuivent d'autres objectifs que l'action du secteur privé, comme l'établissement d'une image des cybermenaces en Suisse ou la sensibilisation du grand public. De manière plus générale et alors que les prestataires privés vont viser davantage des objectifs de marché, l'office agit pour la sauvegarde d'un intérêt public, qui est la sécurité publique.

C. Quelques généralités ayant trait à la responsabilité

765 Les expertes de l'OFCS sont soumises en tant que membres de l'administration fédérale à la Loi sur la responsabilité de la Confédération, des membres de ses autorités et de ses fonctionnaires (art. 1 al. 1 LRCF). L'art. 3 al. 1 LRCF pose le

1385 FF 2023 84, p. 31.

1386 CR Cst.-MARTENET, art. 27 N 82 ; CR Cst.-MARTENET, art. 94 N 29.

1387 NCSC, *Rapport explicatif relatif à l'ouverture de la procédure de consultation – Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques*, 2022, p. 16.

1388 FF 2023 84, p. 31.

principe selon lequel la Confédération répond du dommage causé par un acte illicite d'une fonctionnaire dans l'exercice de ses fonctions, fautive ou non[1389].

766 L'acte peut être illicite, car il porte atteinte à un bien absolument protégé (illicéité de résultat)[1390]. Dans ce cas, un acte commis par une fonctionnaire est illicite, car il a pour conséquence la mort d'un individu, des lésions corporelles ou une atteinte à la personnalité (art. 5 s. LRCF). De la même façon que pour les prestataires privées de gestion de cyberincidents, les atteintes illicites risquent en pratique principalement d'entraîner des conséquences sur les données de citoyennes, donc de constituer des atteintes à la personnalité. Dans ce cas, la personne concernée a droit à une somme d'argent à titre de réparation morale de la part de la Confédération, à condition que la gravité de l'atteinte le justifie et que la collaboratrice de l'OFCS ne lui ait pas donné satisfaction autrement (art. 6 al. 2 LRCF).

767 Un dommage purement économique résulte d'un acte illicite imputable à l'État si ce dernier commet un acte en violation d'une norme protégeant l'intérêt de la personne lésée (illicéité de comportement)[1391]. En ce sens, la Confédération peut engager sa responsabilité vis-à-vis d'une personne dont le patrimoine est affecté par une violation importante du secret d'une fonctionnaire de l'office fédéral, par exemple si elle ne passe pas par la procédure de l'art. 320 ch. 2 CP et qu'un dommage financier en découle.

768 Lorsque l'on est en présence d'un acte illicite, il demeure possible de se prévaloir de motifs justificatifs pour lever l'illicéité de l'atteinte, notamment lorsqu'il en va de la poursuite d'intérêts publics comme la sécurité publique et à condition notamment que le principe de proportionnalité soit respecté[1392]. L'OFCS et ses collaboratrices sont fortement susceptibles d'intervenir dans des situations urgentes et problématiques, voire dans des situations de crises. En cas de crises, l'on ne peut pas actionner l'État à chaque fois qu'il ne prend pas les meilleures mesures possibles, mais bien s'il ne prend pas les mesures qui pouvaient raisonnablement être attendues de lui[1393].

1389 OFJ, *Guide de législation*, 2019, N 921. Il faut en outre un lien de causalité naturelle et adéquate.

1390 TAF, A-7111/2010, c. 4.2 ; ATAF 2009/57, c. 2 ; JAAG, p. 32 ; POLTIER, *La responsabilité de l'État pour acte illicite : l'exigence de l'illicéité,* 2012, p. 48.

1391 TAF, A-7111/2010, c. 4.2 ; ATAF 2009/57, c. 2 ; JAAG, p. 32 ; POLTIER, *La responsabilité de l'État pour acte illicite : l'exigence de l'illicéité,* 2012, p. 48. À noter qu'en cas d'omission, la fonctionnaire doit également violer une norme lui imposant d'agir tout en étant dans une position de garante, ce peu importe le bien touché par l'atteinte, cf. POLTIER, *La responsabilité de l'État pour acte illicite : l'exigence de l'illicéité,* 2012, p. 58 s. et 79, qui soutient que l'illicéité de comportement prévaut en cas d'omission.

1392 ATF 123 II 577, c. 4.ff ; JAAG, p. 33.

1393 POLTIER, *La responsabilité de l'État pour acte illicite : l'exigence de l'illicéité,* 2012, p. 75.

Les fonctionnaires ne sont pas directement responsables vis-à-vis de la personne lésée[1394]. Lorsque la Confédération engage sa responsabilité à cause de l'acte illicite d'une collaboratrice de l'OFCS, elle dispose ensuite d'une action récursoire à l'encontre de la fonctionnaire ayant causé le dommage avec une faute grave (à savoir par négligence grave ou intentionnellement, cf. art. 7 LRCF), à savoir si elle a violé ses devoirs de manière évidente ou si elle a violé des règles élémentaires[1395]. 769

Parallèlement, si une collaboratrice de l'office pour la cybersécurité cause directement un dommage à la Confédération, elle répond envers cette dernière si elle a violé ses devoirs de service intentionnellement ou par négligence grave (art. 8 LRCF). Si plusieurs expertes du service technique ont causé ensemble le dommage, ces dernières répondent envers la Confédération proportionnellement à leurs fautes (art. 9 al. 2 LRCF). 770

À noter que la jurisprudence n'exclut pas l'idée de responsabilité de l'État pour des recommandations, du moins lorsqu'elles font partie des tâches de l'autorité et qu'elles sont critiquables du point de vue des connaissances lors de leur prononcé, ce qui implique un comportement illicite[1396]. 771

D. Une conclusion

GovCERT est le service technique de l'OFCS ; l'office et son équipe d'expertes techniques constituent l'autorité de la Confédération chargée d'intervenir en cas d'urgence informatique. L'Org-DDPS n'est pas aussi claire que ne l'était l'aOPCy sur le statut et sur les compétences de GovCERT, mais l'autorité disposant d'un pouvoir décisionnel est l'OFCS, qui gère GovCERT. 772

L'un des mandats principaux de l'OFCS demeure le soutien technique fourni aux infrastructures critiques dans leur protection contre les cybermenaces. À ce titre, l'autorité détient des compétences préventives et de gestion de la qualité de la sécurité, à l'instar de la compétence de procéder à des veilles technologiques ou de publier des informations sur la cybersécurité. 773

L'OFCS compte dans sa mission le soutien réactif aux cyberincidents, surtout lorsque l'incident vise une infrastructure critique. Il émet des recommandations et peut participer à la mise en place de mesures pour aider à la gestion technique d'un incident. Son soutien se manifeste de différentes façons en fonction des besoins et des ressources disponibles dans chaque situation. 774

1394 JAAG, p. 26 s.

1395 JAAG, p. 27, 36 et 39 s. Pour des exemples où la faute grave n'a pas été admise par le TF : ATF 102 Ib 103, c. 4 ; ATF 89 I 414, c. 6.

1396 Cf. à titre d'exemple ATF 118 Ib 473 c. 6 et 7 ; OFJ, *Guide de législation,* 2019, N 936 s.

775 L'OFCS détient d'autres compétences. Il constitue un point de contact central en Suisse. Il échange à ce titre des informations avec les infrastructures critiques, qui constituent son cercle de clientes, comme avec d'autres autorités poursuivant des missions différentes. L'office échange également avec des CSIRT et organisations fournissant des prestations similaires. En parallèle de sa compétence de point de contact, l'OFCS occupe également un rôle important dans la divulgation coordonnée de vulnérabilités. L'ensemble des tâches accomplies par l'autorité de l'administration fédérale doit respecter la subsidiarité de l'État et ne doit pas créer de distorsion du marché économique.

776 Les collaboratrices de l'OFCS sont soumises en tant que membres de l'administration fédérale à la LRCF en cas d'acte illicite et non aux mécanismes contractuels et civils applicables aux prestataires privées de gestion de cyberincidents. Bien que les mécanismes de responsabilité ne soient pas les mêmes pour toutes les prestataires de gestion de cyberincidents, nous allons voir que les collaboratrices de l'office et d'autres fournisseuses de prestations de gestion de cyberincidents peuvent engager leur responsabilité sur les mêmes fondements, typiquement ce qui concerne leur responsabilité pénale.

III. Un bref détour par le service spécialisé pour la sécurité de l'information

A. La création du nouveau service

777 Janvier 2024 a sonné deux changements primordiaux dans l'organisation de la Confédération pour la cybersécurité. En plus de la transformation du NCSC en OFCS, un nouveau service spécialisé de la Confédération pour la sécurité de l'information a été créé.

778 Le nouveau service spécialisé de la Confédération pour la sécurité de l'information a été établi pour janvier 2024, bien qu'il ne soit pas encore opérationnel. La création de cette autorité a eu lieu en parallèle de la transformation du NCSC en office fédéral. Le service spécialisé de la Confédération pour la sécurité de l'information sert d'autorité nationale pour la sécurité de l'information (art. 42 al. 3 OSI). Il devrait à ce titre devenir l'autorité principale pour l'autoprotection et la sécurité informatique de la Confédération, compétences occupées entre 2019 et 2023 par le NCSC et par le Secrétariat général du DDPS (SG-DDPS) dans son domaine Digitalisation et cybersécurité. Selon le rapport explicatif de 2022 relatif à la législation d'exécution de la LSI, c'est effectivement le SG-DDPS qui occupait le rôle d'autorité nationale de sécurité de l'information, mais le NCSC détenait également des compétences maintenant

attribuées au nouveau service spécialisé dans le cadre de son mandat, à l'instar de la compétence d'adopter des directives pour la sécurité des moyens informatiques des autorités et organisations de la Confédération, comme y fait référence l'art. 51 al. 1 OSI[1397]. Le service spécialisé de la Confédération pour la sécurité de l'information fait partie du Secrétariat d'État à la politique de sécurité (SEPOS) du DDPS (art. 7 al. 2 litt. e ch. 1 Org-DDPS)[1398].

Son activité concerne principalement les autorités et organisations de la 779
Confédération soumises aux art. 6 ss LSI. En vertu de l'art. 83 LSI, il est notamment compétent pour conseiller et soutenir les autorités soumises à la LSI (art. 83 al. 1 litt. a LSI), recommander des mesures si la sécurité de l'information de la Confédération est menacée (art. 83 al. 1 litt. b LSI) ou encore évaluer à la demande des autorités soumises à la loi les risques liés à l'utilisation de nouvelles technologies (art. 83 al. 1 litt. d LSI)[1399].

L'art. 42 OSI concrétise en partie ces tâches en précisant par exemple 780
que le service spécialisé de la Confédération pour la sécurité de l'information élabore des stratégies sur des thèmes pertinents pour la sécurité, participe à la formation ou assume la responsabilité des solutions de sécurité certifiées utilisées dans l'administration fédérale et l'armée (art. 42 al. 1 OSI)[1400]. L'art. 42 al. 3 OSI lui confère également des compétences pour la représentation de la Suisse sur le plan international. Le service spécialisé de la Confédération pour la sécurité de l'information détient d'autres compétences, comme le prévoient différentes dispositions de l'OSI[1401].

B. Le lien étroit entre le service et l'Office fédéral de la cybersécurité

L'OFCS et le service spécialisé de la Confédération pour la sécurité de l'infor- 781
mation doivent coordonner leurs activités afin d'éviter un gaspillage des ressources (art. 43 al. 2 OSI)[1402]. En outre, le service spécialisé de la Confédération pour la sécurité de l'information est une nouvelle autorité, alors que l'OFCS existait déjà en tant que NCSC, raison pour laquelle l'OFCS va accomplir certaines tâches du service spécialisé de la Confédération pour la sécurité de l'information jusqu'en 2025. Le service spécialisé de la Confédération pour

1397 SG-DDPS, *Législation d'exécution relative à la LSI, Rapport explicatif*, 2022, p. 23 s.

1398 FF 2017 2765, p. 2900 ; SG-DDPS, *Législation d'exécution relative à la LSI, Explications*, 2023, p. 6.

1399 FF 2017 2765, p. 2877.

1400 Ce qui ne devrait pas entraver les compétences du secteur TNI dans ce contexte, cf. SG-DDPS, *Législation d'exécution relative à la LSI, Explications*, 2023, p. 24 s.

1401 SG-DDPS, *Législation d'exécution relative à la LSI, Explications*, 2023, p. 24.

1402 SG-DDPS, *Législation d'exécution relative à la LSI, Explications*, 2023, p. 25.

la sécurité de l'information détient d'autres compétences à différentes dispositions de l'OSI, qui sont assumées par l'OFCS jusqu'en 2025 en raison de la récente création du service spécialisé de la Confédération pour la sécurité de l'information (art. 51 al. 6 OSI)[1403]. L'OFCS va donc dans un premier temps participer à la sensibilisation, de concert avec les départements et les unités administratives, des collaboratrices sur les risques pour la sécurité de l'information et établir des outils à cet effet (art. 11 al. 3 et 4 OSI), ainsi qu'émettre à l'attention des organisations de l'art. 2 al. 1 à 3 OSI des directives générales et abstraites relatives à la gestion de la sécurité de l'information (art. 5 ss OSI), relatives à la procédure de sécurité de l'art. 16 LSI ou concernant les exigences minimales pour les catégories de sécurité des moyens informatiques de l'art. 17 LSI[1404].

782 En outre, les deux autorités vont coopérer, notamment pour la gestion auprès des unités administratives et des départements des incidents liés à la sécurité de l'information (art. 12 OSI). Les deux autorités peuvent aider ces autorités à maîtriser les incidents auxquels elles sont confrontées ainsi qu'à traiter les failles de sécurité (art. 12 al. 3 OSI). Elles doivent immédiatement informer le service spécialisé de la Confédération pour la sécurité de l'information dans les cas de l'art. 12 al. 5 OSI, à la suite de quoi le service spécialisé de la Confédération pour la sécurité de l'information évalue le risque et le soutien requis. Il peut également diriger les opérations ou en déléguer la direction à l'OFCS, tout cela avec l'accord de l'autorité concernée (art. 12 al. 6 à 8 OSI)[1405].

783 Les compétences des deux autorités étant pour certaines particulièrement étroites, l'on peut se demander si une coopération sans perte de temps ou gaspillage d'autres ressources est réellement envisageable en pratique. En effet, le NCSC avait déjà adopté différentes directives techniques applicables à l'administration fédérale et dans la mesure où l'OFCS conserve les compétences techniques, attribuer la compétence d'adopter des directives sur la sécurité informatique au service spécialisé de la Confédération pour la sécurité de l'information (art. 29 al. 1 OSI) peut par exemple illustrer une potentielle perte de temps et un gaspillage des ressources de cette autorité. L'OFCS aurait typiquement pu conserver cette compétence. L'OFCS détient un rôle plus technique et dispose principalement de compétences pour la cybersécurité auprès de l'ensemble des infrastructures critiques, alors que le service spécialisé de la Confédération devrait voir ses compétences d'une part limitées à la Confédération et d'autre part renforcées vis-à-vis de cette dernière. Cela étant, il conviendra de

1403 SG-DDPS, *Législation d'exécution relative à la LSI, Explications,* 2023, p. 6 et 27.

1404 Cette compétence est déléguée du CF en vertu de l'art. 85 LSI au service spécialisé de la Confédération pour la sécurité de l'information, avec une délégation à l'OFCS jusqu'en 2025, cf. SG-DDPS, *Législation d'exécution relative à la LSI, Explications,* 2023, p. 16 et 20.

1405 SG-DDPS, *Législation d'exécution relative à la LSI, Explications,* 2023, p. 14 s.

voir dans les années à venir comment les autorités vont se répartir leurs tâches et surtout leur responsabilité, principalement en termes d'élaboration de directives à l'attention d'autorités et organisations de la Confédération ou de soutien et de gestion de cyberincidents auprès de ces dernières.

784 Par ailleurs, le sort réservé à certaines compétences attribuées initialement au NCSC n'est pas certain. À titre d'exemple, le NCSC devait systématiquement être consulté lors de la réalisation de projets pilotes pour la numérisation des prestations de l'administration fédérale centrale dans le contexte de l'utilisation des moyens électroniques (art. 15 al. 5 LMETA). La LMETA prévoit tant des considérations liées à la sécurité de l'information qu'à la sécurité des moyens informatiques. Les autorités assujetties à la loi sont les autorités de l'administration fédérale centrale, auprès desquelles le nouveau service spécialisé de la Confédération pour la sécurité de l'information détient depuis janvier 2024 le rôle principal en termes de sécurité de l'information et des moyens informatiques. Le message ne prévoyant rien de plus[1406], la question se pose de savoir si l'OFCS conservera les compétences du NCSC. Vu le rôle d'autoprotection de la Confédération qu'endosse maintenant le service spécialisé, il n'est pas exclu que cette compétence lui revienne. Reste à voir si l'OFCS devra également être consulté pour la réalisation de tels projets.

785 Au-delà de ces questions de compétences, l'OFCS va certainement également aider le service spécialisé de la Confédération pour la sécurité de l'information, typiquement lorsque ce dernier recommande des mesures en raison d'une menace pour la sécurité de l'information de la Confédération (art. 83 al. 1 litt. b LSI). Bien que le message de la LSI prévoie l'implication de MELANI pour recommander des mesures lorsqu'il s'agit de menaces opérationnelles dans le domaine technique[1407], l'on sait que l'OFCS reprendra cette tâche, MELANI étant dissoute et l'OFCS constituant l'autorité helvétique principale pour la cybersécurité et les aspects techniques y étant liés. Le service spécialisé de la Confédération pour la sécurité de l'information fait par ailleurs appel à l'OFCS et, par la même occasion, à son service technique, GovCERT, pour les compétences techniques de l'autorité et de son service[1408]. En revanche, certaines des compétences susmentionnées n'impliquent pas forcément l'OFCS et GovCERT, par exemple lorsqu'il en va de la coordination par le service spécialisé de la Confédération pour la sécurité de l'information de projets impliquant plusieurs autorités (art. 83 al. 1litt. f LSI).

1406 FF 2022 804, p. 88.

1407 FF 2017 2765, p. 2877.

1408 La révision de la LSI a justement engendré un besoin d'agrandir l'équipe de GovCERT, cf. FF 2023 84, p. 58.

C. Une conclusion sur l'impact du nouveau service

786 L'OFCS n'est pas l'unique nouvelle autorité appréhendant dans son mandat des questions de cybersécurité. Le nouveau service spécialisé de la Confédération pour la sécurité de l'information reprend de nombreuses tâches du NCSC pour l'autoprotection de la Confédération.

787 Le nouveau service spécialisé de la Confédération pour la sécurité de l'information devient depuis janvier 2024 l'autorité principale pour la sécurité de l'information de la Confédération. Ce mandat se recoupe partiellement avec celui de l'OFCS, soit d'assurer le rôle d'autorité principale pour la cybersécurité en Suisse. La création du nouveau service spécialisé de la Confédération pour la sécurité de l'information affaiblit l'OFCS en adoptant certaines compétences qui revenaient jusque-là en partie au NCSC.

788 Le service spécialisé de la Confédération dispose d'un large spectre de compétences réglementaires, de soutien ou de surveillance des autorités et organisations de la Confédération quant à la sécurité des informations qu'elles traitent. L'on peut espérer que le fait que le service spécialisé de la Confédération dispose des compétences principales pour la sécurité de l'information de la Confédération permette de renforcer le rôle de l'OFCS en tant qu'autorité de cybersécurité pour les autres infrastructures critiques, sortant de la Confédération. Des difficultés existent toutefois dans la cohabitation des compétences de ces deux autorités.

789 Une certaine scission entre les compétences de l'OFCS et du service spécialisé de la Confédération pour la sécurité de l'information existe. Cependant, les deux autorités vont étroitement collaborer sur certains aspects, notamment lorsqu'il en va de la gestion d'un cyberincident important impactant une autorité ou une organisation de la Confédération. Autrement, l'OFCS devrait également apporter son concours au service spécialisé de la Confédération pour la sécurité de l'information, typiquement lorsqu'il en va de questions techniques ou opérationnelles impliquant des aspects de cybersécurité.

IV. Un survol de quelques chefs communs de responsabilité

A. La responsabilité pénale

790 Le chapitre 5 a permis l'analyse du cadre légal applicable à l'activité des prestataires de gestion de cyberincidents et de l'OFCS dans le soutien qu'il apporte dans le contexte de gestion de cyberincidents. La violation de normes et la

réalisation de comportements illicites est en principe appréhendé différemment par le cadre légal selon qu'il s'agit d'un comportement de l'OFCS ou d'une autre prestataire.

Les prestataires de gestion de cyberincidents peuvent engager leur responsabilité si elles violent des obligations administratives, des obligations contractuelles ou si elles causent par un acte illicite un dommage à des personnes tierces sous l'angle de leur responsabilité civile[1409]. L'OFCS étant une autorité de l'administration fédérale, les actes illicites de ses collaboratrices sont à appréhender sous l'angle de la responsabilité de l'État[1410]. 791

Cela étant, des chefs de responsabilité sont susceptibles de concerner tant les collaboratrices de l'OFCS que d'autres prestataires de gestion de cyberincidents. Nous allons voir plus tard les responsabilités communes en cas de traitement illicite de certaines informations[1411], mais de façon plus générale et le droit pénal s'appliquant à tous les individus, il pose, en interdisant certains comportements, un cadre important tant dans l'activité de l'OFCS que des autres fournisseuses de prestations de gestion de cyberincidents. 792

B. Pour des infractions au Code pénal

Les personnes actives au sein d'une prestataire de gestion de cyberincidents, qu'elles agissent dans une entreprise privée ou au sein de GovCERT, doivent comme tout individu, s'abstenir de réaliser des infractions (par renvoi de l'art. 13 al. 1 LRCF pour les membres de GovCERT). Certaines infractions revêtent un intérêt particulier dans l'activité des prestataires de gestion de cyberincidents selon les prestations qu'elles offrent à leur clientèle. 793

L'infraction la plus facilement concevable est l'accès indu à un système informatique (art. 143*bis* al. 1 CP). Elle a déjà fait l'objet d'une analyse[1412]. Il s'agit donc de comprendre comment cette infraction se manifeste dans la pratique des prestataires de gestion de cyberincidents. Lorsque ces expertes interviennent sur l'infrastructure informatique de sa cliente, elles agissent en principe conformément à un mandat reçu et dans son cadre[1413]. Les collaboratrices doivent néanmoins veiller, dans leur pratique, à ne pas accéder indûment à des systèmes informatiques protégés. Les clientes doivent donner leur accord pour que des expertes en cybersécurité effectuent par exemple 794

1409 Cf. *supra* N 646 et 675 ss.

1410 Cf. *supra* N 765 ss.

1411 Cf. *infra* en particulier N 928 ss et 976 ss.

1412 Cf. *supra* N 552.

1413 PFPDT, *White Hat Hackers*, 2023, N 2.

des tests de pénétration sur leur infrastructure informatique. Les prestataires de gestion de cyberincidents doivent donc toujours s'assurer qu'elles ont le consentement de la personne concernée pour accéder aux différents systèmes informatiques, dans la mesure où la loi ne les autorise pas à s'infiltrer dans des systèmes informatiques[1414]. Il en va de même pour GovCERT, qui ne peut accéder aux informations et moyens informatiques des infrastructures critiques que moyennant leur accord (art. 74 al. 4 LSI2). Pour réaliser l'infraction de l'art. 143*bis* al. 1 CP, l'experte doit agir intentionnellement. La collaboratrice d'une prestataire de gestion de cyberincidents qui accède à un système informatique spécialement protégé sans être certaine du consentement de l'entité concernée mais s'en accommodant peut engager sa responsabilité pénale en vertu de cette disposition sous l'angle du dol éventuel[1415].

795 Si ce premier pas est franchi par la collaboratrice d'une prestataire de gestion de cyberincidents, d'autres infractions peuvent, par la suite, être réalisées. Il s'agit principalement de la soustraction de données (art. 143 CP), de la détérioration de données (art. 144*bis* CP) ou de la soustraction de données personnelles (art. 179*novies* CP)[1416]. Ces trois infractions sont également intentionnelles. En outre, la soustraction de données selon l'art. 143 CP n'est réalisable que si l'auteure agit avec un dessein d'enrichissement illégitime. Il est donc rare en pratique, sous réserve d'une intention malveillante, que la collaboratrice d'une prestataire de gestion de cyberincidents se rende coupable de soustraction de données[1417]. La détérioration de données suppose, de la même manière que l'accès indu à un système informatique, que l'auteure agisse sans droit. Les collaboratrices d'une prestataire de gestion de cyberincidents doivent s'abstenir d'agir dans une zone grise et sont tenues de s'assurer du consentement des titulaires de systèmes informatiques[1418]. Cette réflexion vaut tout particulièrement pour les prestataires privées de gestion de cyberincidents. La LSI2 rappelle pour l'OFCS qu'il peut, avec le consentement de l'infrastructure critique, accéder à ses informations et à ses moyens informatiques pour la soutenir dans la gestion d'un cyberincident (art. 74 al. 4 LSI2)[1419].

796 Il peut arriver qu'une décision impliquant un accès indu à un système informatique soit prise, par exemple dans le cas où la prestataire de gestion

1414 Au sujet des pirates éthiques, cf. *supra* N 475 ss et *infra* N 1350 ss. Sur le consentement libre, exprès et éclairé, cf. notamment HURTADO POZO/GODEL, N 689 ss.

1415 ATF 137 IV 1, c. 4.2.3 ; BSK StGB-NIGGLI/MAEDER, art. 12 N 52 ; HURTADO POZO/GODEL, N 419.

1416 Pour une analyse de ces infractions, cf. *supra* N 553 ss.

1417 Ce qui peut par ailleurs susciter des critiques, cf. notamment BSK StGB-WEISSENBERGER, art. 143 N 5 et 28 s.

1418 CR CP II-MONNIER, art. 144*bis* N 6.

1419 FF 2023 84, p. 31.

de cyberincidents a l'opportunité de procéder à du *« hackback »*. La personne (ou les personnes) au sein de la prestataire s'introduisant de la sorte dans le système informatique de l'attaquante risque de se voir reprocher un accès indu à un système informatique ainsi qu'une soustraction de données (personnelles ou non), ou une détérioration de données. Elle peut tenter de se prévaloir de la légitime défense ou la défense excusable (art. 15 s. CP). La légitime défense supposant l'immédiateté de la riposte[1420], il est souvent difficile de pirater le système informatique de l'attaquante immédiatement et il est nécessaire dans chaque cas d'évaluer la proportionnalité ainsi que la subsidiarité de la contre-attaque.

797 En parallèle, l'on peut se demander si d'autres infractions peuvent entrer en ligne de compte selon les actions et interactions des prestataires de gestion de cyberincidents. Il en va de la sorte pour la mise sur le marché d'outils de piratage (art. 143*bis* al. 2 CP) ou la fabrication et la mise en circulation de programmes de détérioration (art. 144*bis* al. 2 CP). De nombreuses prestataires de gestion de cyberincidents collaborent et s'entraident par le biais de différentes communautés et plateformes d'échange d'informations[1421]. Elles sont susceptibles, pour s'entraider face à des logiciels malveillants et autres outils d'attaque, d'apprivoiser ces derniers afin de limiter leur évolution dans divers systèmes informatiques. À titre d'exemple, l'art. 143*bis* al. 2 CP implique une « mise sur le marché » et non pas la simple possession, importation ou production de données. En outre, la formulation « sans droit » implique *a contrario* que les comportements licites ne sont pas condamnables. Les outils pour tester la résistance d'un système informatique avec le consentement de l'ayant droit ne sont pas illicites. L'emploi de tels outils par une prestataire de gestion de cyberincidents de manière préventive sur les systèmes informatiques de ses clientes avec leur accord est donc admis[1422]. Il devrait en aller de même pour les instruments partagés entre prestataires de gestion de cyberincidents, sous réserve que ces produits soient ensuite utilisés avec la volonté de mener une contre-attaque *(hack-back),* qui soulèvent la question de la licéité de l'utilisation subséquente du logiciel.

798 D'autres infractions peuvent entrer en ligne de compte dans des cas de réaction à des cyberattaques, typiquement lorsqu'il en va de rançongiciels et de paiements de rançon par la prestataire de gestion de cyberincidents, interne ou externe. En cas de paiement à une organisation criminelle, l'art. 260*ter* CP

1420 CR CP I-MONNIER, art. 15 N 11 ss ; HURTADO POZO/GODEL, N 634.

1421 Sur les plateformes d'échange d'informations et les communautés, cf. notamment *supra* N 336 ss.

1422 CR CP II-MONNIER, art. 143*bis* N 15.

pourrait s'appliquer aux personnes procédant au paiement. En effet, l'infraction est intentionnelle, ce qui implique que la personne qui procède au paiement en se doutant et en acceptant que celui-ci serve de soutien à une telle organisation dans son activité (art. 260*ter* al. 1 litt. b CP) risque d'être condamnée sous l'angle du dol éventuel[1423]. Bien que les collaboratrices d'une prestataire de gestion de cyberincidents puissent tenter d'invoquer les faits justificatifs prévus aux art. 17 s. CP, il n'est pas certain que ceuxci puissent s'appliquer dans tous les cas. La personne prévenue pour soutien à une organisation criminelle qui se prévaut de l'état de nécessité porte atteinte à la paix publique pour sauvegarder, souvent, le patrimoine. L'art. 17 CP requiert que le danger soit imminent, impossible à détourner autrement et que le bien juridique sauvegardé soit de valeur supérieure au bien juridique sacrifié. Il est difficile de savoir si le paiement d'une rançon peut constituer le moyen approprié pour éviter le danger causé par une extorsion au sens de l'art. 156 CP. La même question se pose quant à la nécessité du paiement. De plus, la mise en balance des intérêts peut soulever des questions en pratique[1424]. Si l'art. 17 CP ne peut pas trouver application, l'on peut se demander si le sacrifice du bien juridique pouvait être raisonnablement évité par l'auteure, à savoir la collaboratrice de la prestataire de gestion de cyberincidents procédant au paiement de la rançon. Si c'est le cas, la peine de la personne procédant au paiement est atténuée (art. 18 al. 1 CP). Au contraire, si le bien juridique ne pouvait être raisonnablement sacrifié, la personne procédant au paiement est exemptée de peine (art. 18 al. 2 CP). La réflexion doit être menée dans chaque situation, compte tenu des circonstances du cas d'espèce[1425]. Si la prestataire de gestion de cyberincidents recommande le paiement d'une rançon à une organisation ou l'assiste dans le processus, l'analyse de la complicité, voire de l'instigation (respectivement art. 25 et 24 CP) devrait être conduite[1426].

799 Bien qu'en principe le droit pénal suisse repose sur la responsabilité d'individus, il est possible pour la prestataire de gestion de cyberincidents externe ou pour l'infrastructure critique à laquelle une fournisseuse interne de prestations est rattachée d'engager sa responsabilité en vertu de l'art. 102 CP. En cas d'infraction à l'art. 260*ter* CP par exemple (figurant dans la liste des

1423 ATF 137 IV 1, c. 4.2.3 ; BSK StGB-NIGGLI/MAEDER, art. 12 N 52 ; CR CP I-VILLARD/CORBOZ, art. 12 N 49 et 64 ; SARRASIN/PANGRAZZI/MEYER, p. 1080 s. Contrairement à l'art. 260*quinquies* CP qui implique un dessein avec lequel, dans toute situation ordinaire, la CSIRT ne peut pas agir.

1424 HURTADO POZO/GODEL, N 659 ss ; SARRASIN/PANGRAZZI/MEYER, p. 1084 s.

1425 BENHAMOU/WANG, p. 84 ; CR CP II-LIVET/DOLIVO-BONVIN, art. 260*ter* N 3 ; SARRASIN/PANGRAZZI/MEYER, p. 1085 s.

1426 Sur l'analyse de l'art. 260*ter* CP et l'invocation des motifs justificatifs des art. 17 s. CP, cf. SARRASIN/PANGRAZZI/MEYER, p. 1081 ss et références citées.

infractions de l'art. 102 al. 2 CP), l'organisation répond indépendamment de la punissabilité de personnes physiques si elle n'a pas pris toutes les mesures organisationnelles raisonnables et nécessaires pour empêcher une telle infraction (art. 102 al. 2 CP). Pour les autres infractions susmentionnées, elle peut engager sa responsabilité pénale si le délit ne peut être imputé à aucune personne physique déterminée en raison du manque d'organisation de l'entreprise, moyennant que les autres conditions de l'art. 102 al. 1 CP soient réunies (art. 102 al. 1 CP)[1427]. L'art. 102 al. 1 CP est susceptible d'entrer en ligne de compte subsidiairement à la responsabilité d'une personne physique. La responsabilité de l'entreprise est engagée à condition que le paiement d'une rançon puisse être considéré comme effectué dans le cadre des activités commerciales de l'organisation au sein de laquelle œuvre la prestataire de gestion de cyberincidents[1428].

C. Pour des infractions à d'autres lois

Il existe bon nombre de lois imposant en leur sein des sanctions à caractère pénal. Sans entrer dans les détails, certaines prestataires de gestion de cyberincidents peuvent, selon les prestations qu'elles offrent, être poursuivies en cas de violation d'obligations légales spéciales. 800

Par exemple, les prestataires de gestion de cyberincidents peuvent recevoir ou transmettre au-delà des frontières des codes de logiciels soumis au respect de certaines législations. Par exemple, une actrice malveillante qui aspire à infecter de nombreuses machines est susceptible de passer par l'utilisation d'un serveur pour commander et contrôler la propagation d'un logiciel malveillant. Si une prestataire de gestion de cyberincidents analyse le logiciel de *command and control* et découvre que d'autres organisations à l'étranger font face au même mode opératoire malveillant, elle ne peut pas transmettre le logiciel sans assurer le respect de la Loi sur le contrôle des biens (LCB) et son ordonnance (OCB). La législation implique l'obtention d'un permis de la part du Secrétariat d'État à l'économie (SECO) pour pouvoir exporter ou importer des technologies ou logiciels pouvant être utilisés à des fins civiles et militaires. Ces bases légales semblent s'appliquer en priorité aux armements et aux dispositifs militaires. Elles s'appliquent cependant aussi aux transferts transfrontières de logiciels s'appuyant sur des technologies non accessibles au public. À défaut de permis, une responsabilité pénale peut en découler (art. 14 LCB). 801

1427 BSK StGB-NIGGLI/GFELLER, art. 102 N 79 ; HURTADO POZO/GODEL, N 943 ss ; PK StGB-TRECHSEL/JEAN-RICHARD, art. 102 N 19 s ; SARRASIN/PANGRAZZI/MEYER, p. 1084.

1428 BSK StGB-NIGGLI/GFELLER, art. 102 N 79 ; SARRASIN/PANGRAZZI/MEYER, p. 1084.

802 Une responsabilité pénale peut aussi être engagée si une prestataire de gestion de cyberincidents met en circulation un produit en ne respectant pas les exigences techniques en vertu de la LSPro (art. 16 s. LSPro). Il en va de même si elle viole le droit d'auteure d'une autre organisation ou d'autres obligations imposées par la LDA (art. 67 ss LDA), ou encore si elle viole d'autres prescriptions générales ou spécifiques à un secteur[1429].

D. Une conclusion

803 Les collaboratrices des prestataires de gestion de cyberincidents dont GovCERT sont soumises au respect des normes du CP comme le reste des citoyennes. Cela étant, leur pratique peut soulever quelques questions particulières et impliquer la réalisation d'infractions spécifiques.

804 Les infractions en question impliquent la nécessité pour les prestataires de gestion de cyberincidents d'agir systématiquement avec le consentement de leurs clientes lorsqu'elles agissent sur les infrastructures informatiques de ces dernières. Certaines infractions peuvent être réalisées en fonction des prestations concrètes et du rôle des collaboratrices de prestataires de gestion de cyberincidents. En outre, l'organisation au sein de laquelle elles opèrent peut engager sa responsabilité pénale en parallèle ou subsidiairement à celle d'une collaboratrice en fonction des agissements de cette dernière. Finalement, certaines législations spéciales doivent être respectées pour éviter que les collaboratrices d'une prestataire de gestion de cyberincidents ou l'organisation à laquelle elle est intégrée engagent leur responsabilité pénale.

V. Une conclusion au chapitre 5

805 L'activité des prestataires privées de gestion de cyberincidents est largement laissée à la pratique de ces organisations à double casquette (I.A). Les prestataires de gestion de cyberincidents ne sont pas soumises à des exigences minimales légales de cybersécurité en tant qu'infrastructures critiques, sous réserve de certaines obligations applicables aux fabricantes, ou en termes d'obligation de signaler les cyberattaques visant les prestataires privées de

1429 Voir par exemple la contravention en cas de manquement à la décision de l'OFCS de l'informer d'une cyberattaque (art. 74*h* LSI2). Des dispositions pénales existent aussi pour la fournisseuse de services de télécommunications disposant d'une prestataire interne de gestion de cyberincidents qui ne met pas en place les mesures de sécurité imposées à l'art. 48a LTC (art. 53 LTC), ou la prestataire de gestion de cyberincidents interne à une installation nucléaire qui refuserait de fournir à l'autorité de surveillance l'accès aux documents (art. 93 al. 1 litt. a LENu).

gestion de cyberincidents. (I.B). Elles ne sont pas non plus soumises à des exigences légales spécifiques de cybersécurité dans le cadre de leurs prestations. Elles doivent respecter la loi de façon générales et les exigences attendues de ces dernières dépendent largement du contrat qui les lie à leur clientèle et un certain niveau de sécurité dans leurs prestations peut être attendu en fonction du contrat ou des exigences auxquelles sont soumises leurs clientes (I.C). Quelques autres bases légales permettent d'appréhender d'autres aspects de leur pratique connexes à la cybersécurité. Ces bases légales suivent une approche *ex post,* à savoir qu'elles s'appliquent en passant par des responsabilités postérieures, plutôt qu'une approche *ex ante* par des exigences préventives (I.D). En d'autres termes, la loi permet de sanctionner des comportements de la prestataire de gestion de cyberincidents, mais moins de les anticiper et de les empêcher.

L'OFCS exploite en son sein GovCERT, la prestataire de gestion de cyber- 806
incidents suisse. L'OFCS est soumis au principe de la légalité et son activité doit donc être prévue par la loi. La Confédération se réorganise en termes de cybersécurité et l'OFCS remplace le NCSC (II.A). En se basant sur les compétences de la LSI, de son ordonnance et de l'Org-DDPS, l'autorité responsable de l'équipe d'intervention conserve des compétences préventives et réactives, mais également de divulgation coordonnée de vulnérabilité en lien avec la cybersécurité des infrastructures critiques (II.B). L'OFCS et ses collaboratrices faisant partie de la Confédération, elles peuvent engager leur responsabilité sur la base de la LRCF (II.C).

Les évolutions dans l'organisation de la Confédération pour la cyber- 807
sécurité et la sécurité de l'information ainsi que la connexité entre ces deux domaines a donné lieu à la création d'un nouveau service spécialisé de la Confédération pour la sécurité de l'information. Le nouveau service reprend les tâches principales pour l'autoprotection de la Confédération en termes de sécurité de l'information, tâches effectuées en partie par le NCSC de 2019 à fin 2023 (III.A). Sa création importe dans la présente étude, dès lors qu'il dispose de compétences étroitement liées à celles de l'OFCS. L'OFCS, dans la continuité de l'activité du NCSC, va continuer à exercer quelques compétences incombant maintenant au service spécialisé de la Confédération pour la sécurité de l'information jusqu'à ce que ce dernier soit complètement opérationnel. En outre, les deux autorités vont collaborer étroitement dans certaines situations, typiquement lorsque des autorités ou des organisations de la Confédération subissent un cyberincident (III.B). La coexistence du nouveau service spécialisé et de l'OFCS soulève des questions quant à leurs rôles, aux responsabilités qui peuvent découler de leur action et de l'enchevêtrement de leurs compétences.

808 Il existe certes plusieurs lois instituant des responsabilités, que ce soit pour les prestataires privées de gestion de cyberincidents, pour GovCERT ou pour leurs collaboratrices. Différents chefs de responsabilité peuvent typiquement être engagés pour toutes ces expertes (III.A et B). En revanche, ces mécanismes supposent les compétences de nombreuses personnes autres que les expertes afin de pouvoir actionner ces dernières et effectivement voir des conséquences. Il est à déplorer qu'il n'existe pas de mécanisme plus simple et plus direct, avec par exemple des exigences minimales ainsi qu'une autorité compétente pour la cybersécurité afin de pouvoir agir en amont et plus facilement *a posteriori*.

809 Différents fondements légaux existants sont susceptibles d'engager la responsabilité des prestataires de gestion de cyberincidents ou leurs membres, en distinguant selon l'objectif poursuivi par la procédure, la relation entre les parties et le fondement de la responsabilité. Malgré le fait qu'il n'y ait pas réellement d'obligations légales préventives et très peu de lois proactives en matière de cybersécurité, la responsabilité des prestataires privées de gestion de cyberincidents dépend de la loi en fonction des contrats, des actes commis et ainsi de suite. Les prestataires de gestion de cyberincidents privées et publiques sont susceptibles de devoir répondre si elles ne se comportent pas de la façon adéquate.

810 Cela étant, plusieurs problèmes existent. Tout d'abord, la diligence due dans les différentes situations est à l'heure actuelle difficile à mesurer. Ensuite, les bases légales sont dispersées et incomplètes. De plus, bien que les infrastructures critiques disposent normalement de connaissances juridiques et sont plus à même de connaître le meilleur levier d'action en fonction des circonstances, ce n'est pas toujours le cas. En outre, les prestataires de gestion de cyberincidents doivent être hautement spécialisées dans le domaine de la cybersécurité et leur clientèle ne peut connaître que difficilement le niveau de diligence dont elles doivent faire preuve dans leur activité. Le même problème se pose lorsque des entreprises disposant de peu de moyens font appel à des prestataires de gestion de cyberincidents. Finalement, les bases légales applicables à l'OFCS peuvent soulever des questions de clarté, d'opportunité et questionner sur la potentielle insuffisance du cadre légal et du mandat de l'OFCS.

811 Les bases légales applicables aux prestataires de gestion de cyberincidents ne sont pas suffisantes en termes d'exigences minimales de cybersécurité et la loi intervient bien plus de façon réactive que de façon proactive. Cela étant, au-delà des exigences de cybersécurité applicables à leur clientèle, au droit des contrats, au droit des marchés publics et aux bases légales fondant l'activité de l'OFCS, des exigences connexes à la cybersécurité s'appliquent à l'activité de toutes les prestataires de gestion de cyberincidents. Ces différentes bases légales illustrent l'importance de la protection des informations dans le

contexte de la cybersécurité. Cette dernière étant réglementée de façon limitée, nous allons voir comment le cadre légal applicable à la sécurité de l'information et à la protection de différentes informations peut apporter des éléments de lumière ainsi que d'inspiration.

Chapitre 6 : la protection des informations au centre de la gestion de cyberincidents

Préambule au chapitre 6

La cybersécurité couvre la sécurité informatique et se recoupe en grande partie avec la sécurité de l'information[1430]. La sécurité de l'information et la sécurité informatique sont donc au centre de l'activité des différentes organisations. Alors que la seconde n'est que rarement réglementée, la première, plus ancienne, l'est davantage, en fonction des personnes traitant les informations ou encore du type d'informations traitées. Les bases légales existantes pour protéger l'information sont centrales dans un contexte comme celui de la cybersécurité et plus particulièrement de l'activité de prestataires de gestion de cyberincidents. 812

La sécurité de l'information doit être assurée au même titre que la cybersécurité. Au-delà des normes existantes pour que les infrastructures critiques garantissent la sécurité de l'information, certains types d'informations font l'objet de protections garanties par différentes bases légales dans l'ordre juridique suisse. 813

Les informations et leur protection sont, dans un contexte de cybersécurité, centrales à la gestion de cyberincidents[1431]. D'une part, elles constituent l'un des objets à protéger. D'autre part, les personnes et organisations intervenant dans la gestion de cyberincidents doivent assurer leur protection dans leur activité et doivent éviter de les mettre en péril. 814

En outre, la coopération est l'un des piliers d'une protection efficace, ce qui implique de nombreux échanges d'informations. La réaction face aux cybermenaces implique régulièrement une étroite collaboration entre différentes intervenantes[1432]. La sécurité participative est considérée comme 815

1430 Cf. *supra* N 48.

1431 Et les mesures de la sécurité de l'information sont étroitement liées et doivent être coordonnées avec les mesures de cybersécurité ou de protection des données personnelles, cf. HUSI-STÄMPFLI, N 91 et 95 dans un ordre d'idées similaire.

1432 Il est effectivement nécessaire de trouver des réponses adaptées compte tenu des différents secteurs touchés, cf. SKOPIK/SETTANNI/FIEDLER, p. 157.

centrale, prônant une collaboration étroite par le biais de communautés tant internes qu'externes[1433].

816 L'accent est mis ici sur les prestataires de gestion de cyberincidents, ces dernières constituant les intervenantes principales dans la gestion de cyberincidents. Différentes informations sont concernées par la gestion de cyberincidents et certaines d'entre elles nécessitent une protection particulière (I). Les bases légales applicables à la sécurité de l'information passent notamment par la classification de certaines informations (II). La protection des données personnelles est largement réglementée à l'heure actuelle, ce qui implique la protection de ce type d'informations par le respect de différents principes et obligations (III). Finalement, les informations couvertes par des secrets doivent être protégées dans une certaine mesure (IV). La pratique de gestion de cyberincidents a développé des outils pour chercher à assurer la protection de ces informations, mais également des autres informations non protégées par la loi (V).

I. Les informations et leur protection

A. Les informations

817 Les informations à protéger et à traiter dans le cadre de la gestion de cyberincidents peuvent être plus ou moins sensibles. La sensibilité d'une information peut typiquement dépendre de facteurs tels que sa nature, du moment de son cycle de vie ou de l'écoulement du temps[1434]. Les informations à protéger sont par exemple des données personnelles ou des informations couvertes par des secrets[1435]. Il peut également s'agir de données techniques ou de données non personnelles de façon plus générale. Ces dernières notions comprennent les données ne permettant pas d'identifier une personne ou de la rendre identifiable, les données anonymisées[1436], ou encore d'autres types de données ne se rapportant initialement pas à des personnes. Les informations techniques incluent les descriptions d'architectures informatiques, les descriptions de

1433 NCSC, *Rapport semestriel 2021/1*, 2021, p. 6.

1434 SALAMON, p. 36.

1435 Les notions « donnée » et « information » sont souvent utilisées comme synonymes ; pour une analyse des notions, cf. HUS-STÄMPFLI, N 6 ss. La présente étude se cantonne à utiliser le terme d'« information » pour regrouper les différents types d'informations, comme les données personnelles, et ce bien que la notion d'information ne soit pas définie dans la LSI, cf. FF 2017 2821 ; HUSI-STÄMPFLI, N 14 et 21.

1436 Sur les notions de données anonymisées et pseudonymisées, cf. notamment PC LPD-JACOT-GUILLARMOD, art. 5 N 15 ss.

systèmes informatiques ou leur documentation ou les documents indiquant les exigences posées à des applications[1437]. Entrent également dans cette notion les données environnementales, les données statistiques ou les données générées automatiquement par des machines relatives à une chaîne de production industrielle[1438].

818 Les informations traitées et communiquées dans la gestion de cyberincidents comprennent les informations relatives aux cybermenaces qui permettent aux différentes interlocutrices de se protéger et lutter contre celles-ci[1439]. Il s'agit souvent de données techniques, qui couvrent notamment les données statistiques générées de manière automatique par des machines ou relatives à l'utilisation d'un produit[1440]. Les prestataires de gestion de cyberincidents peuvent se partager entre elles aussi des indicateurs d'incidents (à l'instar des caractéristiques générales d'une attaque), des statistiques, des scénarii communs d'attaques ou encore des profils d'attaques[1441]. Il peut en effet être utile d'utiliser d'autres indicateurs d'incidents que ceux collectés par une organisation elle-même. C'est par ailleurs par le biais de la participation à plusieurs groupes d'échanges et de confiance que les expertes en cybersécurité échangent des idées ainsi que des bonnes pratiques pour tenter d'avoir une longueur d'avance sur les délinquantes[1442].

819 De nombreux types d'informations tombent sous cette catégorie. Elles peuvent être constitutives de données personnelles ou non. Les données techniques principalement partagées par les prestataires de gestion de cyberincidents peuvent l'être sous la forme de données brutes *(raw data)* ou sous la forme de rapports de renseignements (*cyber threat intelligence,* CTI), lorsqu'elles sont le produit d'une analyse d'éléments relatifs aux cyberincidents, attaques, actrices malveillantes ou vulnérabilités[1443]. Les informations peuvent consister en des IOC, des indicateurs d'attaques (*indicators of attacks,* IOA) ou encore des tactiques, techniques et procédures (*tactics, techniques, and procedures,* TTP).

1437 OFCS, *Rapport concernant les analyses de données effectuées après la cyberattaque contre l'entreprise Xplain*, 2024, p. 8.

1438 IPI, *Accès aux données non personnelles dans le secteur privé,* 2021, p. 6 ; DE WERRA, p. 371.

1439 RASHID/NOOR/ALTMAN, p. 443.

1440 JACCARD/ANCELLE, p. 1.

1441 Pour des exemples de flux d'informations passant par les prestataires de gestion de cyberincidents, cf. WEST-BROWN et al., p. 37.

1442 NCSC, *Rapport semestriel 2021/1,* 2021, p. 6.

1443 RASHID/NOOR/ALTMAN, p. 443 ; SALAMON, p. 124 s. Pour un exemple d'échange d'informations notamment sous forme de *threat intelligence* dans le sous-secteur de l'approvisionnement en électricité, voir OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »,* 2021, p. 110.

820 Les IOC consistent en des artéfacts signalant une opération malicieuse sur un système informatique. Ils permettent d'identifier des éléments malicieux dans des systèmes informatiques, à l'instar de commandes, adresses IP ou courriels malicieux. Ils peuvent également inclure des informations permettant aux destinataires de savoir si un élément malicieux leur est utile ou non, ainsi que des informations quant à la durée, l'intérêt porté à l'indicateur et à des incidents en lien avec les personnes malveillantes[1444].

821 Les IOA sont des artéfacts observés sur des systèmes permettant de supposer une attaque ou une tentative d'attaque. Les IOA ont une portée plus proactive que les IOC. Ils ne permettent pas de tirer la conclusion, contrairement aux IOC, qu'un système a effectivement été compromis. Ces indicateurs couvrent typiquement des tentatives de connexion dans le système de journalisation d'un pare-feu indiquant l'utilisation d'outil de reconnaissance de réseau[1445].

822 Les TTP englobent une série d'informations servant à décrire la méthodologie, le comportement et les capacités d'attaquantes (tactiques). Elles contiennent les informations mettant en relation le comportement malveillant avec le contexte de l'approche suivie (techniques) et des descriptions détaillées de leurs techniques (procédures). Ces informations incluent également les outils utilisés, l'ordre des opérations, le type d'entreprises ainsi que les vulnérabilités visées, les *delivery mechanisms* ou les *exploits* utilisés. Parmi ces informations échangées figurent aussi des informations sur les actrices malveillantes ou *threat actors,* en les basant notamment sur les objectifs qu'elles poursuivent, leur association à des groupes criminels ou à des États étrangers, leurs capacités et autres caractéristiques[1446].

823 Les prestataires de gestion de cyberincidents partagent ou publient souvent, dans des cercles de destinataires plus ou moins fermés, des rapports sur des vulnérabilités de logiciel, de matériel, de processus ou d'infrastructures informatiques[1447]. Certaines prestataires de gestion de cyberincidents, comme celle exploitée par l'OFCS, partagent aussi des informations relatives à des pratiques opérationnelles de cybersécurité ainsi qu'à la configuration d'outils ou de paramètres de sécurité de systèmes[1448].

1444 JOHANSEN, p. 432 ; RASHID/NOOR/ALTMAN, p. 443.

1445 JOHANSEN, p. 432.

1446 JOHANSEN, p. 432 ; RASHID/NOOR/ALTMAN, p. 443 s. ; SALAMON, p. 82 ss.

1447 RASHID/NOOR/ALTMAN, p. 444.

1448 RASHID/NOOR/ALTMAN, p. 443.

B. Les garde-fous

Ces informations peuvent revêtir ou non un intérêt particulier et mériter une certaine protection légale. Les informations deviennent dignes de protection lorsque la détentrice initiale (ou le pouvoir législatif) estime qu'elles pourraient devenir intéressantes ou précieuses pour d'autres personnes et qu'elles ne doivent pas être communiquées à tout va[1449]. 824

Certaines de ces informations doivent être protégées en vertu de la loi. Il en va de la sorte des informations classifiées au sens de la LSI, des données personnelles ou encore d'informations couvertes par divers secrets. La loi attribue à ces dernières un caractère spécial et leur traitement est légalement encadré. 825

Ces mécanismes de protection peuvent également avoir un impact sur des informations techniques qui ne sont, de prime abord, pas protégées par la loi. Les informations techniques, à l'instar du nombre d'incidents gérés, du temps utilisé pour la gestion de cyberincidents, ou encore de l'évaluation de la réponse à ceux-ci, peuvent contenir des potentielles données personnelles sous la forme de ressources d'adressage. Ces informations ne se limitent donc pas toujours à des données techniques non personnelles sur les outils et ressources, des données sur la cause de l'incident, de son vecteur d'attaque, des vulnérabilités exploitées et ainsi de suite[1450]. Les prestataires de gestion de cyberincidents doivent tenir compte de la loi dans le traitement et la communication d'informations techniques également. Alors que les données purement techniques peuvent en principe être librement communiquées, tel n'est pas le cas de données techniques couvertes par un secret, typiquement de fabrication ou de fonction. De la même manière, les données permettant d'identifier ou de rendre identifiable une personne (physique ou morale) ne peuvent être traitées et communiquées que moyennant le respect de certains principes et obligations. 826

De manière générale, la proportionnalité est toujours de mise dans les échanges dans ce domaine. Il est important que les différentes émettrices tiennent constamment compte du *« need to know »* des potentielles destinataires quant à une information, technique, soumise à une obligation de confidentialité ou contenant une donnée personnelle. 827

1449 Dans un sens similaire, HUSI-STÄMPFLI, N 11.

1450 NIST, *Computer Security Incident Handling Guide*, 2012, p. 40 s.

C. En résumé

828 Les informations traitées dans le cadre de la gestion de cyberincidents sont d'une grande diversité. De nombreuses informations techniques sont traitées et échangées. Entrent dans cette terminologie les IOC, les IOA, les TTP ainsi que les celles relatives à des vulnérabilités ou aux bonnes pratiques.

829 Certaines informations revêtent des caractéristiques particulières et sont protégées par la loi. Il en va de la sorte pour les celles revêtant un certain niveau de sensibilité devant être classifiées au sens de la LSI. Les données personnelles sont également protégées par la loi. Les informations couvertes par des secrets doivent aussi être protégées dans une certaine mesure. Il s'agit maintenant d'exposer concrètement quelles lois protègent ces différentes informations.

II. La sécurité de l'information dans la LSI

A. Les mesures garantissant la sécurité de l'information

830 La LSI met, surtout dans sa première version, un accent important sur la sécurité de l'information au sein de la Confédération. Ce faisant, elle allie les mesures techniques (relevant en partie de la garantie de la sécurité informatique) et les mesures organisationnelles garantissant la sécurité de l'information[1451]. La raison derrière cette orientation est que la Confédération traite continuellement des volumes importants d'informations, dont des informations cruciales pour la sécurité intérieure et extérieure ou encore pour les intérêts économiques ainsi que les relations internationales de la Suisse[1452].

831 Les personnes dirigeantes sont les premières concernées par les obligations relatives à la sécurité de l'information. Pour assurer la confidentialité, la disponibilité, l'intégrité et la traçabilité des ces dernières (art. 6 al. 2 LSI)[1453], les autorités et organisations soumises à la loi doivent veiller à l'évaluation du besoin de protection des informations relevant de leurs compétences en fonction de l'atteinte potentielle aux intérêts de l'art. 2 al. 1 LSI. Les autorités soumises à la LSI sont responsables de la sécurité de l'information (art. 7 LSI). Elles doivent évaluer les risques et prendre les mesures nécessaires pour les éliminer ou les ramener à un niveau acceptable (art. 8 LSI) ainsi que veiller à ce que les mesures implémentées soient reprises dans les accords et les contrats avec

1451 FF 2017 2765, p. 2784.

1452 FF 2017 2765, p. 2775.

1453 FF 2017 2765, p. 2827 s. ; HUSI-STÄMPFLI, N 29.

les personnes tierces (art. 9 LSI). Elles doivent également gérer les potentielles violations de la sécurité de l'information (art. 10 LSI).

Les mesures se fondent sur une gestion des risques par les autorités et organisations concernées et sont concrétisées par l'OSI[1454]. Une des mesures permettant d'appréhender les différents aspects de la gestion de risques pour les informations traitées est l'adoption d'un système de gestion de la sécurité de l'information (SGSI) en vertu de l'art. 5 OSI. Ce système doit contenir les objectifs en matière de sécurité de l'information, l'ensemble des procédures, des règles, des mesures et des outils définis pour organiser la sécurité de l'information au sein des unités administratives[1455]. 832

B. La classification d'informations

La LSI reprend et précise la classification qui existe depuis longtemps pour que les informations classifiées bénéficient d'une protection particulière[1456]. La classification sert à garantir la protection des informations dont l'accès non autorisé peut nuire à l'accomplissement de tâches ou porter préjudice à des intérêts selon différents niveaux. Elle constitue une exception au principe de transparence. Elle ne doit pas être systématique en raison notamment des coûts qu'elle engendre[1457]. 833

Le cadre légal suisse impose aujourd'hui une classification aux autorités et organisations soumises à la LSI (art. 11 ss LSI et 16 ss OSI). Le pouvoir législatif suisse a limité le cercle des personnes habilitées à prendre connaissance des informations classifiées « secret », « confidentiel » ou « interne ». Ne peuvent accéder à ces informations que les personnes qui offrent d'une part les garanties qu'elles traiteront correctement les données et, d'autre part, qui, alternativement, en ont besoin pour accomplir une tâche légale ou disposent d'une autorisation d'accès convenue contractuellement et nécessitent d'avoir accès à ces informations pour effectuer des tâches confiées (art. 14 al. 1 LSI). Les 834

1454 FF 2017 2765, p. 2789 s. Sur ces mesures, cf. également *supra* N 382 ss.

1455 SG-DDPS, *Législation d'exécution relative à la LSI, Explications,* 2023, p. 11 s. Pour plus d'information sur les SGSI dans ce contexte, cf. HUSI-STÄMPFLI, N 38 ss. Voir à ce titre le concept SGSI de l'administration fédérale dans la méthode HERMES, cf. CHANCELLERIE FÉDÉRALE, *HERMES Online, Concept SIPD*. Le SEPOS doit examiner d'ici l'été 2025 s'il est nécessaire d'obliger les unités administratives à utiliser une application SGSI standard pour la gestion de leur sécurité, cf. SERVICE SPÉCIALISÉ DE LA CONFÉDÉRATION POUR LA SÉCURITÉ DE L'INFORMATION, *Train de mesures pour éviter de nouvelles fuites de données,* 2024, p. 4.

1456 FF 2017 2765, p. 2775 et 2790.

1457 FF 2017 2765, p. 2832 ; HUSI-STÄMPFLI, N 35.

garanties portent sur la capacité de la personne accédant aux informations à respecter les mesures techniques et physiques de sécurité. Si le droit d'accès a été convenu contractuellement, il doit prévoir, outre l'accès aux informations concernées, les modalités de leur traitement[1458]. Par conséquent, les informations classifiées selon la LSI ne peuvent être transmises que moyennant le respect de ces conditions.

835 Pour l'OFCS, cette classification entraîne deux conséquences principales. L'OFCS a d'une part un droit à accéder aux informations classifiées des autorités qu'il sert aux conditions de l'art. 14 al. 1 LSI. D'autre part, il est dans l'obligation de classifier les informations qu'il traite et d'en assurer la sécurité.

836 Pour prétendre à un droit d'accès à ces informations, l'OFCS doit apporter des garanties suffisantes quant à sa façon de traiter les informations classifiées détenues initialement par les autorités qu'il sert. Pour les cas dans lesquels il a besoin d'informations classifiées pour accomplir une tâche légale relative à sa fonction, il réunit l'une des conditions alternatives s'ajoutant à la première condition susmentionnée, plus spécifiquement la condition du besoin des informations pour accomplir une tâche légale. Ses tâches légales découlent des art. 73*a* ss LSI2[1459].

837 L'OFCS, contrairement aux prestataires privées de gestion de cyberincidents, est *a priori* soumis aux obligations de classifier certaines informations en vertu des art. 11 à 15 LSI. L'office doit procéder en fonction du risque que la divulgation des informations est susceptible de causer à des intérêts publics tels que la sécurité publique (liste des intérêts concernés à l'art. 1 al. 2 LSI)[1460] et respecter la classification créée par d'autres autorités. Cette classification protège certaines informations revêtant un haut niveau d'importance pour l'État[1461]. Concrètement, elle doit être limitée au nécessaire et, dans la mesure du possible, être temporaire (art. 11 al. 2 LSI). Les échelons de classification sont déterminés par la gravité du préjudice que la divulgation d'informations à une personne non autorisée serait susceptible d'engendrer pour les intérêts de l'art. 1 al. 2 litt. a à d LSI, à savoir pour la capacité de décision et d'action des autorités et organisations de la Confédération, la sécurité intérieure et extérieure de la Suisse, les intérêts de la politique extérieure du pays ou de ses intérêts économiques, financiers et monétaires. Dans cette logique, l'OFCS doit classifier certaines informations comme suit (art. 13 LSI) :

1458 FF 2017 2765, p. 2836 ; OA, *Enquête administrative « Fuite de données »*, 2024, N 248 ss.

1459 Cf. *supra* N 703 ss.

1460 Sur ces intérêts, cf. HUSI-STÄMPFLI, N 31.

1461 À titre de comparaison, il existe typiquement au niveau européen la décision du 23 septembre 2013 du Conseil sur les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne.

— « internes » lorsque leur divulgation est susceptible de nuire aux intérêts de l'art. 1 al. 2 litt. a à d (art. 18 OSI) ;
— « confidentielles » lorsque leur divulgation peut nuire considérablement à ces intérêts (art. 19 OSI) ;
— « secrètes » lorsque leur divulgation est susceptible de nuire gravement à ces intérêts (art. 20 OSI).

838 Tout d'abord, pour qu'une information doive être classifiée à l'échelon « interne », il faut que sa divulgation à une personne non autorisée puisse être à l'origine d'un dommage potentiel qualifié ou sensible[1462]. Ensuite, il convient de prévoir une classification « confidentielle » dans le cas où un dommage plus perceptible et important peut être engendré. Tel est le cas lorsqu'une organisation soumise à LSI est temporairement dans l'incapacité d'agir, que certaines ressources de l'armée ou d'organes de sécurité de la Confédération ne peuvent temporairement être engagées ou lorsque la Confédération risque de subir un préjudice financier « considérable »[1463]. Finalement, l'information doit être classifiée comme « secrète » lorsque le dommage susceptible d'être engendré est particulièrement grave, voire catastrophique. Ce serait typiquement le cas lorsque la fourniture par des infrastructures critiques de prestations indispensables est interrompue, que la vie ou l'intégrité de certains groupes de population sont menacées, si certaines fonctions sensibles d'une centrale nucléaire sont hors d'usage à la suite d'un sabotage ou encore si la Confédération risque un « grave » préjudice financier[1464]. Ces divers exemples illustrent la mesure dans laquelle l'OFCS pourrait être amené à classifier ou avoir accès à de telles informations.

839 Pour les autres prestataires de gestion de cyberincidents, les conséquences de la classification mise en place par la LSI ne sont pas si évidentes. Les prestataires privées de gestion de cyberincidents ne sont, en tant que telles, pas soumises à l'obligation de classifier les informations qu'elles traitent. Elles peuvent être soumises à l'obligation de classifier si elles sont internes à une organisation ou une autorité de la Confédération, ou si elles peuvent être assimilées à ce cercle d'organisations soumises à l'obligation de classifier. En revanche, toutes les équipes de gestion de cyberincidents (internes comme externes) peuvent nécessiter un accès à des informations classifiées de la Confédération, en fonction de certains facteurs à l'instar de leur clientèle ou de certains incidents. Celles-ci peuvent accéder aux informations classifiées

1462 FF 2017 2765, p. 2834 s.
1463 FF 2017 2765, p. 2835.
1464 FF 2017 2765, p. 2835.

par les autorités soumises à la LSI si elles apportent les garanties qu'elles traiteront correctement ces informations, si elles disposent d'une autorisation d'accès confiée contractuellement et si elles nécessitent en outre d'accéder à ces informations pour accomplir les tâches confiées (art. 14 al. 1 litt. b LSI). Pour qu'une prestataire de gestion de cyberincidents puisse accéder aux informations classifiées, il faut que l'autorisation d'accès et le règlement du traitement des informations concernées soient prévus contractuellement et que cet accès soit nécessaire pour que la prestataire puisse accomplir les tâches qui lui ont été confiées. En d'autres termes, lorsqu'elles offrent leurs prestations à une organisation ou à une autorité soumise à la LSI, elles ne peuvent accéder aux informations classifiées qu'à condition qu'elles offrent les garanties d'un traitement correct des données et, cumulativement, qu'elles disposent d'une autorisation d'accès convenue contractuellement et nécessitent d'avoir accès à ces informations pour effectuer des tâches confiées. La gestion des cyberincidents entrant dans la majorité des exigences légales applicables aux entités soumises à la LSI, l'on pourrait accorder aux prestataires de gestion de cyberincidents l'accès à ces informations sur cette base lorsque c'est nécessaire à leur activité[1465].

C. D'autres mesures

840 D'autres informations que celles classifiées nécessitent une certaine protection[1466]. Les mesures de sécurité des moyens informatiques (art. 17 à 19 LSI) servent *in fine* à la sécurité de l'information. Il en va de même pour les mesures concernant le personnel et les mesures physiques de protection. Entrent typiquement dans ces mesures la formation des personnes pour traiter des informations classifiées ou l'octroi d'autorisations pour accéder aux locaux et utiliser des moyens informatiques permettant l'accès aux informations ou aux systèmes d'information. D'autres mesures intégrées dans la loi comme les contrôles de sécurité des personnes ou les procédures de sécurité relatives aux entreprises visent des objectifs similaires. Ces mesures cherchent respectivement à éviter des actes malveillants à l'interne et à assurer la sécurité de l'information dans le cadre de l'attribution de mandats à des tierces[1467].

1465 À noter que l'existence d'une classification n'implique pas directement que les documents classifiés soient soustraits du principe de transparence, cf. FF 2017 2765, p. 2790.

1466 FF 2017 2765, p. 2775.

1467 FF 2017 2765, p. 2791 ss.

D. Une synthèse

La LSI cherche dans sa première version principalement à assurer la sécurité 841
des informations traitées par la Confédération[1468]. La loi prévoit les responsabilités pour la sécurité de l'information ainsi que des principes et obligations pour la sécurité de l'information, dont l'adoption d'un SGSI par les unités administratives.

La LSI prévoit également la classification d'informations selon trois échelons de protection. Cette classification a pour principales conséquences la responsabilisation des autorités et organisations soumises à la loi et la limitation des personnes autorisées à y accéder. 842

D'autres mesures contribuent à la sécurité de l'information dans le cadre 843
de la LSI. Les mesures servant à garantir la sécurité des moyens informatiques poursuivent la finalité de sécuriser les informations traitées par le biais de moyens informatiques. Les mesures physiques de protection ou les contrôles de sécurité des personnes ou les procédures de sécurité relative aux entreprises contribuent également à la sécurité des informations au sein de la Confédération.

III. La protection des données personnelles

A. Une remarque introductive

Les personnes intervenant dans la gestion de cyberincidents doivent être 844
attentives aux données personnelles qu'elles traitent dans leur activité. En droit suisse, le principal instrument pour la protection des données personnelles est la LPD, entrée en vigueur en 1992 et révisée en 2020. Elle prévoit plusieurs principes et obligations à respecter par les responsables du traitement ou sous-traitantes privées et par les organes fédéraux. Partant, de nombreuses infrastructures critiques et prestataires de gestion de cyberincidents sont, comme l'OFCS, susceptibles d'être soumises à cette loi.

Lors d'un cyberincident, les informations traitées par une responsable 845
du traitement sont susceptibles d'être compromises. Dans le cas d'une cyberattaque, c'est par ailleurs souvent le but poursuivi par l'intruse. Parmi ces informations figurent régulièrement des données personnelles, à l'instar de données d'identification, de données médicales en cas de cyberincident

1468 La version révisée de la loi porte principalement sur la cybersécurité des infrastructures critiques et le rôle de l'OFCS pour la cybersécurité et n'ajoute pas de considérations particulières pour la sécurité de l'information au sein de la Confédération.

touchant un établissement hospitalier, de données financières lors d'un incident auprès d'un établissement bancaire ou encore de relevés électroniques de compteur d'eau lors d'une attaque visant une installation d'approvisionnement en eau[1469].

846 À noter que la présente étude se concentre sur le droit fédéral, raison pour laquelle la LPD est utilisée comme exemple. Néanmoins, il faut garder en tête que les lois cantonales de protection des données, qui prévoient en principe un fonctionnement similaire à ce qui est prévu pour les organes fédéraux au sein de la LPD, conservent une importance primordiale pour certains secteurs et sous-secteurs critiques. Il n'est pas impossible que certaines prestataires de gestion de cyberincidents, par exemple actives au sein d'une administration cantonale ou d'un établissement médico-hospitalier cantonal, soient soumises à des lois cantonales. En outre, certaines prestataires de gestion de cyberincidents peuvent être soumises à la fois à la LPD et à d'autres réglementations à l'instar du RGPD.

B. La distinction entre un organe fédéral et une responsable du traitement privée

847 Le cadre légal en matière de protection des données diffère en Suisse en fonction de la qualité de la personne traitant des données personnelles. La distinction est opérée entre les organes fédéraux et les personnes privées, qui n'ont pas les mêmes obligations et qui ne répondent pas exactement aux mêmes principes.

848 L'OFCS est une autorité centralisée de la Confédération. Partant, l'OFCS est un organe fédéral au sens de l'art. 5 litt. i LPD[1470].

849 La situation n'est pas aussi claire pour les autres prestataires de gestion de cyberincidents. La distinction a déjà été opérée au sein de la présente étude entre les fournisseuses internes et externes de prestations de gestion de cyberincidents. La prestataire de gestion de cyberincidents interne à une autorité considérée comme un organe fédéral au sens de l'art. 5 litt. i LPD, doit être perçue comme un organe fédéral et soumise aux dispositions spécifiques. À ce titre, elle ne peut traiter des données personnelles que si une loi le lui permet

1469 Le TF a estimé que les données relatives à la consommation d'eau étaient des données personnelles lorsqu'il était possible de les rattacher à des habitantes, cf. ATF 147 I 346, c. 5.3.1.

1470 BSK DSG-BLECHTA/DAL MOLIN/WESIAK-SCHMIDT, art. 5 N 173 ss ; CR LPD-MÉTILLE/DI TRIA, art. 2 N 36. GovCERT composant uniquement l'un de ses services et n'ayant pas de pouvoir décisionnel, c'est bien l'OFCS qui est responsable du traitement ; GovCERT en fait simplement partie.

en vertu du principe de la légalité posée à l'art. 34 LPD. L'art. 10*a* al. 1 LSI2 habilite par exemple les autorités et organisations soumises à la LSI à traiter des données personnelles utiles à la sécurité de l'information[1471].

La prestataire de gestion de cyberincidents interne à une responsable du traitement privée est, selon le même raisonnement établi pour un organe fédéral, une responsable du traitement privée. Il est possible qu'une prestataire soit interne à une organisation qualifiée pour certains traitements de données personnelles comme organe fédéral et pour d'autres comme responsable du traitement privée[1472]. La qualification de la fournisseuse interne de prestations doit suivre celle de l'organisation au sein de laquelle elle œuvre. Par exemple, les Chemins de fer fédéraux (CFF) sont assimilés à un organe fédéral pour les activités en relation avec la concession publique qu'ils ont ou avec le domaine public sur lequel ils exercent leur activité, contrairement à leur activité lorsqu'ils agissent dans un cadre de droit privé[1473]. La prestataire interne aux CFF fait partie d'un organe fédéral pour les traitements de données en relation avec la concession publique, et comme faisant partie d'une responsable du traitement privée si elle traite des données personnelles compromises par une attaque visant une autre activité des CFF, à l'instar de la location d'immeubles. 850

La prestataire externe privée de gestion de cyberincidents travaille en tant que prestataire de service de sécurité informatique. Le fait qu'elle soit une infrastructure critique ne revient pas à affirmer qu'elle doit être considérée comme un organe fédéral au sens de la LPD. De nombreuses organisations privées sont effectivement considérées comme des infrastructures critiques[1474]. La fournisseuse externe de prestations de gestion de cyberincidents ne devrait pas non plus être considérée comme un organe fédéral en raison de l'exécution d'une tâche publique (art. 5 litt. i LPD et 2 al. 4 LOGA). La loi ne confie effectivement pas la cybersécurité de la Confédération aux prestataires de services informatiques[1475]. Chaque autorité et organisation est responsable d'assurer sa cybersécurité. La prestataire externe de gestion de cyberincidents peut en revanche agir en tant que sous-traitante, ce qui a pour conséquence qu'elle doit respecter les obligations et le régime applicable à l'organisation à laquelle elle fournit ses prestations. 851

1471 FF 2023 84, p. 24 s.

1472 MÉTILLE/DI TRIA, art. 2 N 38.

1473 Sur le double statut des CFF, cf. MÉTILLE/DI TRIA, art. 2 N 39 ; MEIER, N 603.

1474 Cf. notamment OFPP, *Factsheet zum kritischen Teilsektor IT-Dienstleistungen*, 2012, p. 1.

1475 Contrairement à d'autres situations, cf. notamment les exemples de CR LPD-MEIER/TSCHUMY, art. 5 N 104 ; PC LPD-JACOT-GUILLARMOD, art. 5 N 56.

852 En termes d'obligations spécifiques, la distinction implique que les prestataires privées de gestion de cyberincidents sont soumises aux dispositions des art. 30 ss LPD, alors que l'OFCS et les fournisseuses internes à des autorités ou organisations étatiques doivent respecter en outre les art. 33 ss LPD[1476].

C. Une responsable du traitement ou une sous-traitante

1. Les responsables du traitement et les sous-traitantes

853 Une entreprise fournissant des prestations de gestion de cyberincidents agissant en tant que sous-traitante pour ses clientes n'est pas *de facto* soumise aux mêmes obligations et n'assume pas la même responsabilité ou le même contrôle que celle agissant en tant que responsable du traitement, conjointe ou non.

854 La responsable du traitement est la personne privée ou l'organe fédéral déterminant les finalités et les moyens du traitement de données personnelles (art. 5 litt. j LPD). La responsable du traitement est la personne, physique ou morale, qui a le contrôle sur les données, à savoir celle qui décide de la création, du but, des moyens d'un traitement et de la ou des catégorie(s) de données personnelles que ce dernier va concerner[1477]. Il n'est pas exclu que plusieurs personnes soient responsables du traitement conjointes ou indépendantes[1478]. La responsable du traitement a notamment comme obligation d'assurer la protection des données dès la conception et par défaut (art. 7 al. 1 et 3 LPD) ou l'obligation de s'assurer du respect de la sécurité des données par son éventuelle sous-traitante (art. 9 al. 2 LPD). C'est à celleci que reviennent également le devoir d'information de l'art. 19 ss LPD, l'obligation de mener une analyse d'impact (art. 22 s. LPD) lorsque les conditions en sont réunies ou encore l'obligation d'annonce des violations de la sécurité des données à la PFPDT ou aux personnes concernées (art. 24 LPD)[1479].

1476 PC LPD-JACOT-GUILLARMOD, art. 5 N 54.

1477 BSK DSG-BLECHTA, art. 3 N 86 ; BSK DSG-BLECHTA/DAL MOLIN/WESIAK-SCHMIDT, art. 5 N 182 ss ; MEIER, N 581 et 583 ; PC LPD-JACOT-GUILLARMOD, art. 5 N 62 ss ; RUDIN, art. 3 DSG N 49.

1478 BSK DSG-BLECHTA/DAL MOLIN/WESIAK-SCHMIDT, art. 5 N 186 ; CR LPD-MEIER/TSCHUMY, art. 5 N 110 ; MEIER, N 588. Pour admettre une responsabilité conjointe, l'intervention de chacune des parties doit avoir un effet concret sur la détermination des finalités et des modalités clés du traitement, et le traitement par chacune ne doit pas pouvoir être conçu sans l'autre. C'est le cas par exemple lorsque le traitement sert à la réalisation d'un objectif commun, cf. PC LPD-JACOT-GUILLARMOD, art. 5 N 66 et références citées.

1479 Pour d'autres obligations incombant spécifiquement à la responsable du traitement, cf. CR LPD-MEIER/TSCHUMY, art. 5 N 111.

La responsable du traitement peut faire appel à une sous-traitante, à qui elle délègue une ou plusieurs opérations de traitement[1480]. La sous-traitante est la personne privée ou l'organe fédéral traitant des données personnelles pour le compte de la responsable du traitement (art. 5 litt. k LPD)[1481]. Elle traite des données en fonction des instructions de la responsable du traitement qui définit les limites de l'utilisation des données autorisée par la sous-traitante[1482]. L'enjeu de la qualification se trouve dans les questions d'obligations applicables et de responsabilités. 855

Pour déterminer si l'OFCS et les autres prestataires de gestion de cyberincidents agissent en tant que responsables du traitement (individuelles ou conjointes) ou comme sous-traitantes, la question de la détermination des moyens et finalités du traitement est déterminante. Concrètement, il faut se demander si elles ont le contrôle sur le traitement de données personnelles. Plusieurs éléments peuvent être pris en considération. À titre d'exemples, la question d'un potentiel contrat entre les prestataires et les personnes concernées ou le pouvoir de disposer des données peuvent servir d'indicateurs[1483]. 856

2. L'Office fédéral de la cybersécurité

L'activité de l'OFCS est réglementée aux art. 73*a* ss LSI2[1484]. Il traite, notamment par le biais de son équipe d'intervention, des données personnelles dans le cadre de la gestion de cyberincidents lorsqu'une organisation fait appel à son soutien. Néanmoins, par la nouvelle obligation de signaler les cyberincidents des art. 74*a* ss LSI2, les infrastructures critiques qui y sont soumises sont tenues de transmettre des données à l'OFCS qui les traitent à des fins prévues par la loi. À la différence d'une CSIRT non gouvernementale, l'OFCS poursuit, dans son soutien à la gestion de cyberincidents, l'intérêt public de sécurité du pays. Cette mission lui octroie davantage de pouvoirs, par exemple en ce qui concerne les traitements de données qu'elle peut effectuer, qui peuvent différer de ceux que l'organisation, confrontée à un incident, peut effectuer. Il a en outre des tâches supplémentaires à celle d'assister ses clientes dans la gestion de cyberincidents, telles que celle d'assurer un échange d'informations entre les infrastructures critique (art. 74 al. 2 litt. a LSI2) ou encore l'évaluation technique des menaces ainsi que l'analyse de questions techniques (art. 73*a* al. 1 LSI2). Lorsque l'OFCS traite des données personnelles et compte 857

1480 MEIER, N 1196.

1481 FF 2017 6565, p. 6643.

1482 CR LPD-MEIER/TSCHUMY, art. 5 N 112.

1483 MEIER, N 589 ; WEBER/WILLI, p. 229.

1484 Cf *supra* N 700 ss.

tenu de ses pouvoirs étendus et de ses missions, on peut considérer qu'il détermine les finalités et les moyens du traitement qui découlent de différentes dispositions de la LSI. Partant, son rôle ne se limite pas à celui d'une sous-traitante, il doit être assimilé à une responsable du traitement[1485].

858 On peut se demander si le nouvel OFCS, reprenant les tâches du NCSC en matière de cybersécurité pour les infrastructures critiques[1486], est responsable du traitement conjoint avec l'infrastructure critique à laquelle il fournit son soutien dans la gestion d'un cyberincident ou si, au contraire, les responsables du traitement sont indépendantes. Alors qu'en droit européen, l'art. 26 RGPD impose l'obligation de conclure un accord entre les deux responsables du traitement conjointes sur le partage des obligations entre elles, le droit suisse va moins loin[1487]. L'art. 33 LPD impose au CF l'obligation de régler les procédures de contrôle et les responsabilités lorsque des organes fédéraux traitent des données personnelles conjointement à d'autres organes fédéraux, cantonaux ou à des personnes privées. Le CF n'a à notre connaissance pas encore réglé expressément ces aspects[1488]. Ainsi, à l'heure actuelle, la distinction entre responsables du traitement conjointes ou indépendantes en Suisse implique que chaque responsable du traitement assume son rôle pour les parties du traitement pour lesquelles elle participe à la détermination du but et des moyens[1489].

859 Dans la mesure où l'OFCS est un organe fédéral, une base légale doit lui permettre de traiter des données personnelles (art. 34 LPD)[1490]. L'autorité peut, dans ce cadre, être amenée à traiter des données personnelles, comme des ressources d'adressage susmentionnées ou encore de fichiers journaux[1491].

1485 Contrairement à la conception initiale du DFF lors de l'adoption de l'aOPCy, DFF, *Erläuterungen zur Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung,* 2020, p. 6. GovCERT est un service de la responsable du traitement qui est l'OFCS.

1486 Cf. *supra* N 225 ss.

1487 CR LPD-EPINEY/POSSE, art. 33 N 12.

1488 Certaines dispositions de l'OPDo permettent en revanche d'appréhender certains aspects que les responsables du traitement conjointes doivent appréhender, à l'instar des exigences de sécurité des données ou du devoir d'information, cf. BSK DSG-STÖCKLI/GRÜNINGER, art. 33 N 12 ss.

1489 CR LPD-MEIER/TSCHUMY, art. 5 N 110. L'organe fédéral procédant à un traitement de données personnelles conjoint demeure responsable, cf. CR LPD-EPINEY/POSSE, art. 33 N 4. Pour une analyse de la situation entre responsables du traitement conjointes, cf. ROSENTHAL, N 57 ss.

1490 Le principe de la légalité donne une légitimité démocratique à l'action de l'État, pose par le cadre légal des limites à l'action de l'État et assure la prévisibilité du droit ainsi que l'égalité de traitement, cf. OA, *Enquête administrative « Fuite de données »,* 2024, N 259.

1491 Les données des fichiers journaux sont en effet généralement considérées comme des données personnelles, cf. PFPDT, *Guide surveillance au lieu de travail à l'attention de l'économie privée,* 2013, p. 6.

Les ressources d'adressages sont définies à l'art. 3 litt. f de la loi sur les télécommunications (LTC) et peuvent consister notamment en des adresses IP, des adresses de messagerie ou encore des noms de domaine, permettant typiquement d'identifier des individus. Il peut également s'agir de commandes informatiques sous la forme de codes informatiques (malveillants). Ces ressources pouvant en outre se trouver dans un lien de connexité avec une procédure pénale ou administrative, elles peuvent par conséquent constituer des données sensibles, dont le traitement doit être prévu par une base légale au sens formel[1492]. Pour cette raison, l'art. 75 al. 1 litt. a LSI dispose que les ressources d'adressage peuvent être traitées en lien avec les motivations religieuses, philosophiques et politiques pouvant conduire à une attaque (cf. art. 5 litt. C ch. 1 LPD). En effet, bien que des raisons financières et économiques soient souvent à l'origine d'une attaque, d'autres motivations peuvent y conduire, à l'instar de raisons religieuses, philosophiques ou politiques, à l'image des hacktivistes qui visent des revendications politiques[1493]. Dans une telle situation, l'OFCS doit traiter ces informations afin d'apprécier la menace et le danger concret. En outre, l'art. 75 al. 1 litt. b LSI prévoit que les ressources d'adressage peuvent être traitées lorsqu'elles concernent des poursuites ou sanctions pénales ou administratives (cf. art. 5 litt. c ch. 5 LPD). Les attaques ciblées sur des infrastructures critiques étant généralement pénalement répréhensibles et les données personnelles liées à une procédure pénale étant réputées sensibles, une base légale formelle doit prévoir le traitement de ces données. L'art. 75 al. 1 LSI sert de base légale formelle. Une plainte pénale ne suffisant pas à écarter le danger, du moins à court terme, il est nécessaire que les infrastructures critiques soient informées le plus rapidement possible des vecteurs d'attaques pour ainsi se protéger et identifier d'autres attaques qui sont déjà survenues. Le traitement des ressources d'adressage en lien avec une procédure pénale ou administrative permet d'échanger ce type de données personnelles après le dépôt d'une plainte pénale ou l'ouverture d'une procédure administrative[1494].

L'art. 75 LSI2 sert de base légale pour les traitements de données personnelles concernant des personnes physiques par l'OFCS. En revanche, il n'est pas clair de savoir si les traitements de données concernant des personnes morales sont encadrés par cette disposition, point opaque de coordination entre la LPD et la LSI. Les personnes morales ne sont aujourd'hui plus protégées 860

1492 Art. 34 al. 2 LPD ; FF 2017 2765, p. 2801.

1493 FF 2017 2765, p. 2871.

1494 FF 2017 2765, p. 2871s.

par la LPD[1495]. Elles méritent néanmoins une certaine protection. Tel est le cas typiquement pour les personnes morales de petite taille, qui sont fortement dépendantes des personnes physiques les composant, ou pour les personnes morales à but non lucratif, à l'instar d'associations caritatives ou politiques[1496]. En outre, les autorités doivent fonder leur activité sur une base légale en vertu du principe de la légalité[1497].

861 Durant les cinq ans suivant l'entrée en vigueur de la LPD révisée, l'art. 75 LSI2 encadre également les traitements de données de personnes morales en vertu de l'art. 71 LPD. La disposition transitoire prévoit effectivement que les dispositions de droit fédéral faisant référence à des données personnelles continuent de s'appliquer aux traitements de données de personnes morales durant les cinq ans suivant l'entrée en vigueur de la LPD.

862 À partir de septembre 2028, l'art. 75 LSI2, qui sert de base légale formelle permettant à l'OFCS de traiter des données personnelles, devra dans tous les cas être reformulé si la disposition a vocation à encadrer également les traitements de données de personnes morales, pour des raisons ayant trait à la clarté juridique ainsi qu'au respect du principe de la légalité. En effet, ni l'art. 75 LSI2 ni le message relatif à la loi révisée ne précisent si les personnes morales sont comprises dans les personnes auxquelles se rattachent les données personnelles que l'OFCS peut traiter. Deux interprétations de l'art. 75 LSI2 sont envisageables. Une première interprétation consiste à admettre que les personnes morales sont comprises dans les personnes protégées et que l'OFCS ne peut traiter leurs données que moyennant le respect de l'art. 75 LSI2. Cette position pourrait se justifier par le fait que la notion de personne morale existe dans d'autres dispositions. L'art. 73*c* al. 1 LSI2 fait mention des « données relatives aux personnes physiques ou morales ». En revanche, les art. 75 ss LSI2 ne précisent pas que les personnes morales sont concernées. Dans le sens de cette interprétation, le message relatif à la loi révisée fait aussi mention des personnes morales au même titre que les personnes physiques relativement aux données personnelles dans le contexte de la transmission d'informations de l'art. 73*d* LSI2, en précisant que la personne morale doit, comme la personne physique, donner son consentement pour une communication de données la concernant aux autorités et organisations actives dans la cybersécurité[1498]. Il y a donc une réelle prise en compte des personnes morales et pas uniquement dans les dispositions elles-mêmes.

1495 FF 2017 6565, p. 6632 ; BSK DSG-BLECHTA/DAL MOLIN/WESIAK-SCHMIDT, art. 5 N 47 ss ; BSK DSG-DRECHSLER, art. 2 N 5.

1496 MEIER, N 351.

1497 FF 2017 6565, p. 6722.

1498 FF 2023 84, p. 29.

La seconde interprétation de l'art. 75 LSI2 conduirait à considérer que dans la mesure où ni l'art. 75 LSI2 ni le message de la loi ne prévoient expressément la protection des données personnelles des personnes morales pour les traitements de données effectués par l'OFCS, le traitement de données relatives à ces dernières n'est pas encadré par la base de l'art. 75 al. 1 LSI2. Dans ce cas, le nouvel art. 57*r* LOGA pourrait servir de base légale. La disposition prévoit que les organes fédéraux peuvent traiter les données concernant des personnes morales, si leurs tâches sont définies dans une loi au sens formel et que le traitement de ces données est nécessaire à l'accomplissement des tâches (art. 57*r* al. 1 LOGA). Des données sensibles relatives à des poursuites pénales ou à des sanctions administratives ou pénale ainsi que les données relatives à des secrets professionnels, d'affaires ou de fabrication peuvent être traitées à ces conditions (art. 57*r* al. 2 LOGA)[1499]. 863

La seconde interprétation de l'art. 75 LSI2 est moins cohérente avec le type de données que l'OFCS est susceptible de traiter. Il est effectivement amené dans sa pratique à traiter des données concernant des personnes morales, bien que l'on puisse penser que l'absence de mention de la personne morale à l'art. 75 LSI2 vaille pour une absence de protection de cette dernière. La LSI2 et son message aspirent en outre à protéger les personnes morales, raison pour laquelle il est préférable de considérer que les données des personnes morales doivent également être traitées sur la base de l'art. 75 LSI2 et pas de façon plus large. Finalement, la situation juridique est plus claire si la base légale encadrant les traitements de données de personnes morales figure dans la LSI2, qui constitue une loi spéciale, plutôt que dans la LOGA. L'art. 75 LSI2 devra donc être modifié à partir de 2028 pour y inclure expressément les personnes morales. En parallèle de ces considérations, l'OFCS doit naturellement respecter les droits découlant de l'art. 13 Cst. (à l'instar du droit à l'autodétermination informationnelle), ou encore de l'art. 53 CC. 864

3. Les autres prestataires de gestion de cyberincidents

a. Les prestataires internes ou externes

En pratique, les prestataires de gestion de cyberincidents peuvent être amenées à traiter des données personnelles[1500]. La sous-traitante doit être une personne juridique indépendante, en ce sens qu'elle ne doit pas faire partie de la même entité juridique que la responsable du traitement[1501]. La fournisseuse 865

1499 FF 2017 6565, p. 6722 et 6733.

1500 Pour une opinion sur les zones grises n'impliquant pas nécessairement un réel traitement de données personnelles par une sous-traitante, cf. ROSENTHAL, N 100 ss.

1501 BSK DSG-BÜHLER/RAMPINI, art. 9 N 26.

interne de prestations de gestion de cyberincidents à une organisation ne peut pas être assimilée à une sous-traitante, mais fait au contraire partie de la responsable du traitement[1502]. Bien qu'il ne s'agisse pas de sous-traitance, les principes généraux de la protection des données s'appliquent aux transferts de données personnelles au sein d'une même entité juridique, notamment concernant l'étendue des données communiquées à l'interne en vue d'un traitement et la diligence dans le choix, la surveillance et le contrôle des collaboratrices en charge du traitement[1503]. À noter par ailleurs que dans le cas d'une organisation active dans plusieurs États, les règles de la communication transfrontalière (art. 16 ss LPD) s'appliquent si elle communique des données personnelles de la Suisse à l'étranger pour gérer des cyberincidents[1504].

866 Quant à la prestataire externe de gestion de cyberincidents, il faut examiner si celle-ci détermine les moyens et finalités du traitement ou si elle se limite au contraire à traiter des données pour une responsable du traitement qui ferait appel à ses services. En d'autres termes, il faut se demander si les organisations offrant de telles prestations se limitent à un traitement technique pratique, si elles sont ou non habilitées à décider des données à traiter, comment les utiliser et pour quelles fins. Dans la majorité des cas impliquant une prestataire externe de gestion de cyberincidents, la responsable du traitement est l'organisation cliente. L'organisation faisant appel à une fournisseuse externe de prestations de gestion de cyberincidents lui délègue la gestion des incidents rencontrés pour bénéficier de l'expertise de cette dernière[1505]. Les organisations victimes d'un cyberincident devraient en principe avoir préalablement déterminé les moyens et finalités du traitement et ne transmettre à la prestataire de gestion de cyberincidents que la faculté de traiter des données aux fins de rétablir une situation sûre[1506]. La sous-traitante dispose d'une marge de manœuvre, mais elle ne doit pas porter sur les moyens essentiels du traitement (à savoir le type de données, la durée du traitement ou les catégories du traitement)[1507], ce qui est régulièrement le cas en pratique. Les prestataires de

1502 FF 2017 6565, p. 6652 ; EPINEY/FASNACHT, N 38 ; MEIER, N 1201.

1503 MEIER, N 1201.

1504 BSK DSG-BÜHLER/RAMPINI, art. 9 N 27.

1505 EPINEY/FASNACHT, N 34.

1506 CR LPD-MÉTILLE, art. 9 N 37. Pour plus d'informations sur la finalité du traitement, cf. ROSENTHAL, N 16 s. Pour un exemple similaire, la CEPD a estimé en droit européen que la prestataire de support informatique général devait être considérée comme une sous-traitante, cf. CEPD, *Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD*, version 2.0, 2021, p. 32.

1507 BSK DSG-BLECHTA/DAL MOLIN/WESIAK-SCHMIDT, art. 5 N 195 ; BSK DSG-BÜHLER/RAMPINI, art. 9 N 9 ; CR LPD-MEIER/TSCHUMY, art. 5 N 113 ; PC LPD-JACOT-GUILLARMOD, art. 5 N 64 et 70 ; ROSENTHAL, N 11 et 33 s.

gestion de cyberincidents ont davantage tendance à disposer de liberté quant aux moyens formels, à savoir quant aux modalités techniques et organisationnelles, ce qui conduirait à les qualifier de sous-traitante[1508]. La prestataire de gestion de cyberincidents qualifiée de sous-traitante qui excède le contrat devient responsable du traitement pour les traitements concernés[1509].

867 Certaines prestataires de gestion de cyberincidents disposent de plus de compétences et peuvent par conséquent être considérées comme des responsables du traitement ; tel pourrait être le cas d'une CSIRT sectorielle disposant d'une marge de manœuvre leur permettant de gérer les données comme elle le souhaite et de décider par exemple de partager des informations avec différentes partenaires. La responsabilité de la CSIRT et de l'organisation lésée par un cyberincident peut être indépendante ou conjointe en fonction des circonstances.

b. La sous-traitance

868 Les prestataires externes de gestion de cyberincidents sont souvent amenées en pratique à être qualifiées de sous-traitantes. Elles peuvent être liées aux responsables du traitement par la loi ou par un contrat (art. 9 al. 1 LPD). Il s'agit généralement de contrats.

869 Toutefois, la loi prévoit parfois certains éléments. C'est typiquement le cas pour les responsables du traitement fédérales lorsqu'elles sous-traitent certaines tâches à des fournisseuses tierces (internes à l'administration fédérale ou externes comme des entreprises privées). L'Ordonnance sur le traitement des données personnelles et des données des personnes morales lors de l'utilisation de l'infrastructure électronique de la Confédération (OTUIC) prévoit que les personnes qui sont chargées de travaux techniques à l'instar de la gestion de l'infrastructure électronique ou de la maintenance peuvent traiter des données personnelles ou de personnes morales uniquement si l'accomplissement de ces tâches l'exige (art. 7 al. 1 OTUIC)[1510].

870 Lorsque la sous-traitance est uniquement régie par un contrat, l'organisation, peu importe son caractère public, parapublic ou privé, doit prévoir, outre le contrat de base, un contrat ou des clauses relatives à la sous-traitance de données personnelles. Les clauses relatives à la protection des données doivent prévoir la soumission de la sous-traitante aux règles de la protection

1508 BSK DSG-BÜHLER/RAMPINI, art. 9 N 10.

1509 CR LPD-MEIER/TSCHUMY, art. 5 N 113 ; ROSENTHAL, N 49 s. Elle violerait par la même occasion le contrat. Pour plus d'informations sur la délimitation entre responsable du traitement et sous-traitante, cf. notamment CR LPD-MEIER/TSCHUMY, art. 5 N 117 s.

1510 OA, *Enquête administrative « Fuite de données »*, 2024, N 286.

des données[1511]. Elles doivent également imposer un devoir de garder le secret et une interdiction d'utiliser les données dans un cadre étranger au contrat[1512]. La question du transfert de données à l'étranger doit être traitée, de même que celle relative au droit d'accès selon les art. 25 ss LPD. Il est aussi opportun de prévoir contractuellement les mesures techniques et organisationnelles pour garantir le respect des principes de protection des données personnelles[1513]. En pratique, les contrats de sous-traitance sont des annexes au contrat principal[1514]. Ceux-ci doivent aussi contenir les catégories de données traitées et leur degré de sensibilité. Il convient de préciser l'usage pour lequel des données spécifiques sont traitées. Le contrat doit aussi prévoir les conditions auxquelles les données peuvent être communiquées à l'extérieur par la sous-traitante. Les clauses contractuelles doivent également prévoir l'admission ou le refus d'une sous-traitance par la sous-traitante (sous-traitance de second rang)[1515].

871 Au-delà du contrat, la prestataire de gestion de cyberincidents ne peut effectuer que les traitements que la responsable du traitement est en droit d'effectuer (art. 9 al. litt. a LPD). La sous-traitante est limitée par les finalités fixées par la responsable du traitement[1516]. En outre, les éventuels secrets auxquels la responsable du traitement est contractuellement ou légalement liée doivent être respectés[1517]. La responsable du traitement doit aussi s'assurer que la sous-traitante respecte tous les principes de protection des données[1518]. Ce faisant, elle doit s'assurer que la sous-traitante est en mesure de respecter la sécurité des données (art. 9 al. 2 LPD), bien que la sous-traitante soit individuellement soumise aux obligations de sécurité des données (art. 8 al. 1 LPD et art. 1 à 6 OPDo)[1519]. L'organisation responsable du traitement est responsable de choisir, d'instruire et de surveiller correctement la sous-traitante à

1511 PFPDT, *TOM*, 2024, p. 52.

1512 SURY, *Digital in Law*, 2021, p. 88.

1513 STAUB, p. 211 s.

1514 En principe écrit, bien que la loi n'exige pas de forme particulière, cf. CR LPD-MÉTILLE, art. 9 N 40.

1515 Pour plus d'informations sur le contenu des contrats, cf. CR LPD-MÉTILLE, art. 9 N 43 ss. Voir à titre d'exemple la *checklist* pour l'élaboration d'un contrat de sous-traitance et les clauses-types publiées par l'autorité compétente pour la protection des données et la transparence des cantons du Jura et de Neuchâtel, PPDT-JURA NEUCHÂTEL, *Checklist pour l'élaboration d'une convention de traitement de données personnelles par un sous-traitant*.

1516 CR LPD-MÉTILLE, art. 9 N 50 ss.

1517 CR LPD-MÉTILLE, art. 9 N 53 ss.

1518 MEIER, N 1233.

1519 CR LPD-MEIER/TSCHUMY, art. 5 N 116 ; CR LPD-MÉTILLE, art. 9 N 79.

laquelle elle fait appel[1520]. À noter que les niveaux d'instructions et de contrôle attendus sont appréciés en fonction des éléments du cas concret, dont le niveau de spécialisation de la sous-traitante ou encore du type de traitements délégués[1521].

872 La prestataire externe de gestion de cyberincidents ne peut elle-même sous-traiter des traitements à des personnes tierces qu'avec l'autorisation préalable de la responsable du traitement (art. 9 al. 3 LPD), à savoir sa cliente. La responsable du traitement peut octroyer une autorisation spécifique ou générale (art. 7 al. 1 OPDo)[1522]. En pratique, les prestataires de gestion de cyberincidents sont vraisemblablement souvent amenées à présenter une liste des organisations auxquelles elles sous-traitent des traitements de données personnelles, notamment en cas d'utilisation de solutions en nuage, pour obtenir l'accord de la cliente.

D. La sécurité des données et des obligations s'en rapprochant

1. La sécurité des données

a. Les mesures de sécurité en général

873 La LPD pose à son art. 8 le principe de la sécurité des données, qui exige de la responsable du traitement qu'elle prenne les mesures techniques et organisationnelles afin de garantir la sécurité des données personnelles traitées. Cette disposition est précisée aux art. 1 ss OPDo. La sécurité des données implique la garantie de l'intégrité, de la confidentialité, de la disponibilité et de la traçabilité des données personnelles traitées[1523]. La sécurité des données est à distinguer de la protection des données. La première vise les mesures techniques et organisationnelles des données dans la sphère des responsables du traitement et des sous-traitantes, alors que la seconde vise la personnalité et les droits fondamentaux des personnes concernées[1524]. La sécurité des données est un principe et une obligation servant la protection des données.

874 Toute infrastructure critique doit prendre les mesures pour éviter les violations de la sécurité des données (art. 8 al. 2 LPD). L'approche suivie par la LPD

1520 Renvoi aux notions de *« cura in eligendo », « cura in instruendo »* et *« cura in custodiendo »* de l'art. 55 CO, cf. BSK DSG-BÜHLER/RAMPINI, art. 9 N 41 ; MEIER, N 1218.

1521 MEIER, N 1222.

1522 Sur la sous-traitance de second rang, cf. CR LPD-MÉTILLE, art. 9 N 81 ss.

1523 PFPDT, *Guide pour le traitement des données personnelles dans le secteur privé,* 2009, p. 8 ; OA, *Enquête administrative « Fuite de données »,* 2024, N 247 ; BSK DSG-STAMMPFISTER, art. 8 N 2 et 24 ss ; EPINEY, N 51 ; HUSI-STÄMPFLI, N 64 ; HUSI-STÄMPFLI/MORAND, p. 128 s. ; MEIER, N 786 ; MEYER/DAVIES, N 6 ; PC LPD-BÉGUIN, art. 8 N 7.

1524 FF 2017 6565, p. 6650 ; MEYER/DAVIES, N 12.

est fondée, comme celle suivie par la LSI, sur le risque (art. 1 al. 3 OPDo)[1525]. Plus concrètement, l'art. 3 OPDo impose l'implémentation de mesures notamment pour contrôler les autorisations ou les locaux en termes de confidentialité, pour contrôler la mémoire et le transport de données en termes de disponibilité et d'intégrité, ou encore pour contrôler la saisie dans des systèmes en termes de traçabilité[1526]. Les mesures concrètes ne sont pas forcément prévues par la loi ou par l'ordonnance, mais il s'agit typiquement en pratique de dispositifs comme le chiffrement, l'utilisation de *virtual private networks* (VPN), l'utilisation de mises à jour de sécurité de manière échelonnée en fonction des risques ou encore la journalisation[1527].

b. L'impact de la sécurité des données lors d'un cyberincident

875 Si un cyberincident se produit, il peut être constitutif d'une violation de la sécurité des données au sens de l'art. 5 litt. h LPD lorsqu'il compromet des données personnelles par une destruction accidentelle, une soustraction de données personnelles et ainsi de suite. Si tel est le cas, la responsable du traitement risque d'une part d'être soumise à l'obligation d'annoncer les violations de la sécurité des données au PFPDT et à l'obligation d'en informer les personnes concernées (art. 24 LPD)[1528]. Elle doit d'autre part mettre en place des mesures réactives de sécurité (art. 3 al. 3 litt. c OPDo). Ces dernières consistent typiquement en la restauration rapide de la disponibilité des données personnelles compromise (art. 3 al. 2 litt. d OPDo), ce qui passe entre autres par l'adoption et la mise en œuvre d'un plan de continuité des opérations qui explique comment une organisation doit continuer à fonctionner lors d'une interruption de service[1529]. De la même manière que pour son obligation de restauration, l'organisation subissant une violation de la sécurité des données doit être capable de détecter et de prendre des mesures pour atténuer ou éliminer les conséquences rapidement en cas de violations de la sécurité des données (art. 3 al. 3 litt. c OPDo). L'établissement de procédures prévoyant des marches à suivre en cas d'incident, ainsi que l'utilisation de systèmes de

1525 CR LPD-FANTI/STAEGER, art. 8 N 94 ; HUSI-STÄMPFLI, N 66 ; MEYER/DAVIES, N 16 ss ; PC LPD-BÉGUIN, art. 8 N 15. Pour l'approche fondée sur le risque dans la LSI, cf. notamment *supra* N 832.

1526 OFJ, *Rapport explicatif OPDo,* 2022, p. 25 s.

1527 MEYER/DAVIES, N 22 ss. Pour une analyse des mesures pouvant être considérées comme « appropriées » dans une approche pratique, cf. MEYER/DAVIES, N 25 ss, en particulier N 48 ss.

1528 Sur l'obligation d'annoncer en vertu de l'art. 24 LPD, cf. *supra* N 525 ss.

1529 OFJ, *Rapport explicatif OPDo,* 2022, p. 25. Sur ce sujet, cf. CR LPD-FANTI/STAEGER, art. 8 N 156 ss.

prévention et de détection d'incident (*intrusion detection and prevention systems*, IDPS), font partie de ces mesures concrètes contribuant à la réalisation de ces objectifs[1530].

Les prestataires de gestion de cyberincidents (internes ou externes) étant compétentes pour remédier à des problèmes de sécurité, il va de soi qu'elles risquent de traiter des données. Elles doivent donc s'assurer que les mesures qu'elles prennent dans tout contexte sont protégées de façon appropriée en fonction du risque, comme les infrastructures critiques dans leur activité et indépendamment d'une violation de la sécurité des données[1531]. 876

Qu'un cyberincident soit constitutif d'une violation de la sécurité des données ou non, une prestataire (interne ou externe) de gestion de cyberincidents est susceptible de traiter des données personnelles. Elle doit traiter les données personnelles auxquelles elle accède en respectant les principes et obligations de la LPD, dont le principe de sécurité, en particulier en raison de son statut important pour la sécurité d'une organisation[1532]. 877

2. La protection des données dès la conception et par défaut

Les obligations de protection des données dès la conception et par défaut marquent une anticipation des manquements par l'introduction d'exigences légales proactives plutôt que réactives[1533]. La protection des données dès la conception vise à minimiser le risque du traitement de données pour la personnalité des individus dès la conception du traitement (art. 7 al. 1 LPD). Cette obligation implique l'implémentation de mesures techniques et organisationnelles appropriées pour respecter dès la phase de conception du traitement les prescriptions de protection des données[1534]. Il peut s'agir par exemple de l'accès sécurisé aux données en ligne prévu comme alternative automatique lorsque c'est possible, de l'élaboration à l'avance d'un processus de gestion de cyberincidents ou encore de l'utilisation de référentiels d'architecture respectueux de la protection des données[1535]. 878

1530 OFJ, *Rapport explicatif OPDo*, 2022, p. 36 ; CR LPD-FANTI/STAEGER, art. 8 N 175 s.

1531 Cf. *supra* N 873 s.

1532 CR LPD-FANTI/STAEGER, art. 8 N 98.

1533 Dans un sens similaire, cf. HUSI-STÄMPFLI, N 67 s. ; HUSI-STÄMPFLI/MORAND, p. 110. De la même manière que l'obligation dans certains cas de mener des analyses d'impact relatives à la protection des données personnelles (art. 22 s. LPD).

1534 FF 0217 6565, p. 6648 s. ; PFPDT, *TOM*, 2024, p. 25 ; BSK DSG-WIDMER, art. 7 N 27 ss ; CR LPD-FANTI/STAEGER, art. 7 N 21 s., 26 et 29 ; HUSI-STÄMPFLI, N 68 ; HUSI-STÄMPFLI/MORAND, p. 115.

1535 CR LPD-FANTI/STAEGER, art. 7 N 47.

879 La protection des données dès la conception doit être distinguée de la sécurité des données dans la mesure où elle impose la garantie du respect de toutes les prescriptions de la protection des données dès la conception du traitement, par l'adoption de mesures techniques et organisationnelles. L'art. 8 LPD consacre au contraire la mise en place de mesures permettant d'assurer uniquement la sécurité des données. Cela étant, certaines mesures sont utiles à la réalisation des deux obligations, comme l'anonymisation[1536].

880 La protection des données par défaut impose aux responsables du traitement de prévoir des préréglages appropriés pour garantir que le traitement soit limité au minimum requis par la finalité poursuivie par le traitement de données (art. 7 al. 3 LPD). Il s'agit ici d'une obligation liée à la configuration par défaut des réglages s'appliquant de façon standardisée, en particulier en lien avec la minimisation des données[1537]. Le lien entre la protection des données dès la conception et la protection des données par défaut est naturellement étroit[1538].

E. La coopération par la communication de données personnelles

1. Des généralités sur la communication de données personnelles

881 L'échange d'informations étant au centre de la gestion de cyberincidents, il n'est pas exclu que des données personnelles soient communiquées entre différentes organisations. La communication de données personnelles est définie à l'art. 5 litt. e LPD comme « le fait de transmettre des données personnelles ou de les rendre accessibles ». L'on vise par ici tant les communications actives (comme la transmission ou la diffusion) que passives (à l'instar de la consultation)[1539].

882 De nombreuses communications peuvent avoir lieu autour de la gestion de cyberincidents. À titre d'exemple, l'OFCS peut être amené à échanger des informations avec des autorités de poursuite pénale ou de renseignement[1540]. En outre, si l'office fédéral publie des données personnelles à titre d'information au public ou à l'attention de son cercle fermé de clientes, il s'agit là aussi d'une communication au sens de la LPD[1541]. De plus, lorsqu'une organisation

1536 FF 2017 6565, p. 6650 s. ; MEYER/DAVIES, N 12 ; PC LPD-BÉGUIN, N 28.

1537 FF 2017 6565, p. 6649 s. ; PFPDT, *TOM*, 2024, p. 25 s. ; BSK DSG-WIDMER, art. 7 N 55 ss ; CR LPD-FANTI/STAEGER, art. 7 N 54 s. ; HUSI-STÄMPFLI, N 69 ; HUSI-STÄMPFLI/MORAND, p. 119 s.

1538 Pour un exemple, cf. CR LPD-FANTI/STAEGER, art. 7 N 60.

1539 BSK DSG-BLECHTA, art. 3 N 77 ; BSK DSG-BLECHTA/DAL MOLIN/WESIAK-SCHMIDT, art. 5 N 118 ; BSK DSG-EHRENSPERGER, art. 19 N 5 ; CR LPD-MEIER/TSCHUMY, art. 5 N 78 ; MEIER, N 536, 541.

1540 Cf. *supra* N 739 ss.

1541 MEIER, N 550.

communique des données à une prestataire de gestion de cyberincidents, même dans l'éventualité d'une communication interne, il peut s'agir d'une communication au sens de l'art. 5 litt. e LPD si la prestataire n'en a pas déjà connaissance[1542]. Une prestataire de gestion de cyberincidents peut avoir à coordonner ses forces avec d'autres services internes d'une organisation, ou peut être soumise à une obligation d'annoncer certains événements à une autorité. Des échanges avec d'autres fournisseuses de services de gestion de cyberincidents ou encore d'autres interlocutrices peuvent avoir lieu, notamment dans le cadre de communications aux médias pour le compte de l'organisation affectée[1543].

2. Les flux de communication sur le plan national pour l'OFCS

a. Les communications effectuées par l'office fédéral

L'art. 36 al. 1 LPD pose le principe selon lequel l'organe fédéral communiquant 883
des données personnelles doit fonder cette communication sur une base légale[1544]. Ce principe, découlant de l'art. 34 LPD, s'explique par le fait que la communication de données personnelles est probablement le traitement le plus à risque. Les données personnelles quittent la sphère dans laquelle elles ont été collectées pour être accessibles à un cercle plus large de destinataires, conduisant par la même occasion à une perte de maîtrise sur les données par la responsable du traitement et à une augmentation des risques pour la personne concernée[1545]. En outre, l'autorité législative souhaite contrer le risque lié à une divulgation non souhaitée[1546]. L'art. 36 LPD pose une exigence de base légale pour la communication entre organes fédéraux, mais également lorsqu'un organe fédéral entend communiquer des données personnelles à une autorité cantonale ou communale, ou encore à une entité privée[1547]. La base légale doit porter sur le transfert même, en prévoyant les droits ou obligations

1542 MEIER, N 543, 545.

1543 NIST, *Computer Security Incident Handling Guide*, 2012, p. 10 et 66 s. Au sujet de la coordination interne et externe, NIST, 800-53, rev. 5, IR-4, p. 154 ; concernant la coopération avec des partenaires et organisations externes, NIST, 800-53, rev. 5, IR-4, p. 154. Pour la communication au public, NIST, 800-53, rev. 5, IR-4, p. 156.

1544 OFJ, *Guide de législation*, 2019, N 833 ; PFPDT, *Guide pour le traitement des données personnelles dans l'administration fédérale*, 2009, p. 7. La base légale doit normalement être formelle si des données sensibles sont concernées par la communication, cf. notamment BSK DSG-EHRENSPERGER, art. 19 N 13. L'art. 36 LPD prévoit des exceptions à ce principe, mais il est en pratique plus aisé de prévoir une base légale permettant une communication systématique plutôt que d'agir au cas par cas avec des exceptions qui s'interprètent de manière restrictive, BSK DSG-EHRENSPERGER, art. 19 N 21.

1545 CR LPD-EPINEY, art. 36 N 1.

1546 BSK DSG-EHRENSPERGER, art. 19 N 1 s.

1547 BSK DSG-EHRENSPERGER, art. 36 N 13 ss ; CR LPD-EPINEY, art. 36 N 2 et 12 ; PC LPD-COSSALI SAUVAIN, art. 36 N 8.

de l'autorité divulguant les données et de la destinataire[1548]. En revanche, la communication de données personnelles par la collaboratrice d'un organe fédéral à sa supérieure directe ou par un organe fédéral à l'autorité supérieure ne nécessite pas de se fonder sur une base légale[1549]. La communication entre GovCERT et l'OFCS n'a donc pas besoin d'être prévue légalement.

884 Bien qu'il soit possible de communiquer des données personnelles en l'absence d'une base légale (conformément à l'art. 36 al. 2 à 5 LPD), l'OFCS communique en principe des données personnelles à des entités tierces dans le cadre de ses fonctions seulement en vertu des art. 76 à 77 LSI2. Sur le plan national, l'art. 76 LSI autorise d'une part les communications de données personnelles aux infrastructures critiques, et des ressources d'adressages et données personnelles s'y rapportant aux fournisseuses de services de télécommunication d'autre part, lorsqu'elles sont nécessaires à la protection contre les cybermenaces. Par exemple, dans le cas de la constatation auprès d'une hébergeuse de la présence d'un serveur de commande et contrôle grâce auquel un réseau est piloté par des ordinateurs zombies, l'hébergeuse pourrait livrer à l'OFCS des fichiers journaux contenant les adresses IP des machines infectées et l'office pourrait les remettre à la fournisseuse de services de télécommunication afin que cette dernière puisse alerter ses clientes.

885 En parallèle, l'OFCS peut communiquer aux autorités et organisations actives dans la cybersécurité des données personnelles provenant de signalements lorsque c'est utile à leur activité, à condition que la personne (physique ou morale) concernée ait donné son accord (art. 73*d* al. 1 LSI2)[1550].

886 Finalement, la Loi fédérale sur le principe de transparence dans l'administration (LTrans) s'applique. L'office fédéral pour la cybersécurité doit permettre à toute personne de consulter ses documents officiels en vertu de l'art. 5 LTrans, sous réserve d'intérêts prépondérants conformément à l'art. 7 LTrans et sous réserve des informations secrètes (art. 4 litt. a LTans)[1551]. L'art. 4 litt. b LTrans prévoit qu'une loi spéciale peut déroger aux conditions de la LTrans. L'art. 4 al. 1bis LSI2 prévoit une règle spéciale selon laquelle les informations obtenues par l'OFCS dans son activité de réception et d'analyse des signalements ne peuvent être rendues accessibles en vertu de la LTrans. Cette disposition doit en partie garantir la confidentialité des signalements faits à l'OFCS[1552].

1548 BSK DSG-EHRENSPERGER, art. 19 N 14.

1549 BSK DSG-EHRENSPERGER, art. 19 N 6.

1550 FF 2023 84, p. 29.

1551 La LTrans prime effectivement la LSI (art. 4 al. 1 LSI et art. 4 al. 1 et 1*bis* LSI2).

1552 Ce nouvel alinéa a été adopté à l'encontre du souhait de la PFPDT, qui estime que la LTrans prévoit suffisamment d'exceptions au principe de transparence, cf. FF 2017 2765, p. 62.

Cette réserve ne s'applique pas aux autorités et organisations à l'origine d'un signalement si elles sont elles-mêmes assujetties à la LTrans (art. 4 al. 1bis *in fine* LSI2)[1553].

À noter que l'art. 36 al. 6 LPD permet aux organes fédéraux, dont l'OFCS, de refuser, de restreindre ou d'assortir de charges une communication de données personnelles si un intérêt public important ou un intérêt digne de protection manifeste de la personne concernée l'exige ou si une obligation légale de garder le secret ou une disposition de protection des données l'exige. En outre, la personne concernée qui rend vraisemblable un intérêt digne de protection peut s'opposer à ce que l'OFCS communique des données personnelles déterminées (art. 37 LPD). Elle peut voir son opposition rejetée par l'autorité si cette dernière est juridiquement tenue de communiquer les données personnelles ou si l'absence de communication risque de compromettre l'accomplissement de ses tâches (art. 37 al. 2 LPD). 887

b. Les données personnelles communiquées à l'OFCS

La coopération se fait en principe sur un mode bidirectionnel, dans le but de permettre l'accomplissement de tâches de différentes autorités. Par exemple, lorsque la PFPDT prend connaissance d'une violation de la sécurité des données en vertu de l'art. 24 LPD, elle doit l'analyser. Dans le cadre de cette analyse, il lui est possible de transmettre des données personnelles, y compris sensibles relatives à des poursuites ou sanctions pénales administratives visant la responsable du traitement à l'OFCS en vertu de l'art. 24 al. 5*bis* LPD[1554] à des fins d'analyse. Dans ce cas, l'OFCS interviendrait en tant que sous-traitante pour le compte de la PFPDT. En effet, la loi ne permet pas à l'OFCS de conserver et traiter les données transmises par la PFPDT pour ses propres missions mais uniquement à des fins d'analyse pour la PFPDT. 888

Certains garde-fous sont prévus par la disposition et rappellent le principe de proportionnalité. Tout d'abord, la PFPDT ne transmet que les données personnelles nécessaires à l'analyse de l'incident par l'OFCS. Ensuite, la loi ne permet pas une communication systématique de toute violation de la sécurité des données. En outre, il est nécessaire d'obtenir le consentement de la responsable du traitement. Finalement, il est interdit d'utiliser cette collaboration pour contourner le principe de *nemo tenetur se ipsum accusare* inscrit à l'art. 24 al. 6 LPD[1555]. 889

1553 FF 2023 83, p. 21.

1554 L'art. 24 al. 5*bis* LPD entrera en vigueur lors de l'introduction de signaler les cyberattaques, cf. FF 2023 83, p. 54 s.

1555 FF 2023 84, p. 54 s. ; OFJ, *Rapport explicatif OPDo,* 2022, p. 45. Pour plus d'informations sur le principe de l'art. 24 al. 6 LPD, cf. CR LPD-MÉTILLE/MEYER, art. 24 N 101 ss.

3. La communication de prestataires de gestion de cyberincidents d'autorités

890 Si l'on se cantonne à l'exemple des organes fédéraux soumis à la LPD, il est possible que des prestataires de gestion de cyberincidents internes à des autorités ou organisations de la Confédération soient amenées à partager des informations. L'art. 10*a* LSI2 leur permet typiquement de partager des données personnelles utiles à la sécurité de l'information, entre elles, avec des organisations nationales, internationales ou étrangères de droit public lorsque la communication remplit les conditions de l'art. 10*a* al. 2 LSI2. Selon cette disposition, une communication est possible si elle est utile à la sécurité de l'information, si elle n'enfreint pas d'obligation légale ou contractuelle de garder un secret, si la LPD est respectée et si l'organisation qui reçoit les données a des tâches correspondantes en termes de sécurité de l'information à celles de l'entité à l'origine de la communication.

891 Les autorités et organisations soumises à la LSI2 disposent également de la base légale formelle leur permettant d'échanger des données personnelles, y compris sensibles, relatives aux personnes impliquées dans des violations de la sécurité de l'information ou dans des vulnérabilités, aux conditions de l'art. 10*a* al. 2 LSI2 (art. 10*a* al. 5 LSI2)[1556].

4. La communication de données personnelles par les privées en Suisse

892 Les actrices privées établies en Suisse désirant transmettre des données personnelles ne nécessitent pas de se fonder sur une base légale (art. 36 LPD *a contrario*). Les organisations faisant appel à des prestataires privées de gestion de cyberincidents et ces dernières peuvent communiquer des données personnelles à condition de respecter les principes et les différentes obligations générales de protection des données. Dans le contexte d'obligations de signaler des incidents à différentes autorités, les communications sont obligatoires et non facultatives.

893 La communication de données sensibles à des personnes tierces constitue une atteinte illicite au sens de l'art. 30 al. 2 litt. c LPD, dont l'illicéité peut être levée par l'un des motifs de l'art. 31 LPD. Il est en pratique rare que des données sensibles doivent être partagées par des organisations privées dans le cadre de la gestion de cyberincidents. Cela étant, la loi, le consentement de la personne concernée, un intérêt prépondérant, comme ceux figurant à l'art. 31 al. 2 LPD peuvent permettre de lever l'illicéité de l'atteinte[1557].

1556 FF 2023 84, p. 25.

1557 Cf. notamment CR LPD-BOILLAT/WERLY, art. 31 N 21 ss.

La communication de données sensibles à une sous-traitante, à une entreprise du même groupe ou à une responsable du traitement conjointe dans le cadre d'un traitement de données commun n'est pas considérée comme une communication faite à une personne tierce au sens de l'art. 30 al. 2 litt. c LPD[1558]. Par conséquent, une infrastructure critique peut communiquer des données sensibles à une prestataire de gestion de cyberincidents, à condition que les principes et les obligations de la LPD soient respectées, à l'instar du principe de proportionnalité (art. 6 al. 2 LPD). 894

5. Les communications de données concernant des personnes morales

Les personnes morales ne sont aujourd'hui plus protégées par la LPD et la modification du champ d'application de la LPD devrait faciliter la communication transfrontière de données concernant des personnes morales à destination d'États ne connaissant pas la protection de leurs données, en tout cas lorsqu'il en va des transferts effectués par des personnes privées, car ces communications ne sont plus conditionnées à l'assurance d'un niveau adéquat de protection dans l'État de destination[1559]. Partant, la communication de données personnelles concernant une personne morale par une infrastructure critique ou plus particulièrement par une prestataire de gestion de cyberincidents n'est pas soumise à la LPD, sous réserve qu'une personne physique soit par ce biais identifiable. Il est toutefois nécessaire de respecter les dispositions générales conférant une protection aux personnes morales dont les données sont protégées, que ce soit au titre des art. 28 ss CC (pour la protection de la personnalité en général, y compris la sphère privée) ou de l'art. 53 CC, qui prévoit qu'elles peuvent acquérir tous les droits dissociables des conditions naturelles de l'être humain, ou encore par d'autres sources juridiques spécifiques, à l'instar des normes sur les secrets, de celle découlant du droit d'auteure et ainsi de suite[1560]. 895

La situation est différente pour les communications de l'OFCS en raison de l'art. 36 LPD[1561]. L'art. 57s LOGA concerne spécifiquement la communication de données personnelles d'une personne morale. La disposition ne constitue pas une base légale pour la communication de données dans des cas concret, mais elle précise les exigences auxquelles les bases légales spéciales doivent se conformer[1562]. Les art. 76 à 77 LSI2 ne spécifient pas si les 896

1558 CR LPD-BOILLAT/WERLY, art. 30 N 33 ; MEIER, N 1568.

1559 FF 2017 6565, p. 6595 et 6632.

1560 BO 2918 N 1787 ; FF 2017 6565, p. 6632 ; MEIER, N 351.

1561 Comme rappelé à FF 2017 6565, p. 6595 et 6603 s.

1562 FF 2017 6565, p. 6722.

données susceptibles d'être communiquées sont relatives à des personnes physiques ou morales. Pourtant, le CF avait précisé lors de la révision de la LPD qu'il conviendrait que les lois spéciales précisent ce point, dans la mesure où les bases légales préexistantes ne s'appliquent plus qu'aux traitements de données concernant des personnes physiques[1563]. Il nous paraît alors nécessaire que les art. 76 à 77 LSI2 soient également applicables aux communications de données concernant des personnes morales, comme cela semble être souhaité à la lecture du message accompagnant la loi, à défaut de quoi les dispositions topiques de la LOGA devraient encadrer les échanges de données personnelles concernant les personnes morales[1564]. Dans l'attente de cette modification et durant les cinq ans suivant l'entrée en vigueur de la LPD révisée, l'art. 71 LPD lui permet de continuer à traiter des données relatives à des personnes morales sur la base des art. 76 à 77 LSI[1565]. En parallèle de ces considérations, l'OFCS doit respecter les droits découlant de l'art. 13 Cst. (à l'instar du droit à l'autodétermination informationnelle), ou encore de l'art. 53 CC[1566].

6. La communication de données personnelles à l'étranger

a. Les cas de figure et les normes à respecter

897 Les différentes intervenantes dans la gestion de cyberincidents sont parfois amenées à échanger divers types d'informations avec des entités à l'étranger. Il peut s'agir d'autres prestataires chargées de la cybersécurité, d'autorités ou encore de la même entité répartie sur plusieurs territoires géographiques. Les prestataires de gestion de cyberincidents privées, les CSIRT sectorielles ou encore l'OFCS peuvent, dans le cadre de ces communications, échanger des données personnelles, même s'il est souvent possible en pratique d'anonymiser les données[1567].

898 Plusieurs situations sont en pratique concevables lorsqu'il en va des communications transfrontières que les différentes organisations actives dans la gestion de cyberincidents peuvent effectuer. Elles ne reposent pas forcément

1563 FF 2017 6565, p. 6722.

1564 FF 2017 2765, p. 2872. Il est en effet nécessaire que ces communications soient prévues par une loi au sens formel, dans la mesure où, comme pour les personnes physiques, GovCERT est susceptible de traiter des données sensibles, concernant, pour les personnes morales, des poursuites ou sanctions administratives ou des secrets professionnels, d'affaires ou de fabrication, cf. art. 57s al. 2 LOGA ; FF 2017 6565, p. 6734.

1565 FF 2017 6565, p. 6722.

1566 ATF 137 II 371, c. 6.1 ; MEIER, N 351.

1567 La communication de données anonymisées ou de données pseudonymisées, lorsque la destinataire doit user d'efforts disproportionnés pour accéder à nouveau à la personne concernée, ne tombe pas sous le coup des art. 16 s. LPD, cf. CR LPD-FISCHER, art. 16 N 27 ss.

sur les mêmes justifications et ne nécessitent pas nécessairement les mêmes obligations de la part de l'organisation procédant à la communication :

— il peut y avoir des communications directes entre prestataires de gestion de cyberincidents établies dans des États assurant ou non un niveau de protection des données adéquat ;
— les prestataires de gestion de cyberincidents établies en Suisse peuvent être amenées à communiquer avec différentes communautés de services analogues ou avec des partenaires individuelles par le biais d'organismes ;
— des autorités étrangères peuvent chercher à obtenir des informations auprès d'infrastructures critiques ou plus particulièrement de fournisseuses de services de gestion de cyberincidents ;
— une organisation établie sur le territoire de plusieurs États peut requérir de sa prestataire de gestion de cyberincidents établie en Suisse un transfert de données à d'autres services internes à l'organisation ou, dans le cas d'une CSIRT distribuée, à d'autres collaboratrices de la CSIRT.

899 Lorsque les prestataires sont amenées à communiquer des données personnelles à des entités étrangères, il s'agit principalement de ressources d'adressage permettant d'identifier une personne physique. Dans ce genre de cas, les différentes prestataires de gestion d'incidents doivent respecter la LPD, plus précisément ses art. 16 ss, en plus des autres principes et obligations générales de protection des données[1568]. Il est nécessaire de disposer de règles particulières lorsqu'il en va de communications transfrontières, dans la mesure où ces traitements de données comportent davantage de risques pour la personne concernée. En effet, de par la perte de maîtrise sur les données personnelles au sens de l'ordre juridique suisse, il n'est pas exclu que la législation étrangère permette des traitements interdits en Suisse ou qu'un État tiers n'assure pas, par exemple, l'exercice des droits de la personne concernée, ou qu'une personne soit en danger si un État étranger vient à connaître certaines données la concernant et dont le traitement ne poserait pas de problèmes en Suisse[1569].

900 Le principe est qu'une communication de données personnelles à l'étranger respecte les règles lorsqu'elle est faite à une destinataire établie dans un État étranger ou organisme international[1570] assurant un niveau de protection des données adéquat (art. 16 al. 1 LPD). Lorsque l'État n'assure pas un niveau de

1568 BSK DSG-MAURER-LAMBROU/STEINER, art. 6 N 11a.

1569 BSK DSG-DAL MOLIN, art. 16 N 7 ; BSK DSG-MAURER-LAMBROU/STEINER, art. 6 N 2 ; EPINEY/FASNACHT, N 2 et 8.

1570 L'organisme international comprend toute institution internationale, qu'il s'agisse d'une organisation ou d'une juridiction, cf. FF 2017 6565, p. 6657.

protection adéquat, il demeure possible de procéder à une communication transfrontière, à condition de se baser sur l'une des autres justifications de l'art. 16 al. 2 LPD ou sur l'une des dérogations de l'art. 17 al. 1 LPD.

901 Outre les art. 16 s. LPD et indépendamment de la destinataire et du territoire étranger sur lequel elle se situe, la personne communiquant depuis la Suisse des données personnelles doit respecter les autres principes et les autres obligations de la LPD dès lors que la communication consiste en un traitement de données personnelles[1571].

902 L'OFCS est par ailleurs soumis à une autre obligation incombant spécifiquement aux organes fédéraux lorsqu'il communique des données personnelles à l'étranger. En effet, en tant qu'organe fédéral, nous savons qu'il doit fonder une communication de données personnelles sur une base légale[1572]. C'est pourquoi l'art. 77 LSI2 permet l'échange de données personnelles dans le contexte de coopération internationale. D'après cette disposition, l'OFCS est habilité à communiquer des données personnelles aux services étrangers ou internationaux chargés de la protection des infrastructures critiques pour les aider dans l'accomplissement de leurs tâches similaires à celles de l'OFCS, à condition que les services étrangers ou internationaux garantissent que les données seront utilisées conformément aux fins prévues (art. 77 al. 1 et 2 LSI2). Les données personnelles susceptibles d'être communiquées doivent permettre de connaître l'identité ou le mode opératoire d'auteures de cyberattaques. L'art. 77 LSI2 donne à l'OFCS la possibilité de le faire, ce qui implique qu'il conserve la faculté de refuser un transfert, notamment dans les cas de non-respect des art. 16 s. LPD ou lorsque la proportionnalité ne serait pas respectée[1573]. À noter que l'art. 10*a* LSI2 prévoit également à ses al. 2 et 5 la possibilité pour les autorités et organisations de la Confédération d'échanger avec des organisations nationales, internationales ou étrangères de droit public aux conditions cumulatives de l'art. 10*a* al. 2 LSI2.

b. La communication avec une décision d'adéquation du Conseil fédéral

903 Le principe posé à l'art. 16 al. 1 LPD prévoit qu'une communication transfrontière de données personnelles peut avoir lieu lorsqu'elle vise une destinataire établie ou résidant sur le territoire d'un État ou œuvrant au sein d'une organi-

1571 CR LPD-FISCHER, art. 16 N 39 s. Au-delà de la protection des données personnelles, la communication à un État étranger ne doit naturellement pas être constitutive d'un acte exécuté sans droit pour un État étranger (art. 271 CP).

1572 PFPDT, *Guide pour le traitement des données personnelles dans l'administration fédérale,* 2009, p. 7.

1573 FF 2017 2765, p. 2873.

sation internationale assurant un niveau adéquat de protection des données personnelles. Aujourd'hui, l'annexe 1 de l'OPDo contient la liste des États étrangers, des secteurs ou des territoires déterminés dans un État et des organismes internationaux qui remplissent les standards de la Convention modernisée pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (108+) et qui la mettent correctement en œuvre, tout en respectant les droits humains, la garantie effective des droits des personnes concernées (art. 8 al. 1 OPDo)[1574]. Les États européens, de l'Espace économique européen (EEE) ou ayant ratifié la Convention 108+ sont généralement considérés comme assurant un niveau de protection des données adéquat, si l'on a la certitude que les données ne seront pas réexportées vers un pays tiers.

Par exemple pour les communications à une communauté, le groupe des CERT des gouvernements européens (*European Government CERT Group,* EGC) regroupe uniquement des CERT européennes, et principalement nationales. Seule GovCERT en fait partie à l'heure actuelle en Suisse. Partant, l'on peut considérer (sous réserve de doutes) que les échanges se feront sur la base de l'art. 16 al. 1 LPD. En outre, les serveurs du groupe étant situés en Europe, l'on peut raisonnablement s'attendre à ce que l'organisation figure elle-même sur la liste du CF. Partant, qu'il s'agisse d'une communication directe effectuée à une partenaire ou qu'elle soit faite par le biais d'un canal de l'EGC, il semblerait qu'il s'agisse dans les deux cas d'une communication faite à une partenaire dans un État assurant un niveau adéquat de protection des données. Il convient toutefois de garder à l'esprit qu'il pourrait y avoir une sous-traitance (art. 9 LPD) dans le cas où les partenaires utilisent un canal de l'EGC et que cette dernière héberge des données personnelles. 904

c. La communication sans décision d'adéquation du Conseil fédéral

Lorsqu'un État ne figure pas dans la liste du CF, cela ne veut pas dire pour autant qu'il n'assure pas un niveau de protection adéquat. Il se peut que le CF n'ait pas encore examiné la situation de l'État destinataire[1575]. La deuxième raison pour laquelle un État pourrait ne pas figurer dans l'ordonnance est qu'il ne remplit pas les exigences pour bénéficier d'une décision d'adéquation du CF. Il est également possible d'aboutir à cette conclusion si un État figure sur la liste du CF mais qu'il existe « des indices concrets qu'on ne peut pas considérer le niveau de protection des données comme étant adéquat dans la perspective 905

1574 FF 2017 6565, p. 6657 s. ; OFJ, *Rapport explicatif OPDo*, 2022, p. 25 s. ; CR LPD-FISCHER, art. 16 N 35 s. ; PC LPD-GENECAND, art. 16 N 23. En revanche, la forme de la législation ne semble pas refléter une réelle importance, cf. MEIER, N 1302 ss.

1575 FF 2017 6565, p. 6658.

de l'exportation envisagée »[1576]. En pratique, les responsables du traitement vont vraisemblablement supposer que l'absence d'un État sur la liste implique que ce dernier ne garantit pas un niveau de protection adéquat et que d'autres garanties doivent être mises en œuvre[1577].

906 Le transfert dans un État non adéquat peut garantir un niveau de protection approprié par un traité international, des clauses spécifiques de protection dans un contrat, des garanties spécifiques, des clauses modèles, des règles d'entreprises contraignantes ou d'autres garanties prévues par le CF (art. 16 al. 2 LPD). En pratique, l'exportatrice de données personnelles fonde régulièrement des communications sur des clauses type de protection des données ou clauses contractuelles types (CCT ou *Standard Contract Clauses*) en vertu de l'art. 16 al. 2 litt. d LPD[1578]. La PFPDT publie une liste des clauses modèles qu'elle approuve[1579] et la responsable du traitement fondant une communication sur de telles clauses doit tout de même prendre des mesures adéquates pour s'assurer que la destinataire respecte les clauses modèles (art. 10 OPDo). Ces clauses sont en pratique annexées à un contrat entre la fournisseuse d'informations et la destinataire. Il est fait usage des clauses contractuelles types de l'UE avec des ajustements pour la Suisse, dès lors que ce sont les SCC reconnues par la PFPDT[1580]. La situation avec les États-Unis d'Amérique (*United States of America,* USA) a fait l'objet de nombreux développements et la PFPDT admet aujourd'hui le transfert de données personnelles aux USA sur la base des CCT européennes, moyennant le respect de certaines garanties, jusqu'à l'adoption du *Data Privacy Framework* entre les USA et la Suisse à venir[1581]. Des questions similaires se posent lors de l'utilisation de services en nuage utilisés tant par des organisations privées qu'étatiques dans le cadre de la gestion de cyberincidents, en fonction du territoire sur lequel se situent les serveurs stockant les données personnelles et, selon la position suivie, du risque d'un accès par les autorités étrangères aux données[1582].

1576 PFPDT, *Guide pour l'examen de la licéité de la communication transfrontière de données*, 2023, p. 4.

1577 CR LPD-FISCHER, art. 16 N 37.

1578 PFPDT, *Guide pour l'examen de la licéité de la communication transfrontière de données*, 2023, p. 4 ; PC LPD-GENECAND, art. 16 N 53.

1579 PFPDT, *Infothèque Protection des données, Clauses contractuelles types* ; CR LPD-FISCHER, art. 16 N 61.

1580 PFPDT, *Guide pour l'examen de la licéité de la communication transfrontière de données*, 2023, p. 3 ; CR LPD-FISCHER, art. 16 N 59 ss, plus particulièrement N 60, 62 et 68 ss.

1581 Pour une analyse de la situation actuelle entre l'UE et les USA ou entre la Suisse et les USA, cf. CR LPD-FISCHER, art. 16 N 10 ss ; PC LPD-GENECAND, art. 16 N 16 s.

1582 Pour des analyses de la question, cf. BSK DSG-DAL MOLIN, art. 16 N 123 ss ; CR LPD-FISCHER, art. 17 N 127 ss.

Lorsqu'une organisation ne peut pas fonder une communication souhaitée sur une justification de l'art. 16 LPD, elle peut chercher à se baser sur l'une des dérogations de l'art. 17 LPD. Dans le contexte de la gestion de cyberincidents, il est en particulier possible de transférer des données dans un pays n'assurant pas un niveau de protection adéquat des données lorsque ce transfert est nécessaire à la sauvegarde d'un intérêt public prépondérant (art. 17 al. 1 litt. c LPD). Cette dérogation s'examine au cas par cas et ne vaut pas pour des communications systématiques vers un État étranger[1583]. Elle concerne typiquement la sécurité intérieure de la Suisse ou d'un autre État. L'intérêt ne doit pas être purement hypothétique ; il doit en outre être prépondérant, dans le sens où il doit l'emporter sur l'atteinte portée à la personnalité due au transfert. Il convient d'effectuer cette pesée d'intérêts en fonction de tous les éléments du cas d'espèce, en tenant compte notamment des garanties offertes par l'État de destination[1584]. Cet intérêt pourra notamment être admis dans des cas de lutte contre la fraude ou le blanchiment d'argent, ou dans le cas de disparitions dans une zone de conflit ou d'une catastrophe naturelle[1585]. L'on pourrait imaginer cette justification lors de cyberincidents plaçant un État en crise, par exemple si une large partie de ses capacités électriques venait à être compromise et qu'une organisation en Suisse ait accès à des informations permettant d'identifier la personne à l'origine de l'attaque ayant plongé l'État étranger dans la pénombre. 907

Il est toujours possible, si aucune autre justification ne peut être utilisée dans un cas d'espèce, de se prévaloir du consentement de la personne concernée. L'art. 17 al. 1 litt. a LPD prévoit que la personne concernée peut donner expressément son consentement à la communication dans un État tiers particulier. Le consentement peut par exemple être demandé dans des circonstances extracontractuelles ou lorsque la communication n'est pas directement liée à l'exécution d'un contrat comme entendu par l'art. 17 al. 1 litt. b LPD[1586]. Le consentement ne pouvant être valablement donné qu'après une information appropriée, la personne concernée doit connaître, pour fournir son consentement, le nom du pays destinataire, les risques d'un ou plusieurs transferts déterminés, notamment par rapport au niveau de protection assuré à destination, les finalités de la communication et ainsi de suite[1587]. Il est difficile 908

1583 BSK DSG-DAL MOLIN, art. 17 N 58 ; BSK DSG-MAURER-LAMBROU/STEINER, art. 6 N 32 ; EPINEY/FASNACHT, N 23.

1584 CR LPD-FISCHER, art. 17 N 25 ss ; sur l'ancien droit, cf. notamment EPINEY/FASNACHT, N 23.

1585 FF 2017 6565, p. 6661 ; BSK DSG-MAURER-LAMBROU/STEINER, art. 6 N 32.

1586 MEIER, N 1342.

1587 FF 2017 6565, p. 6661 ; CR LPD-FISCHER, art. 17 N 11 et 13 ; EPINEY/FASNACHT, N 20.

dans le contexte de la gestion de cyberincidents de se prévaloir du consentement de la personne concernée. Elle n'est en effet souvent pas l'organisation communiquant avec d'autres autorités ou organisations.

909 Pour être valable, le consentement doit être « exprès » au sens de l'art. 6 al. 7 LPD. Un consentement est considéré exprès lorsqu'il est formulé oralement, par écrit ou par un signe, tout en découlant directement des mots ou signes employés. Le fait de cocher une case revient pour les autorités suisses à un tel consentement, de même que des gestes clairs et appropriés dans un contexte concret, à l'instar de signes approbateurs de la tête après des explications claires. Le consentement tacite n'est à l'inverse pas suffisant[1588]. L'exportatrice demeure toutefois liée à son devoir de diligence[1589]. La personne concernée est libre de retirer son consentement à tout moment, avec pour conséquence d'interrompre la communication et d'empêcher tout transfert postérieur de données[1590]. Bien que les prestataires de gestion de cyberincidents requièrent souvent le consentement de la fournisseuse de données avant de procéder à une communication transfrontière, il conviendrait soit de se reposer sur une garantie que le consentement a été obtenu, soit de s'assurer dans chaque cas que l'on requiert bien le consentement de la personne concernée et non pas uniquement de l'organisation fournissant les données[1591].

d. La publication de données personnelles sur un site Internet

910 La publication d'informations sur un site Internet à l'attention du public ne constitue pas en tant que telle une communication transfrontière de données, même si ces données peuvent être consultées depuis l'étranger (art. 18 LPD), étant donné que de l'étranger des données publiées n'est pas une finalité en soi mais un simple effet secondaire ou collatéral[1592]. Néanmoins, l'art. 36 al. 5 LPD prévoit une réglementation spéciale pour les organes fédéraux, qui ne peuvent partager des données personnelles que si une base légale les y autorise[1593]. L'art. 73*c* al. 1 LSI2 prévoit que l'OFCS peut publier des informations au sujet de cyberincidents contenant des données personnelles pour prévenir ou combattre les cyberattaques, à condition d'avoir obtenu le consentement de la personne concernée et uniquement s'il s'agit de caractères d'identification ou de ressources d'adressage.

1588 FF 2017 6565, p. 6648.

1589 EPINEY/FASNACHT, N 20.

1590 CR LPD-FISCHER, art. 17 N 14 ; EPINEY/FASNACHT, N 20 ; MEIER, N 1346.

1591 En effet, les personnes morales ne sont plus protégées par la nouvelle LPD, cf. art. 2 al. 1 aLPD *a contrario* ; cf. *supra* N 700.

1592 FF 2017 6565, p. 6662 ; EPINEY/FASNACHT, N 8 ; PC LPD-FRANCEY, art. 18 N 5.

1593 BSK DSG-EHRENSPERGER, art. 36 N 52 ss ; PC LPD-COSSALI SAUVAIN, art. 36 N 59 ss.

e. La question de l'importation de données personnelles

911 L'importation de données personnelles en Suisse n'est naturellement pas soumise à des règles particulières suisses, dans la mesure où le traitement est directement soumis au champ d'application de l'art. 3 LPD. Ce sont les règles du pays d'export qui doivent être respectées[1594]. Les autres principes et obligations du droit suisse doivent en revanche être respectées lors de l'import de données personnelles.

912 Si l'OFCS ou une prestataire de gestion de cyberincidents vient à réexporter les données en direction de l'État d'origine (ou d'un autre État), les art. 16 s. LPD trouveront application, sous réserve que le cercle des destinataires ne soit pas élargi et que les données ne soient pas renvoyées et modifiées, auquel cas il ne s'agirait pas d'une communication de données[1595].

F. La surveillance

1. Les cas de figure

913 Les prestataires de gestion de cyberincidents peuvent traiter différentes données personnelles dans le cadre de leur activité. Dans l'accomplissement de leurs tâches, elles peuvent effectuer de la surveillance ou du *monitoring*. Tel est le cas lorsqu'une prestataire de gestion de cyberincidents dispose de claires compétences préventives de *monitoring* pour vérifier le bon déroulement des différentes opérations et processus sur les infrastructures informatiques de l'organisation pour laquelle elle œuvre. Le *monitoring* permet de détecter des événements ou des incidents. En outre, lorsqu'un incident est découvert et doit être géré, la prestataire de gestion de cyberincidents surveille les mouvements du trafic, effectue de la journalisation et des analyses d'accès et ainsi de suite. Partant, les données personnelles tant d'employées que de tierces personnes, à l'instar de bénéficiaires de prestations de l'organisation, risquent d'être scrutées.

914 Lorsque la prestataire de gestion de cyberincidents peut voir les accès, les ressources d'adressage et d'autres données de clientes par le biais d'une surveillance de réseau ou d'infrastructure, il s'agit de traitements ordinaires de données personnelles ne soulevant, selon nous, pas de question spécifique.

1594 BSK DSG-DAL MOLIN, art. 16 N 42. À noter que la Commission européenne a conclu début 2024 que la Suisse continuait d'assurer un niveau de protection adéquat des données personnelles transférées depuis l'UE, cf. COMMISSION EUROPÉENNE, *Rapport de la Commission au Parlement européen et au Conseil sur le premier réexamen du fonctionnement des décisions d'adéquation*, 2024, p. 15.

1595 BSK DSG-DAL MOLIN, art. 16 N 43 ss ; BSK DSG-MAURER-LAMBROU/STEINER, art. 6 N 9 ; MEIER, N 1282.

Il s'agit de respecter les principes et obligations de protection des données, à l'instar du devoir d'information[1596].

2. La surveillance des collaboratrices

915 Que la prestataire de gestion de cyberincidents soit interne ou externe à une organisation, elle peut être amenée à effectuer des analyses de données relatives aux collaboratrices de celle-ci, et ce qu'elle agisse en tant qu'autorité ou organisation privée. L'art. 26 OLT 3 encadre la surveillance des collaboratrices et s'applique tant à l'administration fédérale qu'aux entreprises privées[1597]. Ce traitement de données personnelles soulève la question de la surveillance illicite des travailleuses. L'interdiction de la surveillance du comportement des employées, fondée sur les art. 328 et 328b CO et sur l'art. 26 de l'Ordonnance 3 relative à la loi sur le travail (OLT 3), n'égale pas une interdiction totale de l'utilisation des moyens de surveillance, mais bien l'interdiction des systèmes « destinés » à surveiller le comportement des employés. Les systèmes nécessaires pour d'autres raisons ne sont en principe pas visés. Ces « autres raisons » concernent principalement des impératifs de sécurité. Le Tribunal Fédéral (TF) a estimé qu'un « système de surveillance est interdit par l'art. 26 OLT 3 s'il vise uniquement ou essentiellement à surveiller le comportement comme tel des travailleurs. En revanche, son utilisation n'est pas prohibée si, bien qu'emportant objectivement un tel effet de surveillance, il est justifié par des raisons légitimes, telles des impératifs de sécurité ou des motifs tenant à l'organisation ou à la planification du travail ou encore à la nature même des relations de travail. Encore faut-il que le système de surveillance choisi apparaisse, au vu de l'ensemble des circonstances, comme un moyen proportionné au but poursuivi, et que les travailleurs concernés aient préalablement été informés de son utilisation »[1598]. Cela implique que le principe de proportionnalité doit toujours être respecté[1599]. Dans un autre arrêt postérieur, notre Haute Cour a estimé que seuls étaient interdits les moyens de surveillance propres à porter atteinte à la santé ou au bien-être de la travailleuse[1600]. Des

1596 Cf. *infra* N 623 ss.

1597 PFPDT, *Guide surveillance au lieu de travail à l'attention de l'administration fédérale*, 2013, p. 5. L'art. 26 OLT3 découle de l'art. 328b CO, selon lequel l'employeuse ne peut traiter des données concernant ses employées que dans la mesure où elles sont nécessaires à l'exécution du contrat de travail ou dans la mesure où elles portent sur les aptitudes de ce dernier.

1598 ATF 130 II 425, c. 4.2 ; Cour de justice de Genève, Chambre administrative, ATA/329//2013, c. 6b.

1599 ATF 130 II 425, c. 4.2 ; GUISAN/HIRSCH, p. 710 ; MEIER, N 2141.

1600 TF, 6B_536/2009 du 12 novembre 2009, c. 3.6.1. Cependant, les techniques de surveillance purement comportementales sont inadmissibles, cf. PÄRLI, p. 173.

raisons opérationnelles liées à la sécurité peuvent donc être légales si elles ne portent pas atteinte de manière inadmissible à sa santé ou à son bien-être[1601]. Compte tenu de cette appréciation jurisprudentielle, l'on peut admettre que le fait qu'une prestataire de gestion de cyberincidents doive analyser et surveiller un certain trafic pourrait, de manière générale et sous réserve de circonstances propres à chaque cas d'espèce, être licite. À noter que la surveillance doit, en plus d'être proportionnée, être faite de manière transparente[1602].

916 La situation serait différente si une employeuse soupçonne l'une de ses collaboratrices d'être impliquée dans la survenance d'un incident impliquant par exemple la violation de la confidentialité des données qu'elle traite et, partant, la violation de normes légales ou contractuelles[1603]. Dans ce cas, la surveillance peut poursuivre l'objectif de surveiller le comportement d'une ou plusieurs collaboratrices. Que la responsable du traitement soit une entité privée ou publique, les principes de protection des données devront être respectés. Principalement, la proportionnalité, la finalité et la transparence devront être assurées[1604]. À noter que, lorsqu'un organe fédéral est concerné, les analyses ne sont en principe pas menées par l'OFCS, mais par l'Office fédéral de l'informatique et de la télécommunication (OFIT). Au sein d'une autorité, le système gradué des art. 57*m* ss LOGA s'applique. La prestataire de gestion de cyberincidents privée détenant cette compétence doit aussi respecter les trois étapes d'intervention, en débutant par une analyse anonyme, en enchaînant avec l'analyse pseudonyme pour finalement procéder éventuellement à une analyse nominale se rapportant aux personnes[1605]. Cette surveillance personnelle est à mettre en place en tant qu'*ultima ratio* dans les cas où l'employeuse cherche à établir la violation de normes légales ou contractuelles[1606].

1601 SURY, *Digital in Law,* 2021, p. 49.

1602 PÄRLI, p. 173.

1603 Au sujet de l'utilisation abusive, voir art. 10 al. 1 ODPoIEC ; PFPDT, *Guide surveillance au lieu de travail à l'attention de l'administration fédérale,* 2013, p. 8 ; PFPDT, *Guide surveillance au lieu de travail à l'attention de l'économie privée,* 2013, p. 9.

1604 PFPDT, *Guide surveillance au lieu de travail à l'attention de l'administration fédérale,* 2013, p. 4 s. ; PFPDT, *Guide surveillance au lieu de travail à l'attention de l'économie privée,* 2013, p. 6 s. ; MEIER, N 2154.

1605 PFPDT, *Guide surveillance au lieu de travail à l'attention de l'économie privée,* 2013, p. 10 ; GUISAN/HIRSCH, p. 710 ; MEIER, N 2210 ss. En tout état de cause, l'utilisation de logiciels espions est jugée disproportionnée, sous réserve d'une ordonnance judiciaire les prévoyant, ATF 139 II 7, c. 5.5.4 ; Cour de justice de Genève, Chambre administrative, ATA/329/2013, c. 6b ; PFPDT, *Guide surveillance au lieu de travail à l'attention de l'administration fédérale,* 2013, p. 6 ; PFPDT, *Guide surveillance au lieu de travail à l'attention de l'économie privée,* 2013, p. 7.

1606 PÄRLI, p. 173.

G. Un survol d'autres dispositions pertinentes dans la gestion de cyberincidents

1. Le principe de proportionnalité

a. Des généralités

917 Le principe de proportionnalité implique principalement que les données soient aptes à atteindre le but poursuivi par le traitement, qu'elles y soient objectivement nécessaires et que le traitement demeure dans un rapport raisonnable entre le résultat légitime recherché et le moyen utilisé, tout en respectant le plus possible les droits des personnes concernées[1607]. À noter que pour l'OFCS, l'existence d'une base légale ne dispense pas du respect du principe de proportionnalité[1608]. Le principe de minimisation est l'un des corollaires de ce principe particulièrement pertinents dans la pratique des prestataires de gestion des cyberincidents. La question de la proportionnalité temporelle se pose également dans ce contexte.

b. La minimisation de données

918 Le principe de minimisation prévoit que seules les données absolument nécessaires au but poursuivi doivent être traitées[1609]. C'est une expression matérielle du principe de proportionnalité, selon laquelle l'étendue des données collectées, traitées et conservées doit être proportionnelle. L'on entend par là que la prestataire de gestion de cyberincidents ne doit pas collecter des données sans lien avec son activité et sans nécessité pour la réalisation du but poursuivi, à savoir la réponse à un cyberincident[1610].

919 À titre d'exemple, il va de soi que, pour comprendre l'origine de l'intrusion dans un système, une prestataire de gestion de cyberincidents doit souvent analyser les accès et, partant, traiter certaines données personnelles s'y rapportant. Elle peut notamment accéder à un ou plusieurs courriels dans un cas d'hameçonnage ou de logiciel malveillant envoyé par courriel à une collaboratrice de l'organisation cliente. Bien qu'il soit possible en pratique que l'accès soit attribué pour l'entier d'une boîte de réception, la CSIRT doit trier au maximum les données auxquelles elle accède afin de ne traiter que les

1607 FF 2017 6565, p. 6644 ; BSK DSG-MAURER-LAMBROU/STEINER, art. 4 N 9 ; EPINEY, N 24 ; MEIER, N 665 s. ; PC LPD-FRANCEY, art. 6 N 24.

1608 EPINEY, N 25.

1609 FF 2017 6565, p. 6644 ; PFPDT, *TOM*, 2024, p. 30 ; CR LPD-MEIER/TSCHUMY, art. 6 N 33. Sur l'interaction entre la minimisation de données et l'évitement, cf. PC LPD-FRANCEY, art. 6 N 25.

1610 Les qualifications « *need-to-know* » ou « *need-to-have* » sont parfois utilisées, cf. BSK DSG-MAURER-LAMBROU/STEINER, art. 4 N 11.

données nécessaires à la résolution de l'incident. Il est en revanche rarement nécessaire d'accéder au contenu de documents d'employées. Ces données-ci ne doivent par conséquent pas être souvent transmises à la prestataire de cybersécurité.

c. La conservation et la destruction de données

Les données collectées par une prestataire de gestion de cyberincidents sont en pratique conservées durant un certain laps de temps. La conservation permet de répondre à certaines obligations légales. Elle permet également de les réutiliser en cas de besoin dans le cadre de nouvelles attaques ou incidents, d'échanger avec des communautés, de constituer une meilleure image des cybermenaces, de conduire des analyses forensiques ou encore de procéder à de l'*active threat hunting*. La durée de conservation de données personnelles doit être limitée à ce qui est nécessaire au regard des finalités pour lesquelles elles sont collectées, ce qui a en principe trait à la gestion de cyberincidents ou, plus généralement, à la sécurité. Les données doivent être détruites ou anonymisées une fois qu'elles ne sont plus utiles (art. 6 al. 4 LPD). C'est une expression temporelle du principe de proportionnalité qui découle du sous-principe de minimisation des données[1611]. 920

La loi peut prévoir une durée maximale de conservation des données personnelles. L'art. 10*a* LSI2 impose aux autorités et organisations de l'art. 2 LSI de conserver au maximum deux ans après la gestion des violations de la sécurité de l'information ou l'élimination des vulnérabilités, mais dix ans au plus (art. 10*a* al. 6 LSI2)[1612]. D'une façon similaire, l'art. 79 al. 1 LSI2 prévoit que l'OFCS conserve les données aussi longtemps qu'elles sont utiles pour prévenir des dangers ou identifier des incidents, mais au maximum pendant cinq ans à compter de leur dernière utilisation, sous réserve des données sensibles qui sont conservées au maximum deux ans. Cette conclusion est justifiée par l'intérêt qu'il y aurait parfois de garder certaines informations concernant les vecteurs d'attaque notamment pour créer des rapprochements entre les cyberincidents, méthodes d'attaque ou modes opératoires, dans la mesure où ces rapprochements font partie des tâches essentielles de l'OFCS[1613]. 921

Pour établir une durée de conservation respectueuse du principe de proportionnalité, il faut prendre en compte plusieurs considérations concrètes 922

1611 ANDERSON/GALETTI, p. 106 ; CR LPD-MEIER/TSCHUMY, art. 6 N 34 ; EPINEY, N 27 ; MEIER, N 679 ; PC LPD-FRANCEY, art. 8 N 42.

1612 FF 2023 84, p. 25.

1613 FF 2023 84, p. 53 ; FF 2017 2765, p. 2874.

pour les organes fédéraux comme pour les personnes privées. Il faut conserver les données suffisamment longtemps pour permettre une utilisation en justice, si une telle action voit le jour ainsi que, plus particulièrement pour l'OFCS, pour permettre le croisement d'informations pertinentes. Certaines bases légales prévoient des durées à respecter pour certaines informations et obligations à mettre en pratique[1614]. Dans tous les cas, les données doivent être anonymisées ou détruites dès que le but du traitement le permet, ce qui dépend des circonstances de chaque cas d'espèce[1615].

2. Le devoir d'information

923 La personne concernée a un droit à être informée du traitement de données la concernant. Par principe, toute personne a le droit de savoir que ses données sont traitées. Sans information, elle ne peut pas exercer ses autres droits et prétentions[1616]. La responsable du traitement doit informer la personne concernée lors d'un traitement de données personnelles (art. 19 LPD et 13 OPDo)[1617]. Les informations à fournir sont au minimum l'identité et les coordonnées de la responsable du traitement, la finalité du traitement et, le cas échéant, les destinataires ou catégories de destinataires auxquels les données personnelles sont transmises (art. 19 al. 2 LPD). La prestataire de gestion de cyberincidents externe qualifiée de sous-traitante n'a pas à procéder à une telle information, mais c'est l'organisation responsable du traitement qui doit informer les personnes concernées qu'une entité de cette catégorie est susceptible d'obtenir des données les concernant à des fins de gestion d'incidents.

924 Les situations des prestataires internes de gestion de cyberincidents et de l'OFCS diffèrent. Ces entités sont effectivement tenues, en principe, au devoir d'information des personnes concernées en vertu de l'art. 19 LPD indépendamment du fait qu'elles collectent les données directement auprès des personnes concernées ou auprès de personnes tierces[1618]. Les personnes concernées ne sont en pratique pas toujours informées de ces traitements.

1614 Dans une optique pratique, le coût est souvent pris en considération pour fixer la durée de conservation de données, car bien qu'il ne soit pas forcément élevé par principe, le coût peut devenir, au fil d'années de conservation, élevé, cf. NIST, *Computer Security Incident Handling Guide*, 2012, p. 42.

1615 CR LPD-MEIER/TSCHUMY, art. 6 N 36.

1616 FF 2017 6565, p. 6668 ; ETTLINGER, N 3.

1617 FF 2017 6565, p. 6668 ; aussi adressé par ISO/IEC 27035-2 : 2016, p. 32 ; PFPDT, *TOM*, 2024, p. 14 s.

1618 BSK DSG-RAMPINI/FUCHS/KUNZ, art. 19 N 21 s. ; ETTLINGER, N 6. Avec la précision que la responsable du traitement ne collectant pas les données directement auprès de la personne concernée doit, outre les informations de l'art. 19 al. 2 LPD, informer des catégories de données traitées, cf. art. 19 al. 3 LPD.

C'est une conséquence des exceptions au devoir d'informer figurant à l'art. 20 LPD. L'OFCS est susceptible de tomber sous le coup de l'art. 19 al. 3 LPD, qui prévoit la situation dans laquelle la responsable du traitement ne collecte pas les données directement auprès de la personne concernée et devrait, de prime abord, l'informer des catégories de données traitées[1619]. Toutefois, l'art. 20 al. 1 LPD prévoit des exceptions générales, dans lesquelles la responsable du traitement est complètement déliée de son devoir d'information. Cette information n'a pas à être fournie notamment lorsque le traitement est prévu par la loi (art. 20 al. 1 litt. b LPD), ce qui est généralement le cas pour les organes fédéraux, qui ne peuvent traiter des données personnelles sans base légale[1620]. La LSI précise dans sa version révisée les données concernées. Elle mentionne par exemple les données personnelles se rapportant aux ressources d'adressage (art. 76 al. 2 LSI2) ou les données relatives aux personnes impliquées dans les violations ou vulnérabilités (art. 10*a* al. 5 LSI2)[1621]. L'art. 76 al. 1 et 2 LSI2 délie aussi les infrastructures critiques privées de leur devoir d'informer les personnes concernées lorsqu'elles entreprennent une communication de données personnelles à l'OFCS nécessaire à la protection contre les cybermenaces.

925 L'OFCS est légitimé à traiter des données personnelles à l'insu de la personne concernée si l'information entraîne des efforts disproportionnés ou si un intérêt public prépondérant s'y oppose (art. 75 al. 2 LSI2). Par exemple, en cas de requêtes WHOIS[1622], il pourrait être disproportionné d'informer toutes les personnes physiques et morales identifiables de tout traitement d'un nom de domaine, alors que les personnes à contacter le sont souvent de manière ciblée en vue de prendre les mesures qui s'imposent. Étant donné que l'identification de l'utilisatrice finale est en pratique difficile, il se pourrait qu'un traitement de données s'effectue sans que les personnes concernées s'en aperçoivent ou en soient informées[1623]. L'analyse doit naturellement être menée au cas par cas.

926 La responsable du traitement qui a une infrastructure informatique doit informer les personnes concernées de ce possible traitement. En outre et plus particulièrement, l'organisation comptant en son sein une fournisseuse interne de gestion de cyberincidents, de la même manière qu'une prestataire externe détenant une qualité de responsable du traitement (comme cela pourrait par

1619 En plus de la responsable du traitement auprès de laquelle l'OFCS collecte les données.

1620 FF 2017 6565, p. 6671 ; BSK DSG- FUCHS/KUNZ, art. 20 N 17 ss ; PC LPD-JACCOUD/FANTI/STAEGER, art. 20 N 23 ss.

1621 Au sujet de la controverse, cf. CR LPD-FLÜCKIGER, art. 20 N 6.

1622 Requêtes permettant de récupérer des informations sur des noms de domaine.

1623 FF 2017 2765, p. 2872.

exemple être le cas pour une CSIRT sectorielle), est en principe soumise au devoir d'information quant au type de traitement qu'est susceptible d'effectuer son équipe technique. Si les données ne sont pas collectées auprès de la personne concernée et que l'information est impossible à fournir ou nécessite des efforts disproportionnés, le devoir d'information ne s'applique pas (art. 20 al. 2 LPD)[1624]. Cela peut être le cas si une prestataire de gestion de cyberincidents ne dispose que d'un accès permettant d'avoir une adresse IP transmise par une organisation tierce sans autres informations. L'information nécessiterait des efforts disproportionnés notamment si une prestataire de gestion de cyberincidents contrôle un nombre incalculable d'accès de l'ensemble des bénéficiaires des prestations de ses clientes[1625]. En effet et bien que cette exception doive être interprétée de manière restrictive, les efforts que doit entreprendre la fournisseuse de prestations pour informer la personne concernée ne se situent pas dans un rapport raisonnable avec les bénéfices que cette dernière peut en tirer[1626]. Finalement, si ces exceptions de l'art. 20 al. 1 et 2 LPD ne sont pas admises, il reste possible d'exempter la responsable du traitement de son devoir d'information sur la base de l'une des exceptions de l'art. 20 al. 3 LPD. La prestataire externe responsable du traitement pourrait tenter, dans certains cas, de se prévaloir de l'intérêt d'une tierce (en l'occurrence de sa cliente) ou du fait que l'information pourrait, dans d'autres cas, empêcher le traitement d'atteindre son but (art. 20 al. 3 litt. a et b LPD)[1627]. La prestataire interne pourrait renoncer, différer ou restreindre l'information des personnes concernées si l'information empêche le traitement d'atteindre son but ou si ses intérêts prépondérants l'exigent et qu'elle ne communique pas les données à une tierce personne (art. 20 al. 3 litt. a et d LPD)[1628].

3. Le respect des autres principes et obligations de protection des données

927 Les différentes prestataires en gestion de cyberincidents doivent naturellement se conformer aux autres principes et obligations découlant de la LPD. À titre d'exemple, le principe de la licéité (art. 6 al. 1 LPD) doit naturellement être respecté, de même que les principes de la bonne foi de la finalité (art. 6 al. 2 et 3 LPD)[1629]. Les prestataires de gestion de cyberincidents doivent se

1624 FF 2017 6565, p. 6671.

1625 Dans le même ordre d'idées, BSK DSG-FUCHS/KUNZ, art. 20 N 35 ; ETTLINGER, N 22.

1626 FF 2017 6565, p. 6671.

1627 FF 2017 6565, p. 6672 s.

1628 Sur ces différentes exceptions, cf. CR LPD-FLÜCKIGER, art. 20 N 24 ss.

1629 Voir par exemple PFPDT, *TOM*, 2024, p. 6.

conformer aux autres obligations de protection des données, à l'instar de l'obligation d'établir un registre des activités de traitement (art. 12 LPD), d'annoncer les violations de sécurité (art. 24 LPD) ou encore de répondre aux demandes de droit d'accès (art. 25 LPD), tout cela conformément aux responsabilités mutuelles des responsables du traitement et des sous-traitantes.

H. Les traitements illicites et les sanctions en cas de violations

1. La responsabilité civile des prestataires de gestion de cyberincidents

928 La prestataire de gestion de cyberincidents agissant à titre privé peut engager sa responsabilité civile, typiquement si elle traite les données d'un individu en violation des principes imposés par la LPD, contre sa volonté expresse ou si elle communique des données sensibles à de tierces personnes (art. 30 LPD)[1630]. Lorsqu'une atteinte à la personnalité a lieu, elle est présumée illicite, sous réserve de l'art. 30 al. 3 LPD qui pose une présomption (réfragable) exceptionnelle d'absence d'atteinte à la personnalité en cas de mise à disposition à tout public de données personnelles par la personne concernée (art. 30 al. 3 LPD).

929 L'illicéité de l'atteinte peut être levée si l'un des motifs justificatifs de l'art. 31 LPD est réalisé. La disposition prévoit des motifs justificatifs permettant à une prestataire de gestion de cyberincidents de lever l'illicéité d'une atteinte à la personnalité[1631]. La prestataire privée de gestion de cyberincidents auprès d'infrastructures critiques pourrait par exemple se prévaloir de la loi ou de l'intérêt public de la sécurité. L'admissibilité de ce motif dépend toujours des circonstances du cas d'espèce. Les intérêts publics étant souvent concrétisés dans des lois, on pourrait envisager la loi comme motif justificatif pour la communication de données sensibles fournisseuse interne à une infrastructure critique à l'OFCS (par exemple la communication de ressources d'adressage en lien avec des sanctions administratives ou pénales) conformément à l'art. 76 al. 1 LSI2. À défaut, l'intérêt public de sécurité, plus spécifiquement de protection des infrastructures critiques contre les cyberrisques peut être invoqué comme motif justificatif. En effet, lorsqu'il en va de la sécurité des infrastructures critiques, la sécurité intérieure de la Suisse peut constituer un intérêt public entrant facilement en considération. De tels motifs sont constitutifs d'un intérêt public à mettre en balance avec l'atteinte à la personnalité. À défaut, l'intérêt privé principal dont il peut être question à ce titre serait la sécurité de l'organisation affectée par un cyberincident. Ces motifs justificatifs

1630 La liste contenue à l'art. 30 al. 2 LPD n'est pas exhaustive, FF 2017 6565, p. 6688.

1631 CR LPD-BOILLAT/WERLY, art. 30 N 19 ss ; MEIER, N 1521.

sont soumis à une pondération d'intérêts et ne suffisent pas systématiquement à justifier une atteinte et lever son illicéité. Il s'agit bien plutôt d'une réflexion à mener au cas par cas. La liste de l'art. 31 LPD étant non exhaustive, il demeure possible d'invoquer d'autres intérêts, à l'instar de la sécurité ou de la continuité des affaires[1632].

930 D'autres comportements sont susceptibles d'entraîner la responsabilité de la prestataire de gestion de cyberincidents en vertu de la LPD. Tel est le cas si elle ne prend pas les mesures techniques et organisationnelles adéquates pour assurer la sécurité des données traitées. Il en va de même si elle ne respecte pas le principe de proportionnalité, par exemple en conservant des données personnelles durant une trop longue durée. Au sujet du temps de la conservation de données par une prestataire de gestion de cyberincidents, il convient de mettre en balance l'intérêt relatif à la sécurité de l'entreprise poursuivi par la prestataire de gestion de cyberincidents et l'intérêt de la personne concernée à ce que ses données ne soient pas conservées durant un laps de temps disproportionné[1633].

931 Si aucun motif justificatif ne peut être invoqué par la prestataire de gestion de cyberincidents, la personne concernée peut faire valoir des prétentions en agissant par voie civile judiciaire, par la voie pénale ou par dénonciation à la PFPDT. Sur le plan civil et lorsqu'une prestataire privée de gestion de cyberincidents est à l'origine d'une atteinte illicite à la personnalité selon l'art. 30 al. 2 LPD sans pouvoir se prévaloir d'un motif justificatif, la personne concernée peut agir sur la base des art. 28, 28a et 28g à 28l CC (par renvoi de l'art. 32 al. 2 LPD). Ces dispositions confèrent à cette dernière des moyens défensifs et elle peut sur cette base demander l'interdiction d'un traitement illicite déterminé, l'interdiction d'une communication déterminée de données personnelles à autrui ou l'effacement ou la destruction de données personnelles (art. 32 al. 2 LPD)[1634].

2. La responsabilité administrative pour l'OFCS

932 En cas de traitement illicite de données personnelles, l'OFCS peut engager sa responsabilité administrative. Il ne bénéficie pas du même principe que le secteur privé pour lequel l'art. 31 LPD prévoit des motifs justificatifs permettant de lever l'illicéité d'une atteinte à la personnalité. En d'autres termes, l'organe fédéral traitant des données en violant la loi commet *de facto* une

1632 FF 2017 6565, p. 6690.

1633 FF 2017 6565, p. 6689.

1634 FF 2017 6565, p. 6693 ; CR LPD-BOILLAT/WERLY, art. 32 N 15 ss ; PC LPD-GENECAND, art. 32 N 72 ss.

atteinte illicite dont le caractère illicite ne peut pas être levé. Nous sommes donc d'avis que si l'OFCS traite des données en violation d'un principe de protection des données ou d'une obligation en découlant ou lui étant applicable par son statut d'organe fédéral, il risque d'engager directement sa responsabilité. Pour un exemple et compte tenu des obligations incombant spécifiquement aux organes fédéraux, il convient d'admettre que l'OFCS engagerait sa responsabilité s'il communique des données personnelles en violation de l'art. 36 LPD. La loi donne à l'OFCS, moyennant le respect de conditions, la possibilité de communiquer avec les fournisseuses de services de télécommunication, avec les infrastructures critiques, avec des services étrangers proposant des services analogues aux siens ou encore avec le SRC, les autorités de poursuite pénale et les services cantonaux chargés de sécurité (art. 76 à 77 LSI2). Si l'OFCS vient à communiquer des informations à d'autres personnes sans que la loi l'y autorise, ce qui pourrait être le cas par exemple à la PFPDT (dans la mesure où l'art. 24 LPD et l'art. 15 OPDo ne semblent pas consacrer une assistance bidirectionnelle) ou à la FINMA, il procèderait à une communication illicite et la personne concernée pourrait agir à son encontre.

933 La personne dont les données sont traitées illicitement peut requérir que l'OFCS s'abstienne de procéder à un traitement illicite, qu'elle supprime les effets d'un tel traitement ou qu'elle en constate le caractère illicite (art. 41 al. 1 LPD)[1635]. La personne concernée dispose de manière générale des mêmes droits si une prestataire privée de gestion de cyberincidents ou si l'OFCS procède à un traitement illicite, mais la procédure dans ce dernier cas est régie par la PA (art. 41 al. 6 LPD)[1636].

3. La responsabilité commune administrative

934 Qu'il s'agisse d'une prestataire privée de gestion de cyberincidents ou de l'OFCS, la PFPDT est en mesure d'ouvrir une enquête à leur encontre si des indices suffisants laissent à penser qu'un traitement de données personnelles pourrait être contraire à des dispositions de protection des données (art. 49 al. 1 LPD). L'enquête peut être ouverte d'office ou sur dénonciation. La procédure a été récemment unifiée entre le secteur privé et le secteur public. La PFPDT peut, dans des cas de peu d'importance, renoncer à ouvrir une enquête (art. 49 al. 1 LPD). Cela étant, il semble rare qu'une violation de la protection des données personnelles par une autorité comme l'OFCS ou par une organisation soutenant des infrastructures critiques dans leur gestion des

1635 CR LPD-EPINEY, art. 41 N 17 ss ; PC LPD-GENECAND, art. 41 N 3.

1636 FF 2017 6565, p. 6699 s. ; PC LPD-GENECAND, art. 41 N 49 ss.

cyberincidents soit de peu d'importance[1637]. La PFPDT peut aussi renoncer à ouvrir une enquête si des conseils suffisent[1638].

935 Cette procédure, à l'issue de laquelle la PFPDT peut prononcer une ou plusieurs mesures administratives, sert par exemple dans les cas où une communication à l'étranger n'a pas été effectuée dans le respect des art. 16 s. LPD (art. 51 al. 2 LPD). De même, si une violation de la sécurité des données susceptible d'entraîner un risque élevé a été subie par une infrastructure critique et que cette dernière n'en a pas informé la PFPDT ou les personnes concernées qui auraient pu prendre des mesures pour se protéger, la PFPDT peut lui imposer de procéder à cette information (art. 51 al. 3 litt. f LPD).

936 La PFPDT n'est pas une autorité dotée de la faculté d'infliger des sanctions administratives ; elle se limite au prononcé de mesures administratives. Néanmoins, il convient de préciser que si une prestataire de gestion de cyberincidents est soumise à d'autres lois de protection des données personnelles, elle peut, comme pour les autres aspects du droit, être soumise en parallèle au droit étranger. La précision est importante, particulièrement en droit de la protection des données personnelles. Elle importe d'une part dans la mesure où d'autres réglementations légales, à l'instar du RGPD dans l'Union européenne (UE), sont plus exigeantes que le droit suisse. Le RGPD octroie la possibilité aux autorités de contrôle européennes d'infliger des sanctions administratives. D'autre part, de nombreuses entreprises fournissant des prestations de gestion de cyberincidents risquent aujourd'hui d'être soumises à de telles réglementations en vertu de la diversité géographique de leur clientèle[1639].

937 La procédure des art. 49 ss LPD est, de la même manière que pour les prétentions soulevées par une personne dont les données sont traitées par l'OFCS, celle de la PA (par renvoi de l'art. 52 al. 1 PA).

938 Après prononciation de la mesure par la PFPDT, deux voies peuvent être ouvertes. D'une part, la décision de la PFPDT peut, en tant que décision au sens de l'art. 5 PA, faire l'objet d'un recours au TAF. D'autre part, la PFPDT peut assortir sa décision de la menace d'une amende en vertu de l'art. 63 LPD dans l'hypothèse d'une prestataire privée de gestion de cyberincidents, auquel cas la poursuite et le jugement de l'infraction incombent aux cantons (art. 65 LPD).

1637 Pour d'autres exemples, cf. CR LPD-RAEDLER, art. 49 N 51.

1638 FF 2017 6565, p. 6706.

1639 Par exemple sur la base du champ d'application extraterritorial du RGPD (art. 3 par. 2 RGPD).

4. La responsabilité pénale fondée sur la LPD

a. Une limitation des violations analysées

939 Outre les moyens de protection civils ou administratifs déjà parcourus, les membres des différentes prestataires de gestion de cyberincidents, privées ou publiques, peuvent engager leur responsabilité sur le plan pénal. Comme les autres personnes privées traitant des données personnelles, elles peuvent être sanctionnées pénalement en cas de violation des devoirs de collaborer, d'informer ou de renseigner la PFPDT dans le cadre de leurs fonctions (art. 60 LPD). Cette infraction ne soulève pas de questions spécifiques, si ce n'est qu'elle ne s'applique pas aux organes fédéraux dont fait partie l'OFCS. Cette différence peut résider dans la confiance accordée par l'autorité législative aux organes fédéraux. Elle peut également s'expliquer par l'existence en Suisse de procédures séparées visant les organes fédéraux, comme la procédure de responsabilité de l'État[1640]. On pourrait également considérer que la surveillance large exercée sur les organes fédéraux est suffisante, avec le fait qu'ils sont soumis au respect de la loi indépendamment de toutes sanctions pénales éventuelles[1641].

940 En parallèle, la PFPDT peut, lorsqu'elle prononce une mesure au sens de l'art. 51 LPD, l'assortir, à nouveau uniquement pour les prestataires privées de gestion de cyberincidents, de la menace d'une amende allant jusqu'à 250 000 CHF en vertu de l'art. 63 LPD.

941 À noter que pour ces différentes infractions, le droit pénal relatif à la protection des données en Suisse vise en premier lieu les personnes physiques, ce qui a par ailleurs soulevé de vives critiques dans le cadre de la révision du droit de la protection des données personnelles récemment menée[1642]. Il est tout de même possible, si les conditions sont réunies, de poursuivre l'entreprise au sein de laquelle la violation a été commise en lieu et place d'une personne physique. Lorsque la DPA s'applique, l'autorité de poursuite pénale compétente (au sens de l'art. 65 al. 1 LPD) peut, si l'amende ne dépasse pas 50 000 CHF et que l'enquête rendrait nécessaires des mesures d'instruction disproportionnées avec la peine encourue par la personne physique poursuivie selon l'art. 6 DPA, renoncer à poursuivre cette dernière et condamner l'entreprise à sa place au paiement de l'amende (art. 64 LPD et 7 DPA)[1643].

1640 Cf. *supra* N 765 ss ; MÉTILLE/MEYER, p. 32.

1641 MEIER, N 1954.

1642 FF 2017 6565, p. 6713 s.

1643 FF 2017 6565, p. 6718.

942 Au-delà de ces différentes considérations, il convient de s'arrêter sur deux infractions suscitant plus d'intérêt dans le cadre de la présente étude. Il s'agit de la violation des devoirs de diligence et de la violation du devoir de discrétion.

b. La violation des devoirs de diligence

943 L'infraction de violation des devoirs de diligence (art. 61 LPD) n'est envisageable que pour l'entreprise fournissant des prestations de gestion de cyberincidents et non pour l'OFCS. La personne active dans une telle entreprise peut être poursuivie et condamnée sur cette base tout d'abord si elle communique des données personnelles à l'étranger à défaut de fondement selon les art. 16 s. LPD[1644]. L'infraction est aussi réalisée lorsqu'une prestataire externe de cyberincidents confie le traitement de données personnelles à une sous-traitante, à l'instar d'une entreprise de solutions en nuage, sans que l'organisation cliente ne donne son accord (art. 9 al. 3 LPD). Finalement, les devoirs de diligence sont également violés si une prestataire ne respecte pas les exigences en matière de sécurité des données édictées par le CF aux art. 1 ss OPDo (par renvoi de l'art. 8 al. 3 LPD). La violation des devoirs de diligence est une infraction intentionnelle. Cette disposition s'adresse aux personnes disposant d'un pouvoir de direction lorsque l'infraction est commise au sein d'une entreprise, dans la mesure où la compétence de décider du respect des devoirs de diligence revient à la direction (comme le prévoit aussi l'art. 29 CP)[1645].

c. La violation du devoir de discrétion

944 Contrairement à l'infraction susmentionnée, la violation du devoir de discrétion (art. 62 LPD) s'applique tant aux personnes privées qu'aux organes fédéraux. Si la collaboratrice d'une prestataire de gestion de cyberincidents révèle intentionnellement des données personnelles secrètes (au sens des art. 320 s. CP) portées à sa connaissance dans l'exercice de ses fonctions, elle peut être condamnée à une amende de 250 000 CHF sur la base de l'art. 62 LPD. Cette infraction peut entrer en concours avec d'autres normes protégeant des secrets. L'avantage de cette disposition est qu'elle élargit le cercle des détentrices du secret, en comparaison au cercle limité des auteures potentielles de l'art. 321 CP ou à l'exclusion jusqu'à l'entrée en vigueur de la LPD révisée des auxiliaires dans l'application de l'art. 320 CP, même si elle leur est subsidiaire[1646].

1644 Sur les communications transfrontières de données personnelles, cf. *supra* N 897 ss.

1645 FF 2017 6565, p. 6716 ; CR LPD-MÉTILLE, art. 60 N 31.

1646 FF 2017 6565, p. 6717 ; BSK StGB-OBERHOLZER, art. 321 N 13 ; CR CP II-CHAPPUIS, art. 321 N 25 ; CR LPD-MÉTILLE, art. 62 N 13 ; PC LPD-GENECAND, art. 62 N 14 ; WEBER/WILLI, p. 61. Pour plus d'informations sur l'art. 62 LPD, cf. PAHUD/PITTET, N 49 ss.

I. Une synthèse

Certaines informations sont protégées légalement, car elles concernent des individus. Les traitements de données personnelles sont soumis à des principes et obligations pour s'assurer que la personnalité et les droits fondamentaux des personnes concernées sont respectés. Certains principes et certaines obligations sont particulièrement pertinentes dans le contexte de la gestion de cyberincidents. La LPD est prise comme exemple, car elle est susceptible de s'appliquer à une majorité de prestataires de gestion de cyberincidents en Suisse. 945

Pour déterminer ces principes et obligations pertinentes, il est nécessaire de faire une distinction entre l'OFCS et les fournisseuses de prestations de gestion de cyberincidents internes à des autorités et organisations publiques d'une part et les prestataires privées de gestion de cyberincidents d'autre part. Les premières constituent des organes fédéraux et sont soumises à des dispositions particulières à ce titre. Les secondes sont soumises au régime applicable aux responsables du traitement et sous-traitantes privées. Il faut donc distinguer les situations dans lesquelles une prestataire de gestion de cyberincidents agit comme une responsable du traitement indépendante ou conjointe ou comme une sous-traitante. 946

La LPD dispose que l'OFCS et les fournisseuses de prestations publiques sont soumises au principe de la légalité. Il est donc nécessaire qu'une base légale prévoit leurs traitements de données personnelles. L'ensemble des prestataires de gestion de cyberincidents sont en revanche soumises aux autres principes et obligations de la LPD. En particulier, le principe de sécurité s'applique à leur activité. Il implique que les prestataires de gestion de cyberincidents doivent prendre les mesures de sécurité qui s'imposent pour assurer l'intégrité, la disponibilité, la confidentialité et la traçabilité des données personnelles qu'elles traitent. Ce principe, sa concrétisation et les obligations qui y sont connexes peuvent également servir à assurer certains aspects de cybersécurité dans leurs activités. 947

En outre, la LPD couvre les questions relatives aux communications de données personnelles. Il est important en pratique de savoir quelles obligations et quelles démarches sont possibles dans le cadre de leurs échanges nationaux et internationaux, dans la mesure où ces échanges sont centraux à leur pratique. 948

D'autres dispositions sont pertinentes dans la pratique des prestataires de gestion de cyberincidents. Par exemple, une attention particulière doit être portée par ces expertes lorsqu'elles prennent des mesures de surveillance ou de *monitoring*. Elles doivent également respecter le principe de proportionnalité, en particulier dans son sous-principe de minimisation de données ou en 949

termes de durée de conservation. Le devoir d'information peut finalement différer en fonction du rôle de la prestataire de gestion de cyberincidents, raison pour laquelle les expertes doivent être conscientes de leur qualité, des données qu'elles traitent et de l'information donnée aux personnes concernées.

950 En cas de violation de ces principes ou obligations, les prestataires de gestion de cyberincidents sont susceptibles d'engager leur responsabilité. La LPD prévoit plusieurs voies permettant aux personnes concernées d'agir en vue de remédier à un traitement illicite.

951 D'autres informations sont protégées légalement. Les raisons de cette protection peuvent varier. Les informations couvertes par des secrets sont consacrées dans la loi pour protéger une multitude d'intérêts. La protection légale des secrets ne porte pas sur des principes et obligations aussi étendues que la protection conférée par la loi aux données personnelles. En revanche, la protection des secrets équivalant à une interdiction de communiquer certaines informations, les conséquences de cette protection légale peuvent être importantes en pratique.

IV. La protection des secrets

A. L'intérêt de la question en pratique

952 De manière générale, un secret couvre un fait connu d'un cercle restreint de personnes, que la personne détenant la maîtrise du secret a la volonté de garder confidentiel pour sauvegarder un intérêt légitime. Ces éléments ont été affirmés par le TF et repris par la doctrine, en tout cas pour le secret de fonction et le secret professionnel[1647]. En pratique, les prestataires de gestion de cyberincidents peuvent être soumises au respect de plusieurs secrets. L'OFCS est naturellement soumise, en tant qu'autorité, au secret de fonction. D'autres secrets obligent l'office fédéral comme les autres prestataires de gestion de cyberincidents et les infrastructures critiques en général. Il peut s'agir du secret de fabrication ou commercial, de secrets spécifiques à certains secteurs à l'instar du secret bancaire ou de différents secrets contractuels.

953 Alors que la protection des données personnelles couvre la protection d'informations par le respect de différents principes et obligations pour une

1647 Voir notamment FF 2017 6717 ; ATF 142 IV 65, c. 5.1 ; ATF 127 IV 122, c. 1 ; ATF 114 IV 44, c. 2 ; CR CP II-CHAPPUIS, art. 321 N 28 ss ; CR CP II-FISCHER/RICHA/RAEDLER, art. 162 N 10 ss et références citées ; CR CP II-VERNIORY, art. 320 N 14 ss ; PC CP-DUPUIS et al., art. 320 N 8, 15 ss ; CORBOZ, volume II, art. 320 CP N 12 ; ÉRARD, N 420 et 424 ss. La même définition est retenue pour les autres types de secrets, cf. par exemple CR CP II-CHAPPUIS, art. 321 N 27 ss pour le secret professionnel.

multitude de traitements, la protection des secrets vise principalement à limiter les communications d'informations couvertes par des secrets. Ces dernières ont un impact dans l'activité de l'OFCS et des autres prestataires de gestion de cyberincidents, dans la mesure où ces intervenantes ne peuvent partager des informations secrètes que, comme nous allons le voir, moyennant le respect de conditions. La divulgation de ces informations est par principe interdite, qu'elle soit envisagée entre deux ou plusieurs entités ou à l'attention du public. L'art. 4 litt. a LTrans prévoit par ailleurs une réserve en faveur des secrets lorsqu'il en va du devoir d'information de l'État. Certaines circonstances prévues légalement ou contractuellement peuvent lever cette interdiction de communiquer des données secrètes et permettre aux différentes prestataires de gestion de cyberincidents de recevoir et partager des informations considérées comme secrètes. Nous allons parcourir quelques exemples de secrets susceptibles de revêtir un intérêt dans la gestion de cyberincidents.

B. Des exemples de secrets pertinents

1. Le secret de fonction

L'on peut fonder le secret de fonction sur l'art. 320 CP ou sur d'autres dispo- 954
sitions de droit public. Dans tous les cas, l'art. 320 CP revêt une importance particulière dans la compréhension de ce secret. La disposition est consacrée à la responsabilité liée à la violation de l'obligation de garder le secret de fonction[1648]. Ce secret a pour objectif de protéger les particuliers et le bon fonctionnement des institutions publiques[1649]. Il couvre des informations relatives aux citoyennes qui doivent communiquer des informations de toute sorte avec les autorités ainsi que les informations sensibles pour le bon fonctionnement de l'administration et de la justice. La transparence régissant par principe l'activité de l'État, la notion de secret est restreinte[1650]. Conformément à l'obligation de garder le secret, les détentrices du secret ne doivent pas transmettre les affaires du service, qui doivent demeurer confidentielles du fait de leur nature ou en vertu de prescriptions légales ou d'instructions.

1648 Au sujet de la controverse sur le fondement du secret de fonction, voir CR CP II-VERNIORY, art. 320 N 3 s. ; ÉRARD, N 541 ss.

1649 BSK StGB II-OBERHOLZER, art. 320 N 4 s. ; CORBOZ, volume II, art. 320 CP N 3 ; CR CP II-VERNIORY, art. 320 N 5 ; PC CP-DUPUIS et al., art. 320 N 2 s. Cette pluralité d'intérêts protégés explique l'importance pratique des secrets parallèlement à la protection des données personnelles, ÉRARD, N 240.

1650 BSK StGB-OBERHOLZER, art. 320 N 4 s. ; CORBOZ, volume II, art. 320 CP N 3 ; CR CP II-VERNIORY, art. 320 N 5.

955 Contrairement à d'autres lois qui le concrétisent (à l'instar de l'art. 110 de la Loi fédérale sur l'impôt fédéral direct (LIFD) ou de l'art. 74 de la Loi fédérale régissant la taxe sur la valeur ajoutée (LTVA), la LSI se limite à rappeler la portée de l'art. 320 CP, à savoir que des informations couvertes par le secret de fonction peuvent être révélées avec le consentement de l'autorité supérieure (art. 320 ch. 2 CP). Elle ne concrétise toutefois pas l'étendue de l'obligation pour l'OFCS qui doit garder secrets les faits dont il a connaissance dans l'exercice de ses fonctions. Partant, la nature secrète d'une information dépend davantage de sa nature ou des instructions que reçoit l'OFCS[1651]. Ses collaboratrices doivent informer la personne à la tête de l'office lorsqu'elles ont connaissance d'une infraction dans le cadre d'un signalement ou de leur analyse. Cette dernière bénéficie de la dérogation de l'art. 73*d* al. 3 LSI2 à l'art. 22*a* LPers. La personne à la tête de l'OFCS peut dénoncer une infraction connue dans le cadre d'un signalement ou d'une analyse si la gravité de l'infraction le justifie. Les infractions dont les collaboratrices de l'office auraient connaissance hors de la procédure de signalement suivent le sort de l'art. 22*a* LPers[1652].

956 Les fournisseuses de prestations de gestion de cyberincidents internes à des autorités ou organisations publiques, à l'instar d'un SOC interne ou de la RSSI d'infrastructures critiques étatiques, sont soumises au secret de fonction de l'art. 320 CP dès lors qu'elles travaillent pour une autorité ou une organisation étatique. Il en va de même pour les prestataires externes à de telles autorités ou organisations. À l'origine, ces dernières prestataires n'étaient pas soumises à cette obligation par ce biais, dans la mesure où l'art. 320 CP ne connaissait pas, contrairement à l'art. 321 CP, la notion d'auxiliaire ; seules les fonctionnaires peuvent être poursuivies pour violation du secret de fonction (délit propre)[1653]. L'art. 62 LPD sert aujourd'hui de fondement pour que ces auxiliaires externes soient soumises à une obligation de garder le secret sur les données personnelles secrètes[1654]. Pour la question des autres données secrètes, le CF a demandé à l'AF d'étendre le cercle des personnes visées par l'art. 320 CP afin que la disposition s'applique de la même façon que l'art. 321 CP en soumettant les auxiliaires au secret, ce qui permet aux fonctionnaires leur communiquant des données secrètes de ne pas violer l'art. 320 CP dans la mesure où la communication est nécessaire à leur mission[1655].

1651 CR CP II-VERNIORY, art. 320 N 25 ; PC CP-DUPUIS et al., art. 320 N 19.

1652 FF 2023 84, p. 29.

1653 FF 2017 2765, p. 2886 s.

1654 FF 2017 6565, p. 6717 ; CR LPD-MÉTILLE, art. 62 N 9. À noter que les questions de concours ne devraient pas poser de problème en pratique, les art. 320 s. CP primant l'art. 62 LPD, cf. CR LPD-MÉTILLE, art. 62 N 13.

1655 FF 2017 2765, p. 2888 ; ÉRARD, N 494.

2. Le secret de fabrication et secret commercial ou d'affaires

Le secret d'affaires, de fabrication ou commercial est consacré dans différentes dispositions légales. L'art. 22 LPers soumet le personnel de la Confédération au secret de fabrication et d'affaires selon l'art. 321a al. 4 CO. Le secret d'affaires est également prévu pour le plan contractuel (par renvoi des art. 364 al. 1 et 398 al. 1 CO pour les contrats d'entreprise et de mandat), dans le domaine de la concurrence (cf. art. 6 et 4 litt. c LCD) ou encore dans le droit pénal (art. 162 et 273 CP). 957

Sont comprises comme des informations couvertes par le secret de fabrication les informations englobant les recettes et moyens de fabrication qui ne sont pas de notoriété publique et qui revêtent une valeur importante pour la fabricante. Cette notion comprend des caractéristiques techniques concernant les procédés et modèles utilisés, les substances et matières employées, les recettes suivies ainsi que le savoir professionnel[1656]. Le secret commercial (ou secret d'affaires) couvre toutes les informations touchant l'exploitation, la situation commerciale et l'organisation d'une entreprise. Cette notion comprend notamment les listes de clientes, les stratégies commerciales adoptées, les sources d'achat et de ravitaillement, les marges de bénéfices ou encore le rendement de machines utilisées[1657]. Bien que la question se pose de savoir si une différence existe entre la notion de secret commercial et celle de secret d'affaires, il semblerait que les deux notions soient régulièrement utilisées comme synonymes[1658]. Il est important que ces informations représentent un avantage pour la personne détenant la maîtrise du secret sur le marché pour être considérées comme des secrets[1659]. 958

La délimitation entre l'expérience professionnelle librement exploitable et les secrets de fabrication ou d'affaires peut être compliquée. Les informations couvertes par ce secret se rattachent à une entreprise. Seules les informations techniques, organisationnelles ou financières spécifiques à l'employeuse peuvent être tenues secrètes sur cette base, en opposition aux connaissances 959

1656 ATF 103 IV 283, c. 2b ; BSK StGB-HUSMANN, art. 273 N 13 ; BSK StGB-NIGGLI/HAGENSTEIN, art. 162 N 18 ; BSK UWG-FRICK, art. 6 N 16 ; CORBOZ, volume I, art. 162 CP N 7 ; CR CP II-FISCHER/RICHA/RAEDLER, art. 162 N 19 ; PC CP-DUPUIS et al., art. 162 N 8, art. 273 N 5.

1657 ATF 103 IV 283, c. 2b ; BSK StGB-HUSMANN, art. 273 N 13 ; BSK StGB-NIGGLI/HAGENSTEIN, art. 162 N 19 ; BSK UWG-FRICK, art. 6 N 17 ; CR CP II-FISCHER/RICHA/RAEDLER, art. 162 N 20 ; PC CP-DUPUIS et al., art. 162 N 9, art. 273 N 5 ; CORBOZ, volume I, art. 162 CP N 8 ; SURY, *Digital in Law,* 2021, p. 97.

1658 CR CP II-FISCHER/RICHA/RAEDLER, art. 162 N 21 précisent que la langue allemande ne fait pas de différence avec la notion *« Geschäftsgeheimnis »,* contrairement aux versions italienne et française, et en citant la jurisprudence fédérale utilisant les deux termes de manière alternative.

1659 BSK UWG-FRICK, art. 6 N 33 ; CR CP II-FISCHER/RICHA/RAEDLER, art. 162 N 4, 15 ; DE WERRA, p. 376.

pouvant être acquises au sein d'autres entreprises de la même branche[1660]. Pour aiguiller la décision, les autorités judiciaires mettent en balance les intérêts de la personne détenant la maîtrise du secret avec ceux de l'employée, dont l'avancement économique après son départ d'une entreprise ne doit pas être rendu excessivement difficile par une obligation de secret[1661]. En d'autres termes, il faudrait que l'information soit propre à une entreprise déterminée pour être qualifiée de secret[1662]. Par ailleurs, l'art. 162 CP ne protège que les secrets matériels, à savoir les informations bénéficiant d'un intérêt suffisant pour justifier leur caractère secret, typiquement en lien avec la valeur commerciale de l'information, en opposition aux secrets formels qui ne sont que des faits déclarés secrets sans qu'il soit nécessaire d'en examiner le contenu ou l'importance objective[1663]. Dans l'optique où l'on reconnaît que seuls les secrets matériels doivent être gardés, il faut, outre l'accord entre les parties portant sur les données soumises au secret et la définition de règles et de mesures pour protéger les informations secrètes[1664], que les parties présentent effectivement un intérêt justifiant le caractère secret de ces informations.

960 Les collaboratrices d'une infrastructure critique sont en pratique régulièrement soumises au secret de fabrication ou d'affaires en fonction des informations auxquelles elles accèdent. Les collaboratrices d'une entreprise active dans la sécurité informatique, peu importe la forme de cette dernière, sont aussi soumises en pratique, soit légalement soit contractuellement, à l'obligation de conserver certaines données secrètes en vertu du secret d'affaires ou de fabrication. Elles peuvent y avoir accès par exemple en investiguant ou, plus simplement, si un cyberincident visant le système informatique d'une entreprise est susceptible d'engendrer la fuite de données de fabrication ou si, durant l'analyse d'un incident, elles ont accès au code source d'un logiciel. Qu'il s'agisse d'une prestataire privée de gestion de cyberincidents ou de l'OFCS, cette obligation de garder le secret les limite dans leurs échanges d'informations. En effet, ces dernières ne peuvent pas communiquer à des tierces des informations couvertes par le secret d'affaires ou de fabrication sans se prévaloir d'un des motifs justificatifs usuels en droit pénal, sous peine de violer leur obligation en vertu de l'art. 162 ou 273 CP.

1660 ATF 138 III 67, c. 2.3.2 ; CR CP II-FISCHER/RICHA/RAEDLER, art. 162 N 22 ; DE WERRA, p. 374.

1661 BSK StGB-NIGGLI/HAGENSTEIN, art. 162 N 20 ; BSK UWG-FRICK, art. 6 N 21. Il peut être plus aisé de procéder à l'analyse sous l'angle de la sauvegarde des intérêts de de l'employeuse selon l'art. 321*a* al. 4 CO, cf. BSK UWG-FRICK, art. 6 N 21 et référence citée.

1662 CR CP II-FISCHER/RICHA/RAEDLER, art. 162 N 22.

1663 CR CP II-FISCHER/RICHA/RAEDLER, art. 162 N 14 et 25 ; DE WERRA, p. 375.

1664 DE WERRA, p. 378.

3. Le secret professionnel

De la même manière que le secret de fonction, le secret professionnel protège tant un intérêt public qu'un intérêt privé[1665]. La liste exhaustive des personnes y étant soumises figure à l'art. 321 ch. 1 CP, qui réprime la violation de ce secret. Cette liste comprend des professions spécifiques assignées dans la société. L'obligation de garder le secret a une portée plus limitée que le secret de fonction notamment, dans la mesure où l'art. 321 CP contient une liste des personnes y étant soumises. 961

L'art. 22 al. 1 LPers prévoit, de la même manière que pour le secret de fonction, une soumission des fonctionnaires au secret professionnel. La définition prévue par la loi se veut large en admettant les divers secrets susceptibles de jouer un rôle dans le cadre d'un emploi auprès de la Confédération[1666]. 962

L'OFCS n'entre pas dans la liste exhaustive de l'art. 321 CP[1667] et n'est par conséquent pas soumis en tant que tel au secret professionnel. De la même manière, les autres prestataires de gestion de cyberincidents n'entrent pas expressément dans le champ d'application de la disposition. En revanche, l'art. 321 CP s'applique aux auxiliaires de la détentrice du secret. La notion d'auxiliaire est large et vise les individus, effectivement aptes à remplir la mission qui leur est confiée, dont la collaboration est nécessaire au travail des personnes pratiquant l'une des professions visées par l'art. 321 CP et qui prennent connaissance de secrets dans ce contexte[1668]. La qualification juridique de la relation entre l'auxiliaire et la personne soumise directement à l'art. 321 CP n'est pas déterminante, de la même manière qu'une relation de subordination n'est pas nécessaire[1669]. 963

Pour se demander si une prestataire de gestion de cyberincidents pourrait être considérée comme auxiliaire, il faut que sa cliente entre dans le champ d'application de l'art. 321 ch. 1 CP. Bon nombre de personnes au sein d'infrastructures critiques n'y sont pas soumises, mais certaines professionnelles y sont personnellement soumises. Il en va de la sorte pour les médecins et autres soignantes et professionnelles de santé énumérées dans la liste de l'art. 321 ch. 1 CP travaillant au sein d'un hôpital ou d'un autre établissement médico-hospitalier responsable de l'exécution de tâches publiques[1670]. À noter 964

1665 CR CP II-CHAPPUIS, art. 321 N 7 ss.

1666 FF 1999 1421, p. 1444.

1667 CR CP II- CHAPPUIS, art. 321 N 1 et 48.

1668 CR CP II- CHAPPUIS, art. 321 N 50 ; CORBOZ, volume II, art. 321 N 16.

1669 CR CP II-CHAPPUIS, art. 321 N 54.

1670 ÉRARD, N 518.

par ailleurs que les médecins des services de santé publique, considérées parallèlement comme fonctionnaires au sens de l'art. 110 CP, sont soumises tant au secret de fonction qu'au secret professionnel[1671].

965 Les auxiliaires sont les personnes qui apportent un soutien étroitement lié à l'exercice de l'activité de la professionnelle soumise à l'art. 321 CP et prennent dans ce cadre connaissance de faits secrets[1672]. Le TF, se fondant sur l'interprétation de CHAPPUIS et ALBERINI, a jugé dans une affaire concernant un avocat que « le professionnel externe chargé de la conservation et de la protection à distance des données informatiques de l'avocat » devait être considéré comme auxiliaire de l'avocat[1673]. Cette réflexion peut s'appliquer par analogie à une médecin selon ÉRARD[1674]. Les médecins de ces établissements doivent, outre prodiguer des soins, satisfaire d'autres obligations dont le devoir de diligence duquel découle une obligation de sécurité (voir notamment l'art. 398 al. 2 CO lorsque la médecin est employée en tant que mandataire)[1675]. Le traitement informatisé des informations de patientèle étant aujourd'hui implanté en pratique, il va de soi que la médecin doit, pour satisfaire à son exigence de diligence, assurer la sécurité des infrastructures et données de santé. Cette tâche, déléguée à une unité technique, fait donc partie des obligations que doivent respecter les médecins et, *a fortiori,* les établissements au sein desquels elles exercent. Voilà pourquoi la prestataire de gestion de cyberincidents doit selon nous être considérée comme apportant un soutien étroitement lié à l'activité des médecins employées par un établissement hospitalier. En outre, bien que l'étendue de l'accès aux données des patientes dépende des missions d'une prestataire de gestion de cyberincidents à une autre, il n'est pas exclu que celle-ci accède à des données de patientes, structurées ou non, plus qu'occasionnellement. Dans la mesure où un débat existe quant à la qualification d'une entreprise de nettoyage d'auxiliaire, il faut selon l'opinion ici défendue considérer qu'une prestataire de gestion de cyberincidents est une personne susceptible d'avoir accès à des données secrètes au sens de l'art. 321 CP, sous réserve des circonstances de chaque cas d'espèce[1676].

1671 ÉRARD, N 385.

1672 BSK StGB-OBERHOLZER, art. 321 N 10 ; PC CP-DUPUIS et al., art. 321 N 19 s. À noter que la qualification du contrat liant l'auxiliaire à la personne soumise au secret n'est pas déterminante, cf. CORBOZ, volume II, art. 321 CP N 16 ; PC CP-DUPUIS et al., art. 321 N 19.

1673 ATF 145 II 229, c. 7.3 ; CHAPPUIS/ALBERINI, p. 339 s.

1674 ÉRARD, N 406.

1675 CR CO I-WERRO, art. 398 N 13 et 25.

1676 Au sujet de la controverse de l'entreprise de nettoyage, ÉRARD, N 402 ss et références citées.

L'OFCS n'agit en revanche pas comme auxiliaire au sens de l'art. 321 CP. Il n'apporte pas un soutien étroitement lié à l'exercice de l'activité de la professionnelle, mais agit pour remplir ses missions. Les personnes qui effectuent auprès de l'OFCS des signalements doivent s'assurer qu'elles respectent leurs obligations légales ou contractuelles de garder le secret[1677]. Les informations que l'OFCS acquiert sont ensuite susceptibles d'être soumises au secret de fonction. Il nécessite donc l'autorisation écrite de l'autorité supérieure pour communiquer plus loin les informations concernées (art. 320 ch. 2 CP)[1678]. 966

Compte tenu de ces informations, nous estimons que la prestataire de gestion de cyberincidents remplit dans ce genre de contexte les conditions à la qualification d'auxiliaire selon l'art. 321 CP. Elle fournit en principe à la personne initialement soumise au secret professionnel, en exécution d'un contrat de service, des prestations contribuant étroitement à l'exercice de sa profession, en nécessitant d'accéder à des données soumises à ce secret[1679]. 967

Selon cette analyse, la prestataire de gestion de cyberincidents peut acquérir des informations secrètes de la part de la détentrice initiale du secret. Cela ne veut pas dire pour autant que la détentrice initiale du secret lui confie des données secrètes, mais qu'elle a la possibilité de le faire[1680]. Par ailleurs, la titulaire du secret peut interdire à la détentrice du secret de transférer des données secrètes à sa ou ses auxiliaire(s)[1681]. Nous peinons néanmoins à concevoir la situation dans laquelle une personne refuserait le transfert de ses données à une personne compétente justement pour assurer la sécurité de celles-ci, à condition que les informations en question soient nécessaires à l'activité de la prestataire de gestion de cyberincidents. Outre la faculté offerte à la prestataire de gestion de cyberincidents de se voir communiquer des informations secrètes, la conséquence principale de sa qualification d'auxiliaire a trait au fait qu'elle doit à son tour respecter l'art. 321 CP. 968

4. Le secret des télécommunications

Selon l'art. 43 LTC, découlant de l'art. 13 al. 1 Cst., il est interdit à toute fournisseuse de services de télécommunication de transmettre des renseignements 969

1677 FF 2023 84, p. 26.

1678 Il ne peut en revanche pas révéler le secret avec le simple accord de la détentrice du secret comme le prévoit l'art. 321 ch. 2 CP).

1679 À noter que le rapport entre les art. 320 et 321 CP fait l'objet de controverses qui ne seront pas examinées, dans la mesure où elles n'ont pas une importante portée pratique dans le contexte étudié dans la présente étude ; au sujet de la controverse, voir ÉRARD, N 1274 ss.

1680 Cf. notamment ÉRARD, N 406.

1681 CR CP II-CHAPPUIS, art. 321 N 77 ; CORBOZ, volume II, art. 321 CP N 72.

sur les communications des usagères à de tierces personnes, ainsi que de permettre à quiconque de communiquer de tels renseignements. Ce secret vise le contenu des communications ainsi que les données secondaires, à savoir les données concernant les participantes à la communication et autres paramètres de lieu et temps[1682].

970 Il semble rare en pratique qu'une prestataire de gestion de cyberincidents interne à une fournisseuse de services de télécommunication soit le service compétent pour transmettre des informations couvertes par le secret des télécommunications au Service chargé de la surveillance de la correspondance par poste et télécommunication (Service SCPT) en vertu de l'art. 1 al. 1 de la Loi sur la surveillance de la correspondance par poste et télécommunication (LSCPT) dans le cadre d'une procédure pénale.

971 En tant que requérantes d'informations couvertes par le secret des télécommunications, les organisations privées et publiques offrant des prestations de gestion de cyberincidents ne sont pas habilitées à demander au Service SCPT d'obtenir ces données auprès des fournisseuses de services de télécommunication. En revanche, l'art. 76 al. 2 LSI2 permet à l'OFCS d'obtenir des informations (y compris des données personnelles) relatives aux ressources d'adressage directement auprès des fournisseuses de services de télécommunication si elles sont utiles à la protection des infrastructures critiques contre les cybermenaces. La lecture du message de la première version de la LSI ne permet pas d'affirmer que ces informations s'étendent aux données couvertes par le secret des télécommunications, et le message de la version révisée de la loi n'apporte pas de précisions quant à cette question. Les seules communications de données prévues par le premier message visent les informations telles que des fichiers journaux contenant les adresses IP d'ordinateurs infectés par des logiciels malveillants[1683]. Une fois en possession des informations de l'art. 76 al. 2 LSI2, l'OFCS ne peut par ailleurs les transmettre aux autorités de poursuite pénale qu'à condition que les fournisseuses de services de télécommunication y aient, en tant que détentrices initiales, consenti[1684]. Dans ce cas de figure, les informations relatives aux communications des usagères semblent demeurer protégées par le secret des télécommunications et sont probablement rarement nécessaires en pratique. De plus, l'OFCS n'est pas une autorité habilitée par la LSCPT à accéder aux informations couvertes par le secret des télécommunications et est donc limité par le secret des télécommunications s'il souhaite avoir accès aux flux de communications auprès des

1682 WERLY/BARRELET, N 1094 ; WEBER/WILLI, p. 60.

1683 FF 2017 2765, p. 2873.

1684 FF 2017 2765, p. 2872 s.

fournisseuses de services de télécommunication. Ce flux permet d'avoir accès aux données secondaires qui ne peuvent être transmises qu'aux conditions de la LSCPT et des art. 269 ss CPP, auxquels renvoie l'art. 179*octies* CP.

Le secret des télécommunications peut donc constituer une barrière à 972
l'obtention d'informations pour les autres prestataires de gestion de cyberincidents. De manière générale, il ne paraît pas nécessaire pour ces organisations d'obtenir des données couvertes par le secret des télécommunications en vue de contenir un cyberincident, limiter ses dommages et restaurer une situation sûre.

5. D'autres secrets spécifiques

De nombreux autres secrets existent pour des secteurs ou sous-secteurs par- 973
ticuliers. À titre d'exemple, les art. 272 et 274 CP ainsi que 86 CPM consacrent les secrets d'État et les secrets militaires[1685]. Il existe dans le secteur critique des finances le secret bancaire consacré à l'art. 47 LB. D'autres secrets sont consacrés dans la loi, à l'instar du secret en matière de recherche médicale (art. 321*bis* CP), du secret fiscal et ainsi de suite. L'obligation des prestataires de gestion de cyberincidents de garder des secrets spécifiques à certains secteurs dépend des organisations pour lesquelles elles opèrent.

6. Les secrets contractuels

Certains contrats soumettent la prestataire de gestion de cyberincidents à une 974
obligation de garder le secret, comme le contrat de travail (art. 321*a* al. 4 CO) ou le contrat de mandat (art. 398 al. 1 CO). Une violation de garder un secret sur le plan pénal constitue en principe également une violation de l'obligation contractuelle de secret. Néanmoins, les deux protections, pénale et civile, ne se recoupent pas entièrement. Alors que le droit pénal ne protège que la volonté objectivement justifiée du maître du secret, la protection civile du secret couvre toutes les informations déterminées comme subjectivement secrètes par la mandante. En parallèle, une obligation de discrétion peut exister dans le contrat liant une prestataire de gestion de cyberincidents à sa cliente. Elle peut porter sur des informations plus connues ou accessibles et impliquer que la prestataire de gestion de cyberincidents ne peut pas en parler inutilement au public.

L'obligation de secret et de discrétion porte sur toutes les informations 975
que la mandataire apprend à l'occasion de l'exécution de son mandat, sous

1685 Concernant ces secrets, GovCERT est principalement tenue de ne pas communiquer des secrets d'État ou des secrets militaires. Une autre équipe de gestion de cyberincidents susceptible de voir sa pratique impactée par ces secrets est la MilCERT, la CERT de l'armée.

réserve des informations que la mandante a autorisé la mandataire à révéler à de tierces personnes ou d'autres circonstances découlant de l'exécution diligente du mandat et conforme aux instructions, ou de la loi[1686].

C. Des exemples de violations d'une obligation de garder le secret

1. La violation du secret de fonction

976 Nous avons vu que plusieurs prestataires de gestion de cyberincidents, dont l'équipe exploitée par l'OFCS, sont susceptibles d'être soumises au secret de fonction de l'art. 320 CP. Naturellement, elles peuvent engager leur responsabilité pénale si elles contreviennent à leur obligation de garder le secret[1687]. Pour retenir une violation du secret de fonction, il faut réunir les éléments constitutifs de l'art. 320 CP, à savoir la révélation intentionnelle[1688] d'un secret[1689], par la collaboratrice d'une autorité ou par une fonctionnaire, à une personne non autorisée, ainsi que le lien de causalité entre la révélation du secret et la prise de connaissance. Pour admettre qu'une collaboratrice de l'OFCS, d'une autre autorité ou qu'une auxiliaire soumise à l'art. 320 CP contrevient à son secret de fonction, il faut que le secret soit rendu accessible à une personne tierce ne faisant pas partie du cercle de personnes autorisées[1690].

977 Ce partage d'informations est permis dans certaines situations. Il l'est pour les communications entre collègues de la même autorité, entre une fonctionnaire et sa supérieure ou dans des contextes d'entraide et d'assistance entre autorités à condition qu'une loi le prévoie. À défaut, la communication d'informations secrètes revient à une violation de son devoir de garder le secret selon l'art. 320 CP[1691].

978 En dehors de ces situations et si aucune loi n'existe, le consentement écrit de l'autorité supérieure ou le consentement de l'intéressée peuvent permettre à une fonctionnaire de communiquer des informations soumises au secret. L'art. 320 ch. 2 CP permet à l'autorité supérieure, à savoir probablement le

1686 Dans le cadre du contrat de mandat, cf. MÜLLER, N 2820 ss.

1687 L'infraction est par ailleurs poursuivie d'office, contrairement à la violation du secret professionnel qui est poursuivie uniquement sur plainte ; ATF 106 IV 131, c. 5 ; PC CP-DUPUIS et al., art. 320 N 7.

1688 La négligence entraîne une exclusion de la punissabilité sur le plan pénal, ce qui n'exclut pas des sanctions disciplinaires, cf. PC CP-DUPUIS et al., art. 320 N 32.

1689 Pour la définition du secret, cf. *supra* N 952.

1690 Et ce même si la destinataire est soumise à un secret, cf. CR CP II-VERNIORY, art. 320 N 30. En outre, l'infraction par une fonctionnaire peut être commise par omission, cf. TPF, SK.2006.18 du 31 mai 2007, c. 3.4 ; CR CP II-VERNIORY, art. 320 N 29 ; PC CP-DUPUIS et al., art. 320 N 25.

1691 BSK StGB-OBERHOLZER, art. 320 N 12 ; CR CP II-VERNIORY, art. 320 N 33.

DDPS, sa cheffe ou son SG[1692] pour l'OFCS, d'effectuer une pesée des intérêts et de donner son consentement lorsque ses collaboratrices ont besoin de partager des données secrètes, par exemple avec une CERT établie à l'étranger qui aurait des informations permettant de rétablir une situation sûre après l'attaque d'une organisation soutenue par l'office fédéral.

En pratique, les différentes prestataires de gestion de cyberincidents, dont l'OFCS lorsqu'il soutient des infrastructures critiques, se basent probablement davantage sur le consentement de l'intéressée[1693]. Néanmoins, ce motif n'est envisageable que lorsque seul un intérêt privé est en jeu[1694]. Les secrets protégés par l'OFCS couvrent souvent, outre un intérêt privé, un intérêt public. Partant, elle ne peut pas systématiquement se limiter au consentement de l'intéressée ou de la fournisseuse de l'information pour fonder des communications de données secrètes. 979

Il reste finalement toujours le motif justificatif de l'intérêt légitime, qui doit dans chaque cas être proportionné au but poursuivi et dont l'auteure de l'infraction peut se prévaloir uniquement subsidiairement aux autres moyens légaux[1695]. À noter à nouveau en termes de concours que l'art. 62 LPD, réprimant la violation du devoir de discrétion de celui ou celle ayant pris connaissance de données personnelles secrètes dans l'exercice de ses fonctions, est subsidiaire à l'art. 320 CP[1696]. 980

2. La violation du secret de fabrication et d'affaires

Plusieurs infractions peuvent être réalisées en cas de révélation d'un secret de fabrication ou d'affaires. Il est possible de se rendre coupable de révélation de ce secret au sens de l'art. 162 CP en cas de violation d'une obligation légale ou contractuelle de garder le secret à son profit ou à celui d'une personne tierce. En cas de mise à disposition de tels secrets à un organisme officiel ou privé étranger, à une entreprise privée étrangère ou à leurs collaboratrices, l'art. 273 CP risque d'entrer en application. Plus rarement, la LCD s'applique en cas de divulgation de secret surpris ou appris indûment dans un contexte de concurrence (art. 6 et 23 al. 1 LCD). 981

1692 L'autorité supérieure concrète dépend de l'organisation des départements fédéraux, mais l'organigramme du DDPS depuis sa réorganisation en janvier 2024 n'étant pas disponible à l'heure du dépôt de la présente étude, il conviendra de s'assurer de ce point une fois la réorganisation officielle du département achevée.

1693 Différentes dispositions de la LSI illustrent ce souhait de tenir compte du consentement des personnes intéressées, cf. notamment art. 73c al. 2 ou art. 74 al. 4 LSI2.

1694 BSK StGB-OBERHOLZER, art. 320 N 13.

1695 Voir notamment ATF 127 IV 122, c. 5c et référence citée ; BSK StGB-OBERHOLZER, art. 320 N 17.

1696 CR CP II-VERNIORY, art. 320 N 59 ; PC CP-DUPUIS et al., art. 320 N 44.

982 L'art. 162 CP protège l'intérêt économique ou commercial découlant du patrimoine de la personne détenant la maîtrise du secret. Pour que l'art. 162 al. 1 CP entre en compte, il faut premièrement un secret commercial ou de fabrication matériel, en ce sens que les informations concernées doivent, en plus d'avoir été déclarées secrètes, bénéficier d'un intérêt important pour justifier leur caractère secret[1697].

983 Deuxièmement, le secret doit présenter une valeur économique sur le marché, procurer ainsi un avantage sur celui-ci à la personne détenant la maîtrise du secret et sa divulgation doit être susceptible d'impacter le résultat commercial de cette dernière[1698].

984 Troisièmement, un devoir légal ou contractuel de garder le secret doit exister. La doctrine semble partagée sur la question de savoir si ce devoir ne peut découler que d'une clause contractuelle explicite ou s'il peut intervenir par interprétation de l'accord[1699]. Nous estimons, en suivant la position du TF, que l'obligation peut découler d'une interprétation de l'accord ou des circonstances dans le cas où la travailleuse doit être consciente du fait qu'elle n'a été initiée aux secrets qu'à la condition de les garder confidentiels et que le contrat, sa formation, sa position dans l'entreprise et ainsi de suite y sont liés d'une certaine manière, ce bien qu'une convention explicite soit naturellement souhaitable et en pratique récurrente sous forme d'un accord de confidentialité[1700]. Pourraient être concernées les informations auxquelles peut accéder une collaboratrice seulement après s'être connectée avec un mot de passe protégé au réseau interne d'une entreprise disponible uniquement à un cercle limité de personnes[1701].

985 Quatrièmement, la personne soumise au secret doit rendre accessible l'information à une personne non autorisée, à savoir qu'elle doit élargir le cercle des détentrices du secret en portant à la connaissance d'autrui, même partiellement, le secret[1702].

1697 CR CP II-FISCHER/RICHA/RAEDLER, art. 162 N 14 et 25. Sur le plan subjectif toutefois, il faut que la volonté de la personne détenant la maîtrise du secret, portant sur le maintien du secret, soit suffisamment claire pour la détentrice, cf. BSK StGB-NIGGLI/HAGENSTEIN, art. 162 N 16.

1698 TF, 6B_65/2015 du 25 mars 2015, c. 1.3.3 ; CR CP II-FISCHER/RICHA/RAEDLER, art. 162 N 4, 15 et 18.

1699 BSK UWG-FRICK, art. 6 N 37 ; CR CP II-FISCHER/RICHA/RAEDLER, art. 162 N 25 ; PC CP-DUPUIS et al., art. 162 N 5 semblent partager cette opinion, à l'inverse de BSK StGB-NIGGLI/HAGENSTEIN, art. 162 N 24.

1700 Comme décidé par le TF dans son ATF 80 IV 22, c. 2b. Le manque de clarté de cette position peut être critiqué, cf. BSK StGB-NIGGLI/HAGENSTEIN, art. 162 N 23 s. et références citées.

1701 Dans un ordre d'idées comparable, cf. BSK UWG-FRICK, art. 6 N 38.

1702 CR CP II-FISCHER/RICHA/RAEDLER, art. 162 N 27 s. ; PC CP-DUPUIS et al., art. 162 N 10.

Cinquièmement, il faut l'intention de communiquer les informations soumises au secret et, par conséquent, de violer les devoirs imposés[1703]. 986

À noter que les motifs justificatifs usuels du CP, en particulier le consentement de la personne détenant la maîtrise du secret, peuvent être invoqués dans le cadre de l'art. 162 CP[1704]. Si la révélation est utilisée à des fins de profit, par exemple pour une organisation concurrente (ou travaillant avec des organisations concurrentes), les membres de cette dernière risquent également d'engager leur responsabilité pénale sur la base de l'art. 162 al. 2 CP, dans le cas où elles utiliseraient cette information à leur profit ou à celui d'une personne tierce[1705]. 987

L'art. 273 CP protège quant à lui la souveraineté territoriale, l'indépendance de la Suisse et l'économie nationale d'intrusions étrangères (par exemple d'espionnage) et, dans un second temps, les intérêts économiques des personnes et entreprises établies en Suisse[1706]. L'art. 273 al. 2 CP réprime le fait, pour la collaboratrice d'une prestataire de gestion de cyberincidents assistant une organisation établie en Suisse[1707], de rendre accessible un secret de fabrication ou d'affaires à un organisme officiel ou privé étranger, à une entreprise privée étrangère ou à leurs collaboratrices. 988

Pour que l'infraction soit réalisée, il faut premièrement des renseignements économiques pour lesquels la Suisse, en tant qu'entité politique ou économique, a un intérêt direct à la préservation ou pour lesquels des personnes tierces ont un intérêt digne de protection au maintien et n'ont pas donné leur consentement préalable [1708]. Il semblerait que la volonté de la 989

1703 CR CP II-FISCHER/RICHA/RAEDLER, art. 162 N 35 ; PC CP-DUPUIS et al., art. 162 N 13.

1704 CR CP II-FISCHER/RICHA/RAEDLER, art. 162 N 40.

1705 CR CP II-FISCHER/RICHA/RAEDLER, art. 162 N 31 s. ; PC CP-DUPUIS et al., art. 162 N 11 s.

1706 CR CP II-FISCHER/RICHA, art. 273 N 3 ; PC CP-DUPUIS et al., art. 273 N 2. Le TF a retenu que l'espionnage économique d'une entreprise suisse entraînait en tout cas une mise en danger des intérêts de l'État, ATF 101 IV 312, c. 1 ; ATF 98 IV 209, c. 1b ; CR CP II-FISCHER/RICHA, art. 273 N 11.

1707 Ce qui suffit en principe à admettre un rattachement territorial avec la Suisse, à condition encore que les données concernent l'économie suisse, question qui importe notamment lorsque le secret a principalement une portée privée, cf. CR CP II-FISCHER/RICHA, art. 273 N 17 ; PC CP-DUPUIS et al., art. 273 N 8. Si seule la prestataire de gestion de cyberincidents se situe en Suisse, mais qu'elle fournit ses prestations à une organisation étrangère, le rattachement territorial à la Suisse n'est pas suffisant pour que l'art. 273 CP s'applique. À noter que BSK StGB-HUSMANN, art. 273 N 55 estime que l'art. 273 CP conserve sa pertinence si la personne détenant la maîtrise primaire du secret ne fait pas partie de l'économie suisse, mais que le maintien du secret de faits économiques touche également les intérêts de l'économie suisse.

1708 La notion de renseignement économique se base sur celle de secret de fabrication ou commercial de l'art. 162 CP, cf. BSK StGB-HUSMANN, art. 273 N 10 ss ; PC CP-DUPUIS et al., art. 273 N 4.

personne détenant la maîtrise du secret puisse résulter d'une expression explicite ou des circonstances elles-mêmes (par exemple lorsque des données sont remises à une détentrice du secret tenue au secret par la loi)[1709]. Il existe plusieurs intérêts au maintien du secret, tels que celui à ne pas dévoiler des informations à ses concurrents ou à ne pas être poursuivi pénalement par des autorités étrangères[1710]. Contrairement à ce qui est prévu à l'art. 162 CP, l'art. 273 CP ne requiert pas une obligation préalable de garder le secret, dans la mesure où la notion de secret à l'art. 273 CP est plus large que celle de l'art. 162 CP et peut englober tous les faits de la vie économique[1711]. Les secrets protégés par l'art. 273 CP peuvent être de deux types. Il peut s'agir d'une part de secrets d'importance nationale pour la souveraineté et l'économie de la Suisse. D'autre part, il peut s'agir de secrets de nature privée concernant des individus ou entités suisses ou établies en Suisse et dont la divulgation peut avoir un impact médiat sur les intérêts économiques nationaux[1712].

990 Deuxièmement, l'auteure de l'infraction doit rendre accessible le secret[1713], par exemple en transmettant des données en utilisant une technique de chiffrement pouvant être surmontée sans effort considérable.

991 Troisièmement, elle doit rendre accessible le secret à une destinataire, à savoir un organisme officiel ou privé étranger, une entreprise étrangère ou leurs agents[1714].

992 Quatrièmement et sur le plan subjectif, il faut l'intention et le dessein de rendre le secret accessible à l'une de ces destinataires[1715].

993 Dans le cadre de l'art. 273 CP, l'état de nécessité (art. 17 CP) peut, dans de rares cas et suivant une pesée des intérêts, servir de motif justificatif, par exemple dans le cas où un État étranger mettrait l'auteure sous pression. Il en

1709 BSK StGB-HUSMANN, art. 273 N 34.

1710 CR CP II-FISCHER/RICHA, art. 273 N 14.

1711 BSK StGB-HUSMANN, art. 273 N 10 ; PC CP-DUPUIS et al., art. 273 N 5, 12.

1712 Cf. notamment ATF 104 IV 175, c. 4a ; ATF 98 IV 209, c. 1b ; BSK StGB-HUSMANN, art. 273 N 7 ; CR CP II-FISCHER/RICHA, art. 273 N 16.

1713 CR CP II-FISCHER/RICHA, art. 273 N 26.

1714 Il se justifie que les organismes privés étrangers soient compris au même titre que les institutions politiques publiques, dans la mesure où ils peuvent être tout autant amenés à vouloir espionner d'autres organisations, BSK StGB-HUSMANN, art. 273 N 62. Sont compris dans cette notion également les organes communautaires d'une communauté à laquelle plusieurs États auraient cédé une partie de leurs droits de souveraineté, cf. ATF 104 IV 175, c. 5a ; BSK StGB-HUSMANN, art. 273 N 28 ss ; CR CP II-FISCHER/RICHA, art. 273 N 21 ss ; PC CP-DUPUIS et al., art. 273 N 18 ss. La question du caractère étranger d'une organisation se pose toujours dans le contexte notamment des filiales et groupes de sociétés, bien que l'on puisse utiliser l'élément de la dépendance économique pour s'aider, cf. BSK StGB-HUSMANN, art. 273 N 64-66.

1715 BSK StGB-HUSMANN, art. 273 N 75 ss ; PC CP-DUPUIS et al., art. 273 N 3 ; CORBOZ, volume II, art. 273 CP N 15.

va également de la sorte lorsqu'une demande intervient dans le cadre d'une procédure d'entraide judiciaire internationale, qui est, elle, considérée comme un motif justificatif légal selon l'art. 14 CP[1716]. La question du consentement comme motif justificatif est délicate et a trait à la question de savoir qui est la personne détenant réellement la maîtrise du secret[1717]. La sauvegarde d'intérêts légitimes peut également constituer un motif justificatif extralégal, typiquement dans les cas de lancements d'alerte ou de *whistleblowing*[1718].

L'on peut retenir un concours entre l'art. 162 al. 1 et l'art. 273 CP, dans la mesure où les intérêts protégés par les dispositions ne sont pas les mêmes[1719]. Dans le domaine bancaire, si la collaboratrice d'une prestataire de gestion de cyberincidents interne à un établissement divulgue la liste des clientes d'une banque, elle peut se rendre coupable d'une violation du secret de fabrication ou d'affaires en concours avec une violation du secret bancaire selon l'art. 47 LB. À l'inverse, si le secret a trait uniquement à la cliente de la banque, l'art. 47 LB devrait primer[1720]. Les art. 320 s. CP sont en principe considérés comme des *leges speciales* par rapport à l'art. 162 CP, contrairement à l'art. 273 CP qui peut se retrouver en concours avec ces dispositions[1721]. Il en va de même pour l'application cumulée des art. 6 et 23 LCD qui sanctionnent pénalement la violation des secrets de fabrication et commerciaux dans le cadre spécifique de la concurrence déloyale, dans la mesure où la loi ne s'applique que dans le complexe de faits dans lequel un avantage concurrentiel est en jeu[1722]. 994

3. D'autres violations

Il existe naturellement d'autres infractions à une obligation de garder des secrets, qui sont propres à certains secteurs, qui supposent certaines pratiques 995

1716 BSK StGB-HUSMANN, art. 273 N 78 et 83 ss ; CR CP II-FISCHER/RICHA, art. 273 N 26 ; PC CP-DUPUIS et al., art. 273 N 29 s. ; CORBOZ, volume II, art. 273 CP N 18.

1717 Pour des avis sur la controverse, cf. notamment BSK StGB-HUSMANN, art. 273 N 87 ; CR CP II-FISCHER/RICHA, art. 273 N 36 ; PC CP-DUPUIS et al., art. 273 N 31 et références citées.

1718 BSK StGB-HUSMANN, art. 273 N 88 et références citées.

1719 BSK StGB-HUSMANN, art. 273 N 99 ; BSK StGB-NIGGLI/HAGENSTEIN, art. 162 N 47 ; CR CP II-FISCHER/RICHA/RAEDLER, art. 162 N 41 ; CR CP II-FISCHER/RICHA, art. 273 N 33 ; PC CP-DUPUIS et al., art. 162 N 16, art. 273 N 33.

1720 De la même manière que l'art. 42 LIMF, cf. CR CP II-FISCHER/RICHA/RAEDLER, art. 162 N 41 s. À noter que certains courants retiennent un concours de manière moins nuancée en admettant purement le concours entre les art. 162 CP et 47 LB, cf. BSK StGB-HUSMANN, art. 273 N 99 ; CORBOZ, volume I, art. 162 N 19 ; PC CP-DUPUIS et al., art. 162 N 18.

1721 ATF 113 Ib 77, c. 3a ; BSK StGB-NIGGLI/HAGENSTEIN, art. 162 N 48 s. ; CR CP II-FISCHER/RICHA/RAEDLER, art. 162 N 42 ; CR CP II-FISCHER/RICHA, art. 273 N 34 ; PC CP-DUPUIS et al., art. 162 N 17, art. 273 N 34.

1722 BSK UWG-FRICK, art. 6 N 61 ; CORBOZ, volume I, art. 162 N 21 ; CR CP II-FISCHER/RICHA/RAEDLER, art. 162 N 42 ; PC CP-DUPUIS et al., art. 162 N 19. Sur la controverse théorique, voir BSK StGB II-NIGGLI/HAGENSTEIN, art. 162 N 53 s.

et qui soulèvent d'autres questions. Ces autres infractions peuvent être réalisées selon le domaine d'activité de la prestataire de gestion de cyberincidents, typiquement pour les cas où elle est interne à une infrastructure critique. Les collaboratrices de certaines fournisseuses internes de prestations de gestion de cyberincidents[1723] peuvent engager leur responsabilité pénale pour violation du secret professionnel selon l'art. 321 CP, infraction poursuivie sur plainte. Il faut pour admettre cette infraction un secret, une personne soumise à l'obligation de garder le secret, une information confidentielle apprise dans l'exercice d'une profession, une révélation[1724], la prise de connaissance par une personne non autorisée et l'intention[1725]. La révélation doit rendre le secret et la personne détenant sa maîtrise identifiable aux yeux de la personne non autorisée. Par exemple, des informations permettant de connaître l'existence d'une relation entre une patiente et une professionnelle de santé constituent déjà un fait secret. Les informations permettant d'identifier une telle relation ne doivent donc pas être communiquées, sous réserve de motifs justificatifs[1726]. Si une prestataire communique un secret totalement anonymisé à des fins scientifiques, elle ne serait pas considérée comme ayant violé son devoir de conserver le secret[1727]. Nous y voyons une échappatoire pour la prestataire qui échangerait notamment avec d'autres entreprises fournissant des prestations de gestion de cyberincidents, dans un intérêt d'établissement d'une vue des cybermenaces. En outre, il est toujours possible pour l'autorité compétente de lever le secret ou d'agir avec le consentement de l'intéressée[1728].

996 Il existe naturellement d'autres infractions à une obligation de garder des secrets, qui sont propres à certains secteurs, qui supposent certaines pratiques et qui soulèvent d'autres questions. Pour un autre cas de figure, l'art. 47 LB criminalise à son al. 1 litt. a le fait de transmettre ou vendre des données soumises au secret bancaire et à son al. 1 litt. c l'utilisation pour son propre profit ou celui d'une tierce personne des secrets obtenus en violation du secret professionnel[1729]. Si ces données sont utilisées pour son propre profit, il n'est pas nécessaire qu'elles soient transmises à une personne tierce. L'art. 47 al. 1bis LB

1723 CR CP II-CHAPPUIS, art. 321 N 138 s. ; CORBOZ, volume II, art. 321 CP N 84 ; cf. *supra* N 964 s.

1724 Susceptible d'être commise, comme la violation du secret de fonction, par omission (art. 11 CP), cf. CORBOZ, volume II, art. 321 CP N 68 ; CR CP II-CHAPPUIS, art. 321 N 70.

1725 PC CP-DUPUIS et al., art. 321 N 9.

1726 ÉRARD, N 434.

1727 CORBOZ, volume II, art. 321 CP N 69 ; CR CP II-CHAPPUIS, art. 321 N 71.

1728 BSK StGB-OBERHOLZER, art. 321 N 22 s. ; CR CP II-CHAPPUIS, art. 321 N 140 ss ; PC CP-DUBUIS et al., art. 321 N 38 ss ; CORBOZ, volume II, art. 321 CP N 43 ss.

1729 FF 2014 5997, p. 6002. L'on voit donc que l'art. 47 LB prévoit un mécanisme similaire à celui de l'art. 162 al. 1 et 2 CP.

prévoit une peine menace plus lourde pour l'individu révélant ou exploitant un secret à son profit ou à celui d'une autre personne s'il a le dessein d'obtenir un avantage pécuniaire, pour lui ou pour autrui. L'art. 47 al. 2 LB réprime l'infraction commise par négligence[1730]. Contrairement à la violation du secret professionnel, la violation du secret bancaire est une infraction poursuivie d'office[1731]. À noter que l'illicéité de l'infraction peut être levée lorsque des obligations légales imposent à la personne soumise au secret de témoigner ou renseigner les autorités, qui priment alors le secret bancaire (art. 47 al. 5 LB)[1732]. Ainsi, la personne membre d'une prestataire de gestion de cyberincidents soumise au secret bancaire devant témoigner sur la base des art. 166 al. 2 du Code de procédure civile (CPC) ou 173 al. 2 CPP ne se rend pas coupable d'infraction à l'art. 47 LB si l'intérêt à la divulgation du secret l'emporte sur l'intérêt à son maintien. Elle est considérée comme déposant licitement en vertu des art. 160 al. 1 litt. b CPC ou encore 265 CPP malgré sa soumission au secret bancaire[1733]. Les motifs justificatifs classiques, à l'instar du consentement typiquement du client de la banque ou de l'état de nécessité (sous réserve d'une mise en balance des intérêts concernant ce second motif), continuent à s'appliquer[1734].

997 Nous rappelons qu'une attention doit être portée au fait que plusieurs infractions peuvent être réalisées en fonction des circonstances. La violation du secret bancaire peut par exemple entrer en concours idéal avec d'autres violations de secrets, à l'instar du secret professionnel, dans la mesure où les deux secrets protègent des intérêts différents et qu'un seul acte suffit à réaliser les conditions de plusieurs infractions[1735].

D. Une synthèse

998 Les obligations de garder des informations secrètes servent à empêcher des accès non autorisés à certaines informations méritant une protection particulière. Il existe une diversité d'obligations de garder le secret dont la violation est susceptible d'engager la responsabilité pénale de la personne trahissant son obligation.

1730 BSK BankG-STATENWERTH, art. 47 N 18.

1731 FF 2014 5997, p. 5998 ; BSK BankG-STATENWERTH, art. 47 N 4.

1732 BSK BankG-STRATENWERTH, art. 47 N 30 ss.

1733 BSK BankG-STRATENWERTH, art. 47 N 33 et 35.

1734 BSK BankG-STRATENWERTH, art. 47 N 25 et 43 ss.

1735 CR CP II-CHAPPUIS, art. 321 N 26.

999 Le secret de fonction concerne une diversité de prestataires de gestion de cyberincidents en pratique. L'OFCS est soumis au secret de fonction qui implique notamment des procédures particulières si ses collaboratrices prennent connaissance d'infractions dans le cadre de leur activité. D'autres fournisseuses internes de prestations de gestion de cyberincidents publiques sont également soumises au secret de fonction.

1000 Le secret commercial est consacré dans différentes lois et de nombreuses prestataires de gestion de cyberincidents risquent d'être concernées par ce secret, ce qui implique une attention dans leurs échanges d'informations quant aux informations qu'elles partagent.

1001 Le secret professionnel peut être applicable à certaines prestataires de gestion de cyberincidents en fonction de l'organisation qu'elles servent. Ce secret soulève la question de savoir si une telle prestataire doit être considérée comme une auxiliaire au sens de l'art. 321 CP. Le cas est possible bien qu'il faille toujours tenir compte de l'ensemble des circonstances du cas d'espèce.

1002 L'importance du secret des télécommunications se manifeste différemment en pratique. Dans la pratique de l'OFCS, ce secret peut impliquer un obstacle à l'obtention d'informations auprès des fournisseuses de services de télécommunication.

1003 Il existe d'autres secrets légaux et contractuels envisageables dans la pratique des prestataires de gestion de cyberincidents. La violation des différentes obligations est susceptible d'entraîner la responsabilité pénale de la personne communiquant de façon illégale une information couverte par le secret. Chaque infraction est soumise à des éléments constitutifs différents et les communications peuvent dans certains cas se fonder sur des motifs justificatifs spéciaux ou généraux.

1004 Les obligations de garder le secret impliquent en particulier l'interdiction de communiquer des informations couvertes par un secret sous réserve de motifs justificatifs. En revanche, ces obligations ne vont pas plus loin dans la sécurité qui doit être assurée pour éviter que des personnes non autorisées accèdent aux informations concernées.

V. En pratique

A. De la théorie à la pratique

1005 Une diversité d'informations plus ou moins sensibles est susceptible d'être traitée par les prestataires de gestion de cyberincidents. Pour assurer le respect des différentes obligations accompagnant le traitement de certaines données, notamment couvertes par des secrets ou constitutives de données

personnelles, la loi prévoit des garde-fous. Néanmoins, en pratique, le respect de ces obligations s'assure au travers des contrats et accords liant les prestataires de gestion de cyberincidents à leurs clientes (et autres interlocutrices). Certains outils servent à concrétiser les obligations susmentionnées. Il en va principalement des accords de confidentialité, des classifications et des contrats de sous-traitance de données personnelles, qui permettent de prévenir la communication illicite d'informations et de s'assurer de la responsabilisation de la prestataire de gestion de cyberincidents.

L'OFCS ne nécessite pas d'être lié par un contrat aussi précis que les prestataires de gestion de cyberincidents privées, dans la mesure où la loi institue son cadre d'action. Néanmoins, ses clientes peuvent se lier avec l'autorité par un *gentlewoman's agreement,* par des clauses de confidentialité qui poursuivent principalement la finalité de préciser quelles informations peuvent ou non être partagées avec quel cercle de destinataires[1736]. Les prestataires de gestion de cyberincidents sont en principe liées par des contrats de prestations de services informatiques, qui concrétisent les obligations relatives aux secrets de l'employeuse ou de la mandataire (voir notamment art. 321*a* al. 4 et art. 340 CO imposent un devoir de discrétion à la travailleuse, de même que la prohibition de faire concurrence à son employeuse, ou les art. 364 al. 1 et 398 al. 1 CO qui imposent aux prestataires externes le devoir de garder le secret dans le cadre d'un contrat d'entreprise, respectivement de mandat)[1737]. Le secret ne se limite en effet pas à la communication indue à une personne tierce, la prestataire ne doit pas non plus stocker imprudemment des données y étant soumises[1738]. 1006

Compte tenu de ces éléments, il est important de comprendre que des solutions pratiques sont exploitées afin de prévenir le risque de divulgation ou mise à disposition illicite d'informations méritant une certaine protection, dans le cadre de contrats liant une prestataire de gestion de cyberincidents à ses clientes ou de conventions entre différentes intervenantes. 1007

B. Les outils contractuels

1. Le périmètre

De nombreux contrats liant les différentes intervenantes comptent des clauses contractuelles portant sur les données comprises dans le contrat afin de régler 1008

1736 Ce type d'accords ne prennent pas forcément la forme écrite et ils ont une valeur de contrat. En revanche, disposer d'une trace écrite (même électroniquement) est à préférer pour des questions de preuve. Sur les accords de confidentialité, cf. *infra* N 1011 ss.

1737 CR CP II-CHAPPUIS, art. 321 N 24 ; WEBER/WILLI, p. 62.

1738 WEBER/WILLI, p. 62.

contractuellement les questions liées aux définitions, aux responsabilités et aux communications envisageables. Ces questions doivent être prévues en sus de celles concernant les services complémentaires (à l'instar de la maintenance et autres prestations)[1739].

1009 En pratique, les prestataires de gestion de cyberincidents sont liées à leurs clientes par des contrats. Ces contrats prévoient en principe les prestations concernées, leurs modalités, les questions relatives aux prix et ainsi de suite. Parmi les points à régler figure normalement le périmètre ou « *scope of engagement* » qui regroupe les informations visées par le contrat. En ce sens sont entendues les informations auxquelles peut accéder la prestataire de gestion d'incidents, celles qu'elle peut traiter ou communiquer et le cas échéant à qui. En principe, la relation contractuelle entre la prestataire et sa cliente prend une certaine forme[1740] et est assortie de clauses sur les informations utilisables par la fournisseuse de prestations. En revanche, les prestataires de gestion de cyberincidents coopérant ou communiquant avec des tierces ayant des fonctions analogues ont parfois pour seule interaction la communication ou l'échange de données. Partant, dans ce cadre, des contrats de transfert ou d'échange de données (techniques d'une part et personnelles d'autre part et si nécessaire) sont conclus[1741].

1010 Il est en tout cas aujourd'hui nécessaire de prévoir contractuellement le partage de données, techniques, secrètes ou constitutives de données personnelles. Plusieurs questions se posent en pratique, dont des questions juridiques relatives au traitement de certaines données et d'éventuels secrets ainsi qu'à l'appréhension de la complexité légale et réglementaire de la situation[1742]. Le traitement de données personnelles convenu contractuellement devant faire l'objet d'une annexe spécifique (art. 9 LPD)[1743], la communication d'autres données doit être analysée en tenant compte de la relation entre les parties contractantes, de la durée ou non dans laquelle elle s'inscrit, d'une potentielle contrepartie prévue et ainsi de suite. Ces contrats doivent être assortis de garanties venant des parties et des restrictions à l'utilisation de données (souvent relatives à des secrets). Dans les secteurs critiques, ces pratiques sont en principe déjà implémentées, du moins auprès des entreprises de grande taille[1744].

1739 JACCARD/ANCELLE, p. 8 s.

1740 Cf. *supra* N 630 ss.

1741 Au sujet des contrats de transfert et d'échange de données techniques, ou des accords de partage de données ou *data sharing agreeements,* cf. DE WERRA, p. 367 ; JACCARD/ANCELLE, p. 4 s.

1742 JACCARD/ANCELLE, p. 2 s.

1743 Cf. *supra* N 870.

1744 Contrairement aux PME, JACCARD/ANCELLE, p. 3.

2. Les accords de confidentialité

Il est possible de prévoir au sein des contrats quels types de données peuvent être transmises et à quel cercle de destinataires. Un moyen d'y procéder est de passer par des accords de confidentialité (*non-disclosure agreements,* NDAs), permettant de définir quelles données ne doivent pas être transmises. 1011

Nous avons pu voir qu'en théorie, plusieurs obligations s'imposent aux prestataires de gestion de cyberincidents en raison du traitement de données personnelles ou soumises à un secret. Certaines données techniques peuvent également faire l'objet de clauses contractuelles distinctes afin d'assurer une utilisation conforme aux intérêts de la fournisseuse de données. La pratique contractuelle illustre la possibilité de procéder par l'adoption d'accords de confidentialité afin de soumettre la prestataire de gestion de cyberincidents ou la destinataire d'informations à ces différentes exigences. Il est courant en pratique de voir de telles clauses de confidentialité qui instaurent une forme de secrets convenus contractuellement[1745]. Ces devoirs contractuels de confidentialité prennent souvent la forme de clauses générales standardisées. 1012

Pour les secrets légaux, un accord de confidentialité n'est pas nécessaire, mais la pratique encourage la conclusion de tels accords pour clarifier la situation entre les parties contractantes. La loi primant le contrat, l'accord de confidentialité ne soumettant pas une prestataire de gestion de cyberincidents à la confidentialité pour des secrets légalement prévus n'a pas d'effet. La prestataire demeure soumise au secret légal. À l'inverse, le secret de fabrication ou d'affaire devrait faire l'objet d'une clause contractuelle entre une cliente et sa prestataire, afin d'éviter de devoir interpréter les circonstances concrètes du contrat, dans la mesure où il faut que cette dernière puisse savoir qu'elle traite des données soumises au secret[1746]. Partant, cet accord nous semble nécessaire en pratique, du moins quand des données soumises à cette forme de secret sont en jeu. 1013

3. L'utilisation du Traffic Light Protocol

Il existe plusieurs types de classifications utilisées en pratique. Une classification qui s'est imposée dans le contexte international et qui sert au partage 1014

1745 EPINEY/FASNACHT, N 45 et 47 ; MEYER/MÉTILLE, *Computer security incident response teams : are they legally regulated ? The Swiss example*, 2022, p. 50. MELANI utilisait déjà ce type d'accord avec les organisations adhérentes, cf. OFPP, *Protection de la population 27,* 2017, p. 11. À ce sujet, cf. notamment VOYAME, p. 342 s.

1746 Sur ces secrets, cf. *supra* N 957 ss. À noter que, contrairement aux violations relatives aux secrets légaux auxquelles la loi attache des sanctions, la responsabilité en cas de violation d'un secret conventionnel doit être analysée sous l'angle des violations contractuelles, cf. EPINEY/FASNACHT, N 48.

d'informations est le *Traffic Light Protocol* (TLP). Il s'y est notamment imposé pour les échanges entre prestataires de gestion de cyberincidents[1747]. Il est décrit par FIRST comme un schéma intuitif et simple pour indiquer quand et comment des informations sensibles peuvent être partagées en vue de faciliter la collaboration entre différentes actrices[1748]. En d'autres termes, le TLP permet d'assortir les échanges d'informations de prescriptions spécifiant à qui les informations doivent, peuvent ou non être transmises (par exemple si une information peut être librement accessible, si elle ne peut être transmise qu'à un secteur spécifique et ainsi de suite)[1749]. Les CSIRT utilisent largement cette classification (c. 9 Directive SRI2). À noter toutefois que ce n'est pas une solution universelle applicable à tous les échanges d'informations et ce n'est pas un schéma contraignant[1750].

1015 Le TLP s'articule autour de quatre couleurs. La couleur rouge (TLP : RED) implique que l'information transmise ne peut être divulguée à aucune autre personne individuelle externe à l'échange originaire, sous peine d'impacter la réputation, les opérations ou la sphère privée d'une personne. La couleur ambre (TLP : AMBER) est utilisée lorsque les membres de l'organisation dont fait partie la destinataire ainsi que ses clientes peuvent se voir communiquer les informations échangées. Les IOC transmis à la CSIRT d'une organisation portent typiquement l'apposition de ce code couleur, dans la mesure où ils doivent tout à fait pouvoir être transmis par la CSIRT au SOC de la même organisation. La couleur verte (TLP : GREEN) implique que les informations communiquées peuvent être échangées avec les organisations et les pairs de la communauté ou du secteur, mais non par des canaux publiquement accessibles, à l'inverse de la couleur blanche (TLP : CLEAR) selon laquelle les informations, n'engendrant pas ou peu de risque de mauvaise utilisation, peuvent être révélées sans restriction[1751]. Comme exemple pour la classification TLP : GREEN, l'on pourrait citer la communication d'une analyse d'un logiciel malveillant avec un secteur industriel spécifique.

1016 Contrairement aux classifications légales, le TLP n'a aucune valeur légale ni ne présente de lien avec des classifications légales. Partant, il ne doit pas être appliqué conjointement ou de la même façon que les classifications

1747 Il est même préconisé par l'OFCS concernant les échanges d'informations communiquées à ce dernier par les autorités et organisations enregistrées sur les systèmes d'informations de l'office, cf. OFCS, *Commentaire concernant l'OCyS*, 2024, p. 20.

1748 FIRST, *Traffic Light Protocol*, version 2.0, 2022, p. 1.

1749 FF 2017 2765, p. 2873 ; MEYER/MÉTILLE, *Computer security incident response teams : are they legally regulated ? The Swiss example*, 2022, p. 50.

1750 FIRST, *Traffic Light Protocol*, version 2.0, 2022, p. 1.

1751 FIRST, *Traffic Light Protocol*, version 2.0, 2022, p. 3 s.

prévues légalement, car cela conduirait vraisemblablement à une confusion et au risque de divulgation illicite d'informations. Il convient de garder à l'esprit que les classifications légales priment le TLP. L'utilisation du TLP peut en revanche servir d'indice pour illustrer un potentiel secret d'affaires. Finalement, il est possible de coupler l'utilisation du TLP avec l'utilisation d'autres règles par la fournisseuse de données, à l'instar de la *Chatham House Rule,* selon laquelle la source de l'information ne doit pas être divulguée[1752].

C. Une synthèse

Beaucoup d'éléments relatifs à l'activité des prestataires de gestion de cyber- 1017
incidents sont laissés à la pratique. La loi et la volonté des différentes personnes physiques et morales dans ce contexte impliquent que des arrangements doivent être convenus entre cocontractantes. C'est particulièrement vrai concernant les échanges d'informations centraux à la pratique.

Par conséquent, les personnes actives dans le contexte de la gestion de 1018
cyberincidents développent des pratiques pour assurer la confiance entre intervenantes et le traitement d'information conforme à la volonté des parties et à la loi.

De nombreux contrats prévoient aujourd'hui des éléments tels que le 1019
périmètre des informations auxquelles une cocontractante peut accéder. Les accords de confidentialité sont particulièrement utilisés pour que les parties à un échange d'information ou à un contrat plus élaboré puissent s'assurer que les informations ne sont pas communiquées de façon contraire à la volonté des partenaires. Finalement, des schémas sont utilisés par une multitude d'expertes de cybersécurité, par exemple pour préciser les personnes physiques, même au sein d'une même entreprise, qui sont autorisées par l'émettrice d'informations à accéder à celles-ci. Ce type de schéma permet de renforcer la confiance entre les intervenantes.

Des outils pratiques existent. Les conséquences liées à la violation des 1020
obligations contractuelles diffèrent des conséquences liées à la violation d'obligations légales. Dans la mesure où la loi n'est pas toujours claire et exhaustive sur les différents éléments de la pratique de gestion de cyberincidents, ces instruments et ces pratiques sont les bienvenues. La confiance qu'ils permettent entre les différentes cocontractantes est également un élément important. Leur utilité est en revanche limitée. Ces outils sont consacrés principalement aux échanges d'informations et ils ne sont pas particulièrement encadrés.

1752 Au sujet de la *Chatham House Rule* et de sa relation avec le TLP, voir notamment : FIRST, *Traffic Light Protocol,* version 2.0, 2022, p. 1 ; CHATHAM HOUSE, *Chatham House Rule*.

VI. Une conclusion au chapitre 6

1021 La gestion de cyberincidents et les prestations qu'elle implique soulèvent de nombreuses questions et mêlent de multiples domaines juridiques. La cybersécurité se recoupe avec la sécurité de l'information et est par conséquent étroitement liée à la protection de différentes informations. Alors que la notion même d'information peut être floue et regrouper différents types d'informations, certaines sont protégées dans l'ordre juridique suisse (I.A et B). Ces informations méritent une protection légale particulière (I.C). Tel est typiquement le cas des informations d'une certaine sensibilité traitées par les autorités, des données personnelles ou des informations couvertes par des secrets.

1022 La LSI pose les responsabilités pour la sécurité de l'information ainsi que des principes et obligations pour la sécurité de l'information au sein de la Confédération (II.A). Elle reprend et adapte le mécanisme de classification qui a pour principales conséquences la responsabilisation des autorités et organisations soumises à la loi et la limitation des personnes autorisées à y accéder (II.B). La LSI impose d'autres mesures contribuant conjointement à assurer la sécurité de l'information (II.C).

1023 La protection des données personnelles est réglée dans différentes lois, dont principalement la LPD sur le plan fédéral. l'OFCS et les différentes prestataires de gestion de cyberincidents sont susceptibles d'être soumises à des régimes différents à la loi et en revêtant des qualités différentes (III.A, B et C). Parmi les principes et obligations s'imposant pour garantir la protection de ces informations spécifiques, la sécurité des données est particulièrement importante et est étroitement liée à la cybersécurité, les deux domaines se recoupant (III.D). En revanche, la LPD ne vise pas la sécurité d'informations ne permettant pas d'identifier une personne physique ou de la rendre identifiable. La protection des données personnelles implique d'autres principes et obligations permettant de garantir que ces données sont traitées de façon appropriée pour la personnalité et les droits fondamentaux des personnes concernées. La loi prévoit typiquement des garde-fous en ce qui concerne la communication de données personnelles, dans un contexte où l'échange d'informations est central (III.E, F et G). Ces principes et obligations doivent être respectées sous peine d'engager différents chefs de responsabilité (III.H).

1024 Les informations couvertes par des secrets sont protégées par plusieurs dispositions légales. Les législations applicables dans ce contexte dépendent des informations et des domaines d'activité des intervenantes. Partant, différentes intervenantes dans la gestion de cyberincidents peuvent être soumises à des obligations de garder le secret sur certaines informations (IV.A et B). Les lois se rapportant aux secrets comportent principalement des aspects

protecteurs en lien avec les communications à de tierces personnes. Les personnes violant leurs obligations de garder le secret peuvent être condamnées, sous réserve d'un motif justificatif (IV.C). Les secrets incitent surtout à éviter une communication indue et ce bien que l'on puisse en déduire dans une certaine mesure une obligation de sécuriser les informations concernées. Cela étant, elles ne sont pas prévues, à l'inverse de la cybersécurité, pour protéger de façon plus large l'intégrité, la disponibilité ou la traçabilité des informations.

Des outils pratiques se développent pour appréhender les échanges d'in- 1025
formations. Ces outils servent à assurer la conformité avec les différentes lois susmentionnées, mais également à protéger d'autres informations non couvertes par la loi et à assurer la confiance entre cocontractantes (V.A). Ils sont ajoutés aux contrats pour prévoir les informations auxquelles les cocontractantes peuvent accéder et les modalités selon lesquelles elles peuvent ou non les communiquer à de tierces personnes. Des classifications largement utilisées apportent également un indicateur aux actrices de la pratique quant à la possibilité de partager plus loin ou non des informations transmises dans un contexte de cybersécurité (V.B). Ces outils ont à nouveau vocation à éviter des accès non autorisés.

La protection des informations dans le contexte de la gestion de cyber- 1026
incidents consiste en une facette importante de ces pratiques, tout en illustrant la complexité de la cybersécurité, étroitement liée à d'autres domaines juridiques plus réglementés. Ces bases légales existent en parallèle des normes de cybersécurité et couvrent des aspects se recoupant avec le domaine, mais n'en demeurent pas moins distinctes. Elles ne permettent pas d'appréhender toutes les subtilités de la cybersécurité ou de la sécurité informatique. Les instruments existant en pratique pour assurer la protection de certaines informations ont principalement vocation à assurer la confidentialité des informations partagées, mais non les autres aspects de leur sécurité. Pour ces raisons, elles ne sont pas suffisantes pour permettre de pallier un manque de réglementation en termes de cybersécurité. Bien qu'il puisse être tentant de combler des lacunes liées au manque de réglementation de la cybersécurité par différentes bases légales applicables à d'autres domaines juridiques voisins, force est de constater que certaines lacunes demeurent, malgré la diversité de bases légales existantes.

Bien que de nombreuses pratiques soient établies afin de protéger les in- 1027
formations échangées entre les différentes parties concernées par un cyberincident, ce n'est pas toujours le cas. À défaut d'information de la part de la fournisseuse de données, la prestataire de gestion de cyberincidents estime en pratique que les informations ne doivent pas être divulguées, sous réserve

du consentement de l'émettrice[1753]. Il demeure tout de même important que la personne communiquant les données prévoie une politique de catégorisation ou de classification des informations à l'interne, qui dépend de la mission et de la clientèle de la prestataire[1754]. Les solutions pratiques existant aujourd'hui permettent d'appréhender certains aspects relatifs aux communications d'informations, mais de nombreuses questions relatives plus spécifiquement à la cybersécurité restent sans réponse.

Chapitre 7 : une conclusion intermédiaire sur les lacunes observées en droit suisse

Préambule au chapitre 7

1028 Les chapitres précédents ont permis d'établir une vue d'ensemble des bases légales applicables en matière de cybersécurité en Suisse. Le cadre légal pour la gestion de cyberincidents a également fait l'objet d'une attention particulière, concrétisant des aspects centraux de la cybersécurité pour les intervenantes principales.

1029 Le chapitre 4 a tout d'abord servi à parcourir les différentes bases légales sectorielles et transversales pour la cybersécurité des infrastructures critiques en Suisse, en tenant compte des autres domaines de la protection helvétique contre les cybermenaces. Ce chapitre s'est conclu en constatant que les organisations de nombreux sous-secteurs critiques ne sont pas soumises à des exigences minimales légales de cybersécurité ou de façon inégale et non harmonisée.

1030 Le chapitre 5 a ensuite permis de conclure que les intervenantes dans la gestion de cyberincidents ne sont pas soumises à des exigences légales spéciales de cybersécurité. En revanche, certaines lois s'appliquent plus généralement à leur activité en fonction de leur clientèle et une approche *ex post*. L'OFCS se fonde en tant qu'autorité sur une base légale pour garantir le respect du principe de la légalité. Les bases légales applicables à son activité manquent en revanche de clarté.

1031 Finalement, le chapitre 6 a permis de soulever l'importance de domaines juridiques étroitement liés à la cybersécurité, surtout lorsqu'il en va de la protection de différentes informations circulant dans le cadre de la gestion de cyberincidents. Les bases légales protégeant différents types d'informations

1753 Cf. notamment WEST-BROWN et al., p. 144 s.

1754 WEST-BROWN et al., p. 143.

n'incitent les assujetties qu'à des obligations limitées et qui se recoupent seulement avec la cybersécurité. Bien que des outils pratiques se développent, ils sont aussi limités en termes de cybersécurité.

Il s'agit à présent de faire un résumé de cette vue d'ensemble. Il est important de parcourir à nouveau les bases légales existantes lorsqu'elles couvrent la cybersécurité des infrastructures critiques, les autres domaines de la protection contre les cybermenaces, la gestion de cyberincidents et les domaines juridiques connexes (I). Il est également nécessaire de retracer les principales lacunes pour analyser lesquelles doivent faire l'objet de propositions de comblement au sein de la présente étude et quelles questions doivent ici rester ouvertes (II). 1032

I. Le cadre légal existant

A. Les trois domaines de la protection contre les cybermenaces

1. La cybersécurité des infrastructures critiques

En Suisse, la réglementation de la cybersécurité est émergente. La nécessité de se concentrer aujourd'hui sur la cybersécurité des infrastructures critiques est confirmée et leur résilience constitue l'un des piliers de la cybersécurité en Suisse. La question de leur réglementation se pose et il en découle les premiers jalons d'une législation en la matière. Les efforts législatifs se divisent entre réglementations sectorielles et transversales. Les différents secteurs et sous-secteurs critiques en Suisse ne sont pas tous réglementés à un niveau similaire ou comparable. 1033

En termes stricts de cybersécurité, la révision de la LSI vise à introduire une nouvelle obligation de signaler les cyberattaques. C'est un premier pas vers une législation transversale. Elle est applicable à une multitude d'infrastructures critiques figurant dans la liste de l'art. 74*b* LSI2[1755]. Cette obligation légale constitue l'une des rares obligations transversales de cybersécurité applicables aux infrastructures critiques. 1034

Toujours plus d'exigences minimales de cybersécurité sont adoptées de façon dispersée au sein de l'ordre juridique suisse, souvent en fonction de secteurs ou sous-secteurs critiques. Les exigences peuvent être contraignantes ou non. Elles sont orientées vers les organisations actives dans certains soussecteurs critiques, en conséquence de l'autoréglementation et de l'autonomie sectorielle reconnue et souhaitée par les autorités dans le domaine de la cybersécurité. L'on peut néanmoins y percevoir certaines lacunes : les 1035

1755 Cf. *supra* N 521 ss.

réglementations sectorielles sont adoptées plus ou moins rapidement, diffèrent dans le niveau d'exigences prévu et ne concernent pas toutes les organisations actives dans les secteurs et sous-secteurs critiques.

1036 Le secteur critique des autorités, la LSI, son ordonnance et les directives du NCSC permettent d'encadrer de façon relativement complète les mesures de cybersécurité pour les autorités et les organisations des art. 2 s. LSI[1756]. Comme nous le verrons[1757], certains éléments peuvent néanmoins être mieux appréhendés par la réglementation. En revanche, les cantons sont encore loin de disposer d'un cadre équivalent, limitant souvent la législation à des questions d'organisation et de compétences, de cyberadministration ou de prestations électroniques à destination des administrées[1758]. Les autres soussecteurs critiques des autorités, comprenant les biens culturels ainsi que la recherche et l'enseignement, n'ont pas été pensés de sorte à prendre en compte la cybersécurité au niveau de la loi et soulèvent différentes questions de compétences législatives. Il n'est pas exclu que certaines directives internes aux organisations comportent des aspects de cybersécurité, mais il n'est pas certain que les organisations dans ces sous-secteurs disposent d'incitations suffisantes pour mettre en place des mesures de cybersécurité appropriées.

1037 Le secteur critique de l'énergie est également en pleine avancée législative. Le sous-secteur de l'approvisionnement en électricité est un bon exemple d'avancée avec la modification de la LApEl et de l'OApEl pour introduire des exigences minimales de cybersécurité basées sur la Norme minimale pour améliorer la résilience informatique de l'OFAE[1759]. Des développements législatifs et des évolutions externes vont possiblement être prises en compte dans différentes bases légales[1760]. Plusieurs sous-secteurs du secteur critique de l'énergie disposent par ailleurs de normes minimales pour une utilisation résiliente des TIC[1761].

1038 Dans le secteur critique des finances, certaines lois prévoient des obligations générales de gestion des risques et attribuent la compétence à la FINMA de les concrétiser. La FINMA est compétente pour adopter des circulaires et des communications à destination des organisations placées sous sa surveillance. Ces lois ne s'appliquent pas à l'ensemble des organisations actives dans le secteur critique[1762]. Il existe plusieurs obligations d'annonce dans ce secteur

1756 Cf. *supra* N 382 ss.
1757 Cf. *infra* N 1217 ss.
1758 Cf. *supra* N 394 ss.
1759 Cf. *supra* N 414 ss.
1760 Cf. *supra* N 423 ss.
1761 Cf. *supra* N 428 s.
1762 Cf. *supra* N 445 s.

critique dont la plus connue est l'obligation de signaler les cyberattaques à la FINMA en vertu de l'art. 29 al. 2 LFINMA[1763].

Le secteur critique de la santé comprend tant les soins médicaux que les prestations de laboratoire ou les produits thérapeutiques. Il compte un ensemble de compétences législatives. Les organisations de certains sous-secteurs sont soumises à des réglementations fédérales, d'autres cantonales, ce qui est susceptible de conduire à un déséquilibre entre les exigences de cybersécurité applicables aux différentes organisations[1764]. Outre les obligations d'annonce, les exigences légales générales de cybersécurité ou de sécurité des données existent pour des technologies spécifiques, à l'instar des dispositifs médicaux ou des dossiers électroniques de patientes[1765]. Certaines recommandations ont vocation à s'appliquer à divers établissements de santé et prévoient quelques exigences concrètes de cybersécurité[1766]. Il n'est en outre pas exclu que des directives internes existent, mais il n'est pas pour autant certain que les différents établissements hospitaliers, par exemple, assurent un niveau similaire de cybersécurité. 1039

Le secteur critique de l'information et de la communication englobe le sous-secteur des télécommunications, dont certaines organisations sont soumises à quelques exigences pour se protéger de certaines cyberattaques[1767]. En revanche, d'autres sous-secteurs, particulièrement critiques également, ne sont pas soumis à des réglementations similaires. Il en va ainsi pour les fournisseuses de services informatiques, qui doivent répondre à des exigences particulières en raison de leur double casquette, de la même manière que les fournisseuses de services de télécommunication[1768]. 1040

Les autorités et organisations actives dans le secteur critique de la sécurité publique, comprenant l'armée, les services d'urgence ou la protection civile, sont en partie soumises à des exigences réglementaires. En effet, l'un des sous-secteurs a pour mission d'assurer la cyberdéfense du pays. En revanche, la réglementation n'est pas complète pour tous les sous-secteurs de la sécurité publique[1769]. 1041

1763 Cf. *supra* N 447 ss.

1764 Ce qui peut poser des questions lorsque l'on voit les disparités au niveau des réglementations cantonales existant déjà pour les cantons.

1765 Cf. *supra* N 455 ss.

1766 Cf. *supra* N 463 ss.

1767 Cf. *supra* N 493 ss.

1768 Pour une analyse critique du cadre légal applicable aux fournisseuses de services informatiques, cf. *supra* N 482 ss.

1769 Cf. *supra* N 511 ss.

1042 Certains autres secteurs sont soumis à des lois prévoyant des aspects de sécurité. Ces lois ne prévoient pas expressément des considérations de cybersécurité. Il en va de la sorte pour les secteurs critiques de l'élimination, des transports ou de l'alimentation. Ces secteurs critiques disposent en parallèle des normes minimales non contraignantes permettant de guider les organisations dans la mise en œuvre de mesures pour assurer la résilience des systèmes informatiques qu'elles exploitent[1770].

2. La cybercriminalité et la cyberdéfense

1043 Les deux autres domaines de la protection contre les cybermenaces sont aussi réglementés. Le domaine de la cybercriminalité est couvert par les bases légales applicables à la criminalité en général, avec en outre des normes plus spécifiquement dirigées vers la cybercriminalité et sa poursuite[1771]. Les bases légales pour la cybercriminalité ne sont pas exhaustives et certains points méritent encore d'être réglés. Par ailleurs, il faut admettre que le droit national n'a pas pour mission de régler toutes les questions ayant trait aux composantes internationales de bon nombre de cas de cybercriminalité.

1044 En ce qui concerne la cyberdéfense, les autorités législatives manifestent une volonté de se doter des bases légales nécessaires. Le domaine est déjà réglementé et la loi évolue, principalement en ce qui concerne la défense de la Suisse par l'armée et l'extension des capacités d'action d'autorités telles que le SRC[1772].

B. La gestion de cyberincidents

1045 Lorsque l'accent est mis sur les compétences des intervenantes dans la gestion de cyberincidents, la législation fait une distinction entre les prestataires privées de gestion de cyberincidents, les prestataires publiques et l'OFCS. L'activité des prestataires de gestion de cyberincidents autres que l'OFCS n'est pas régie par des dispositions légales particulières en matière de cybersécurité. En revanche, certaines dispositions légales prévoient quelques aspects de leur pratique, en raison de leur statut d'infrastructure critique ou en fonction des prestations qu'elles fournissent[1773]. Les fournisseuses internes à certaines infrastructures critiques, notamment étatiques, doivent se conformer aux exigences potentiellement imposées à l'organisation au sein de laquelle elles

1770 Cf. *supra* N 510 et 516.

1771 Cf. *supra* N 548 ss.

1772 Cf. *supra* N 592 ss.

1773 Cf. *supra* N 619 ss.

œuvrent. Les prestataires externes peuvent être indirectement liées par les exigences légales de cybersécurité auxquelles leur clientèle est soumise et les contrats les liant à leurs clientes peuvent leur imposer différentes obligations[1774]. La loi peut servir à engager leur responsabilité de façon réactive en fonction de leurs agissements[1775].

L'OFCS exploite l'équipe nationale de gestion de cyberincidents et détient à ce titre un statut et des compétences spéciales. L'art. 15*a* Org-DDPS définit les grandes lignes des compétences de l'OFCS mais c'est surtout la LSI2 qui sert de cadre légal à son activité quant à la cybersécurité des infrastructures critiques. La LSI pose dans sa version révisée les fondements légaux pour l'activité de l'OFCS avec, à ses art. 73*a* ss, les compétences du NCSC devenu OFCS. L'organisation de la Confédération pour la cybersécurité est en pleine évolution, de la même manière que la sécurité de l'information au sein de la Confédération[1776]. 1046

C. Les autres domaines juridiques

La cybersécurité est étroitement liée à la sécurité de l'information et, plus largement, à la protection des informations. Certaines informations méritent une protection particulière octroyée par la loi en raison de leur sensibilité ou des enjeux qui les entourent. C'est notamment le cas pour les informations traitées par la Confédération, pour les données personnelles ou pour les informations couvertes par des secrets. La LSI prévoit un catalogue de mesures permettant de sécuriser les informations traitées par les autorités et les organisations de la Confédération[1777]. La LPD (et les autres lois de protection des données personnelles) appréhende des aspects de sécurité susceptibles de s'imbriquer en partie avec la cybersécurité[1778]. Les bases légales protégeant les informations couvertes par des secrets prévoient des garde-fous relatifs au traitement, mais surtout à la communication de certaines informations[1779]. 1047

De telles législations ne permettent en revanche pas d'appréhender toute la cybersécurité. En effet, il s'agit de considérations limitées à certaines informations, à certaines exigences et elles ne se recoupent qu'en partie avec la cybersécurité. Ces bases légales sont nécessaires, mais elles ne permettent pas de pallier l'absence d'une législation en matière de cybersécurité. 1048

1774 Elles sont soumises au droit du contrat applicable en cas de relation entre cocontractantes privées, ou aux règles des marchés publics lorsqu'elles servent des autorités.

1775 Ce qui n'est pas propre aux équipes de gestion de cyberincidents.

1776 Cf. *supra* N 700 ss.

1777 Cf. *supra* N 830 ss.

1778 Cf. *supra* N 844 ss, en particulier N 873 ss.

1779 Cf *supra* N 952 ss.

D. En résumé

1049 Quelques bases légales ont récemment été adoptées ou sont en voie de modification pour imposer des exigences minimales de cybersécurité à certaines infrastructures critiques. Le niveau d'exigences dépend des infrastructures critiques et de leur activité. L'adoption par le pouvoir législatif de nouvelles obligations transversales de cybersécurité laisse aussi présager une réglementation plus adéquate.

1050 La gestion de cyberincidents ne fait pas l'objet d'une réglementation légale. En revanche, quelques dispositions permettent indirectement de soumettre les prestataires de gestion de cyberincidents à des exigences de cybersécurité sujette à interprétation. L'OFCS, en tant qu'autorité fédérale, voit son activité réglée dans la loi, mais son rôle et son mandat peuvent être questionnés dans le contexte actuel de réorganisation au sein de la Confédération et de révision du cadre légal.

1051 La protection de certaines informations implique des obligations connexes à la cybersécurité. En revanche, les domaines juridiques concernés se recoupent seulement avec la cybersécurité, raison pour laquelle la loi est incomplète.

II. Les questions et les lacunes légales

A. Les lacunes et les questions traitées

1. La cybersécurité des infrastructures critiques

1052 Les infrastructures critiques ne sont dans l'ensemble pas soumises à des exigences suffisantes et harmonisées de cybersécurité. Il peut être délicat de disposer d'un cadre légal suffisant dans la mesure où la définition même d'infrastructure critique n'est pas claire dans la loi à l'heure actuelle. Sur cette base et en raison de la disparité des bases légales et réglementaires, de nombreux secteurs et soussecteurs critiques ne disposent pas d'une législation appropriée pour la cybersécurité. La réglementation n'est généralement pas exhaustive et se limite parfois à des normes non contraignantes.

1053 Plusieurs sous-secteurs critiques ne disposent pas d'exigences minimales de cybersécurité. L'exemple le plus frappant est celui des services informatiques, particulièrement importants dans une perspective de cybersécurité. En outre, de nombreuses infrastructures critiques comptent uniquement sur des recommandations dispersées, applicables seulement à une partie d'organisations actives dans un soussecteur critique et limitées en termes d'exigences concrètes. Par exemple, les autorités cantonales et communales dépendent de la réglementation cantonale, ainsi que des conventions conclues

entre les cantons et les communes. Partant, un important décalage entre les incitations réglementaires et le niveau de cybersécurité en résultant est à déplorer. Par ailleurs, les organisations actives dans le secteur de la santé ne sont pas toutes soumises à des exigences, dont la majorité n'est pas contraignante ou s'applique à un cercle d'organisations limité aux membres d'une association professionnelle. Une telle pratique réglementaire engendre à nouveau un important décalage entre les différents établissements de santé. Un autre exemple est celui des fournisseuses de services de télécommunication, dont la majeure partie n'est pas soumise à des exigences de cybersécurité. L'OST limite les quelques exigences de cybersécurité qu'elle prévoit aux fournisseuses d'accès à Internet et contient un catalogue d'exigences limitées. Le reste des incitations réglementaire pour le sous-secteur demeure opaque. De nombreuses infrastructures critiques sont soumises à des exigences fragmentées, figurant dans une diversité d'instruments adoptés par des autorités et par des associations professionnelles, souvent mal coordonnés[1780]. Résultent de ces différents exemples un réel flou juridique ainsi que de réelles lacunes légales.

Dans la mesure où des normes supplémentaires doivent être adoptées, il est nécessaire d'examiner les possibilités de réglementation pour permettre aux infrastructures critiques d'assurer un niveau adéquat de cybersécurité. Dans la mesure où le niveau de maturité des réglementations dépend largement des sous-secteurs critiques, il faut se demander si tous les secteurs critiques devraient être couverts par des exigences légales. Une réflexion quant au cercle d'organisations soumises à de potentielles exigences de cybersécurité doit être menée : est-ce que seules les infrastructures critiques particulièrement importantes sur le plan national devraient être soumises à ces exigences ou est-ce qu'un cercle plus étendu d'organisations doit être soumis à certaines obligations ? Finalement, la question du contenu des exigences minimales doit être analysée, de même que les mécanismes de mise en œuvre de la réglementation. 1054

Le souhait d'une réglementation plus claire en matière de cybersécurité et pour certains aspects de la gestion de cyberincidents est partagé au sein de la communauté d'infrastructures critiques[1781]. La loi ne doit pas être trop précise pour laisser la place à l'innovation et aux évolutions[1782]. Il faut en outre 1055

1780 L'OFCS a par ailleurs récemment relevé le flou juridique dans le domaine de la cybersécurité et a estimé que le manque de coordination entre les instruments des autorités et ceux du domaine privé était problématique, cf. OFCS, *Stratégie de l'OFCS*, 2023, p. 3.

1781 KNIEPS et al., p. 23.

1782 JAQUIER, p. 225.

que la loi serve d'incitation pour améliorer la résilience des infrastructures critiques sans tomber dans la surréglementation.

2. L'activité des prestataires de gestion de cyberincidents

1056 Le manque de réglementation du sous-secteur critique des services informatiques est particulièrement choquant en raison de l'importance pratique de celui-ci, principalement s'agissant des fabricantes de matériel et de logiciels informatiques, ou de prestataires de sécurité informatique. Ces prestataires doivent assurer la cybersécurité de leur infrastructure informatique et de leurs prestations.

1057 La gestion de cyberincidents n'est pas une question spécifiquement traitée auprès des infrastructures critiques. Les réglementations la prévoyant, contraignantes ou non, sont particulièrement rares en Suisse. Les questions relatives à l'établissement, aux compétences ou à l'activité des prestataires de gestion de cyberincidents le sont encore moins. L'absence de réglementation pour ces questions pose des problèmes. Outre le fait que les infrastructures critiques doivent détenir des compétences de gestion de cyberincidents (en leur sein ou en externalisant), les prestataires de gestion de cyberincidents sont des infrastructures critiques et des prestataires particulièrement importantes pour l'ensemble des infrastructures critiques et pour la société ; c'est pourquoi elles doivent être soumises à des exigences minimales légales de cybersécurité. Ces prestataires peuvent revêtir plusieurs formes : elles peuvent être internes à une organisation ou elles peuvent être des prestataires externes offrant régulièrement leurs services à une clientèle[1783]. Il convient d'examiner si la forme de la personne physique ou morale détenant les compétences peut être laissée à la discrétion des parties comme c'est le cas aujourd'hui, afin de permettre une plus grande flexibilité et une marge d'appréciation aux infrastructures critiques, ou si des impératifs pratiques ont pour conséquence que la profession doit être réglementée.

1058 L'activité de l'OFCS est réglementée au sein des bases légales récemment adoptées. Il est néanmoins important d'analyser comment le mandat de l'OFCS peut être renforcé et mieux encadré par la loi.

B. Les lacunes et les questions laissées ouvertes

1. Quelques exemples de questions juridiques

1059 La cybersécurité fait partie des trois domaines composant la protection de la Suisse contre les cybermenaces. La cybercriminalité et la cyberdéfense ne

1783 Cf. *supra* N 272 ss.

vont pas faire l'objet de propositions de réglementation dans le cadre de la présente étude. Ces deux domaines peuvent néanmoins être à l'origine de questions[1784]. À titre d'exemple, le droit pénal matériel existant permet une application aux actes pénalement répréhensibles perpétrés dans le cyberespace, mais quelques comportements peuvent toujours être commis dans une sorte d'impunité. On peut à ce titre déplorer l'inexistence d'infractions de *phishing* ou de recel de données. En parallèle, certaines infractions réalisées dans le cyberespace ne sont poursuivies que sur plainte, ce qui est problématique pour que les autorités compétentes puissent ouvrir une procédure pénale.

D'autres barrières techniques existent en rapport avec la loi, par exemple 1060
s'agissant des limites des recherches en *Open Source Intelligence* (OSINT). Certaines difficultés peuvent également être soulevées par le caractère international de bon nombre d'infractions à caractère informatique, ce qui implique une obligation pour les États de respecter le principe de territorialité et de ne pas intervenir sur le territoire d'un État tiers sans son consentement et sans le respect de certaines exigences légales. Les domaines de la cybercriminalité et de la cyberdéfense ont été brièvement parcourus lors de l'analyse du cadre légal, mais les questions et lacunes spécifiques de ces domaines ne seront pas approfondies dans le cadre de la présente étude.

La présente étude cherche à proposer des solutions permettant de com- 1061
bler de manière satisfaisante et globale les lacunes en matière de cybersécurité des infrastructures critiques en Suisse. Partant, si d'autres problématiques plus sectorielles doivent être relevées, notamment relatives à la réglementation sur le plan technique de technologies spécifiques, il se peut que la présente étude n'y réponde pas ou du moins pas totalement.

En parallèle, certaines réglementations dispersées couvraient quelques 1062
aspects ayant trait à la cybersécurité, comme en matière de protection des données personnelles. Différents débats concernent la législation de protection de données personnelles et différentes controverses portent sur les secrets consacrés en droit suisse[1785]. Ces questions ne seront pas approfondies dans le cadre de la présente étude.

2. Les autres lacunes et questionnements

De nombreux problèmes n'ont ni leur origine ni leur réponse dans la régle- 1063
mentation. La cybersécurité doit être appréhendée de façon holistique. Les stratégies nationales et régionales ainsi que différentes directives sont émises

1784 Pour un bref examen des bases légales applicables, cf. *supra* N 548 ss.

1785 Par exemple relativement aux transferts de données personnelles aux USA, cf. *supra* N 906 et références citées ; sur les controverses relatives à la violation du secret de fabrication, cf. *supra* N 984 et références citées.

par des entités compétentes pour surveiller et accompagner différentes tranches de la population et de l'économie. La sensibilisation, les mesures d'ordre technique et organisationnel sont aussi nécessaires pour le domaine dans sa globalité. Par conséquent, il est nécessaire de voir que tant des lacunes que de potentielles solutions n'ont pas trait à la réglementation.

1064 Les questionnements et lacunes étudiées dans la présente étude ne permettent pas en tant que telles de pallier les problématiques pratiques ou techniques, ayant trait par exemple aux difficultés techniques de tracer certaines informations, de collecter ou d'exploiter techniquement des traces numériques. D'autres questions, notamment en lien avec les ressources, l'organisation ou les différences culturelles entre les régions du pays se posent également et sont exclues de la présente étude.

1065 Des questions pratiques liées aux ressources doivent se poser, en relation avec l'implémentation d'une réglementation, la mise en place de mesures ou encore l'élaboration de cultures d'entreprise efficaces pour la cybersécurité. Ces questions échappent à l'objectif poursuivi par la présente étude, à savoir l'élaboration d'un cadre légal de cybersécurité pour les infrastructures critiques.

C. En résumé

1066 Les lacunes principales et pertinentes dans le cadre de la présente étude portent sur les exigences légales de cybersécurité pour les infrastructures critiques et pour la cybersécurité des prestataires de gestion de cyberincidents.

1067 En ce qui concerne la cybersécurité des infrastructures critiques, il est délicat de comprendre quelles organisations précises sont considérées comme des infrastructures critiques en Suisse. Le fait que la notion même d'infrastructure critique ne soit pas claire pose des problèmes dans l'imposition d'exigences minimales. Par ailleurs, certaines infrastructures critiques ne sont pas soumises à des exigences de cybersécurité, à des obligations insuffisantes pour assurer un niveau adéquat de cybersécurité ou à des exigences opaques et dispersées. Ces raisons impliquent la nécessité d'adopter des exigences minimales légales de cybersécurité pour les infrastructures critiques.

1068 La gestion de cyberincidents doit également faire l'objet d'une réglementation, dans la mesure où nous sommes quasiment confrontées à un désert juridique dans ce domaine. La cybersécurité au sein des fournisseuses de services informatiques, dont font partie les prestataires de gestion de cyberincidents, doit être assurée. Leurs prestations doivent également être encadrées. En outre, les pouvoirs de l'OFCS qui l'abrite peuvent être renforcés et clarifiés.

En dehors de ces questions qui soulèvent une réflexion en profondeur et centrale à la cybersécurité des infrastructures critiques, d'autres lacunes et questionnements demeurent. Ils ne sont pas approfondis dans le cadre de la présente étude. Les questions laissées ouvertes ont trait à la lutte contre la cybercriminalité, à la cyberdéfense ou encore aux domaines connexes à la cybersécurité, à l'instar de la protection des données personnelles ou des secrets. 1069

III. Une conclusion au chapitre 7

Certaines bases légales existent en droit suisse pour appréhender certains aspects de la cybersécurité. Des exigences minimales légales de cybersécurité pour certaines infrastructures critiques ont récemment été adoptées ou sont en voie de l'être. Les principales intervenantes dans la gestion de cyberincidents sont également soumises à quelques obligations découlant des circonstances concrètes variant d'une prestataire à une autre (I.A et B). Il existe également un cadre légal encadrant la lutte contre la cybercriminalité et la cyberdéfense (I.C). 1070

Cela étant, la réglementation du domaine n'est pas complète, des lacunes existent et la loi et la réglementation doivent être plus largement exploitées à titre d'incitation pour améliorer la cybersécurité des infrastructures critiques en Suisse. Les lacunes observées ont trait au manque de clarté autour des infrastructures critiques, au manque d'harmonisation entre les exigences légales de cybersécurité applicables aux infrastructures critiques, à l'absence d'exigences légales applicables en particulier aux prestataires de gestion de cyberincidents et à une réglementation insuffisante pour appréhender au mieux le rôle que peut occuper l'OFCS (II.A). D'autres lacunes et questionnements se posent dans des domaines connexes et sortent du cadre de la présente étude (II.B). 1071

Les prochains chapitres vont servir à analyser différents axes de réglementation pour permettre à cette dernière de servir plus adéquatement d'incitation pour un niveau plus élevé de cybersécurité des infrastructures critiques en Suisse. Il s'agira également d'examiner comment les compétences et les prestations de gestion de cyberincidents peuvent être mieux appréhendées par la loi, en tenant compte de la diversité d'actrices concernées par la cybersécurité. 1072

Troisième Partie :
les pistes réglementaires

Chapitre 8 : la nécessité de développer la réglementation

Préambule au chapitre 8

Le chapitre 7 a exposé les principales lacunes identifiées dans cette étude. Plus précisément, il a permis de délimiter les problèmes et les lacunes auxquelles cette troisième partie cherchera à remédier. Ces principaux problèmes portent d'une part sur le déficit de cybersécurité des infrastructures critiques et d'autre part du manque de clarté et de niveau de cybersécurité des prestataires de gestion de cyberincidents. 1073

Premièrement, la notion d'infrastructure critique n'est pas claire. Deuxièmement, certaines organisations considérées comme des infrastructures critiques ne sont pas soumises à des exigences minimales de cybersécurité ou sont soumises à des exigences ou des recommandations insuffisantes. Troisièmement, les exigences étant largement dispersées, il est difficile pour les infrastructures critiques de s'y conformer. 1074

Les prestataires de gestion de cyberincidents doivent être distinguées entre l'Office fédéral de la cybersécurité (OFCS) et les fournisseuses internes et externes de prestations de gestion de cyberincidents. Les prestataires privées de gestion de cyberincidents ne sont pas soumises à des exigences minimales de cybersécurité et ne sont pas obligées d'assurer leur cybersécurité et celle de leurs prestations, sous réserve d'interprétations larges des obligations légales ou de circonstances particulières ayant trait à leurs prestations ou à leur clientèle. Les fournisseuses internes de prestations sont soumises à des exigences de cybersécurité lorsque l'autorité ou l'organisation à laquelle elles sont intégrées est elle-même soumise à des exigences. L'OFCS fonde son activité sur la Loi sur la sécurité de l'information (LSI) et ses ordonnances, mais le cadre légal et son mandat peuvent être améliorés. 1075

La réglementation doit être utilisée[1786] pour pallier les lacunes soulevées et pour améliorer le niveau de cybersécurité des différentes intervenantes. La réglementation fait partie des leviers d'action pour améliorer la cybersécurité, surtout lorsqu'il en va d'autorités et d'organisations telles que des infrastructures critiques (I.A). La réglementation de la cybersécurité doit naturellement répondre et tenir compte de différents enjeux (I.B). La réglementation étudiée par la présente étude ne peut pas porter sur l'ensemble des problématiques liées à la cybersécurité et se limite ainsi aux lacunes susmentionnées (I.C). 1076

1786 Sur la notion de réglementation comprenant la notion de législation, cf. *supra* N 357.

1077 Des pistes réglementaires doivent être examinées pour chercher à combler, dans la mesure du possible, les lacunes observées (II.A). Premièrement, la troisième partie de la présente recherche étudie des pistes de réflexion pour que la loi incite correctement les infrastructures critiques à améliorer leur cybersécurité. Le Conseil fédéral (CF) a estimé dans la Cyberstratégie nationale (CSN) de 2023 que les besoins réglementaires devaient être étudiés en continu et que les lacunes observées devaient le cas échéant être comblées. Nous verrons qu'une alternative à la direction prise par la CSN est à notre avis préférable (I.B). La réglementation doit également contribuer à clarifier et à améliorer la cybersécurité des prestations fournies par les prestataires de gestion de cyberincidents. La réglementation finalement sert aussi à donner davantage de sens aux tâches de l'OFCS (II.B).

I. Les contours

A. L'origine du besoin de réglementer

1078 La cybersécurité auprès des infrastructures critiques en Suisse doit être réglementée pour combler les lacunes identifiées. L'importance factuelle de la cybersécurité est indéniable pour répondre à l'augmentation des cyberattaques et leurs potentielles conséquences dévastatrices. Entre attaques malveillantes, vulnérabilités et erreurs humaines, la cybersécurité doit être implémentée à tous les échelons et par tous les moyens nécessaires pour prévenir, anticiper, détecter les cybermenaces et y réagir.

1079 La nécessité d'agir et d'encadrer ces pratiques est admise par les autorités suisses et supranationales[1787]. L'autonomie des différents secteurs est privilégiée par la Confédération qui confère une portée particulièrement importante à la responsabilité propre, à la subsidiarité de l'intervention étatique et au fédéralisme dans le contexte de la réglementation de la cybersécurité des infrastructures critiques. Bien que le principe de subsidiarité doive être appliqué et respecté, il est regrettable qu'aucune loi n'impose de telles normes à l'ensemble des infrastructures critiques, ce qui affaiblit leur protection[1788].

1080 Certains secteurs critiques adoptent progressivement certaines exigences de cybersécurité, contraignantes ou non[1789]. D'autres secteurs examinent actuellement cette possibilité. Néanmoins, des lacunes légales sont à déplorer,

1787 CF, *CSN*, 2023, p. 21.

1788 Dans un sens similaire, ChF, *Rapport « Suisse 2035, les grands défis de demain en 20 questions »*, 2022, p. 115.

1789 Cf. *supra* N 1033 ss pour un résumé des réglementations adoptées.

que l'on regarde la cybersécurité dans les différents secteurs critiques ou plus précisément la gestion de cyberincidents, l'un des points centraux du domaine. C'est pourquoi des besoins réglementaires se font présentement sentir.

B. Un rappel des enjeux pour développer la réglementation

Les enjeux majeurs en matière de cybersécurité ont déjà été parcourus[1790]. Il va de soi qu'ils exercent une influence sur la réglementation de la cybersécurité. Une telle réglementation doit tenir compte de l'importance des informations et de leur sécurité. À la croisée de la sécurité de l'information et de la sécurité informatique, elle doit également prendre en considération la sécurité des moyens informatiques. Bien que des questions de terminologie puissent se poser, la législation pour la cybersécurité doit englober la sécurité des informations traitées par des moyens informatiques et celle des systèmes informatiques[1791]. Ces différents domaines se recoupant, les exigences de cybersécurité peuvent servir également à la sécurité de l'information ou à la sécurité informatique. 1081

La cybersécurité doit toujours être envisagée dans une approche holistique et les mesures issues de la catégorie réglementaire doivent être considérées comme faisant partie d'un ensemble de mesures pour assurer la cybersécurité, notamment auprès des infrastructures critiques[1792]. 1082

La réglementation de domaines transversaux tels que la cybersécurité soulève systématiquement plusieurs questions relatives à certains enjeux. La loi doit refléter le fait que la cybersécurité s'applique de façon transversale à différents secteurs spécifiquement réglementés. L'intervention étatique et en particulier l'intervention de la Confédération comme autorité réglementaire doit être limitée de sorte à respecter le fédéralisme et à privilégier l'autoréglementation. L'intervention limitée de la Confédération doit permettre aux autorités et organisations cantonales ou sectorielles de conserver leurs compétences et leur autonomie. 1083

Le droit n'avance pas aussi rapidement que la technologie. Partant, il faut que la réglementation de la cybersécurité applicable aux infrastructures critiques puisse évoluer rapidement, s'adapter aux évolutions technologiques et prendre facilement en considération les nouvelles technologies et les nouvelles menaces pouvant rapidement apparaître. La réglementation de la 1084

1790 Cf. *supra* N 117 ss.

1791 Cf. *supra* N 48.

1792 GCSCC, *Cybersecurity capacity review – Switzerland*, 2020, p. 7 ; OFPP, *Protection de la population 27*, 2017, p. 14.

cybersécurité doit trouver un équilibre entre clarté juridique et adaptabilité face à la rapidité de ces évolutions.

1085 La prise en compte du déficit de législation en matière de cybersécurité auprès des infrastructures critiques permet de proposer également des solutions concernant la gestion de cyberincidents en droit suisse. La résilience des infrastructures critiques revêt une importance capitale pour la protection de la Suisse contre les cybermenaces. Cependant, compte tenu de la diversité des questions soulevées dans le domaine de la cybersécurité, il est envisageable que ces aspects juridiques aient une portée plus large, notamment en ce qui concerne la protection des PME, de la population et ainsi de suite.

C. La limite des propositions

1086 Cette étude n'a pas vocation à analyser les propositions susceptibles de régler tous les problèmes et questions touchant de près ou de loin la protection de la Suisse contre les cybermenaces ou même de cybersécurité.

1087 L'objectif n'est pas de résoudre les questions relatives à la lutte contre la cybercriminalité ou la cyberdéfense, bien que certaines propositions puissent contribuer à une amélioration de la situation dans ces domaines. À titre d'exemple, les problèmes liés à la collecte des preuves numériques en procédure pénale seront laissés à l'analyse d'autres études, de même que l'impact pour la Suisse de réglementations et initiatives européennes ou internationales[1793].

1088 En outre et comme susmentionné, la présente étude se limite à la cybersécurité auprès des infrastructures critiques et aux prestataires de gestion de cyberincidents. En conséquence, les questions relatives à certains phénomènes particuliers (comme les rançongiciels), à d'autres pratiques spécifiques (comme la cyberassurance) ou à d'autres actrices (comme les PME ou la population) ne seront pas abordées en priorité.

D. En résumé

1089 L'importance de la cybersécurité est indéniable et la réglementation constitue l'un des leviers d'action à mobiliser pour l'assurer. La réglementation permet dans ce contexte d'inciter les actrices de la pratique à mettre en place

1793 Voir par exemple ENISA, *Roadmap on the cooperation between CSIRT and LE*, 2019, p. 66 ss ; voir également la proposition de règlement du Parlement européen relatif à l'échange automatisé de données dans le cadre de la coopération policière (« Prüm II »), du 8 décembre 2021 ; au sujet de la Directive ePrivacy voir EUROPOL, *Internet Organised Crime Threat Assessment IOCTA 2021*, 2021, p. 28 et 39 s.

des processus appropriés et d'encadrer ces derniers. Le développement d'un cadre réglementaire pour la cybersécurité se justifie en particulier pour les infrastructures critiques dès lors que les risques qui y sont associés sont importants pour la société. Il est nécessaire de poursuivre ce développement.

La réglementation doit tenir compte d'une diversité d'enjeux et chercher 1090
à les satisfaire. Il en va typiquement de la sorte pour la sécurité des informations traitées par le biais de moyens informatiques ou de la sécurité informatique. La réglementation de la cybersécurité doit également tenir compte des outils extralégaux complémentaires permettant par la même occasion d'éviter la surréglementation. Les évolutions technologiques et leur rapidité doivent également faire l'objet de réflexions durant le processus réglementaire.

De nombreuses questions de cybersécurité peuvent faire l'objet de ré- 1091
flexions avec à leur terme une réglementation. Cela étant, des questions plus précises et s'éloignant du cadre central de cette recherche ne seront pas étudiées. Il en va typiquement des questions légales ayant trait aux paiements de rançongiciels ou à l'encadrement légal des cyberassurances.

II. Des hypothèses légales

A. Les angles d'approche

La présente étude émet des propositions tendant à combler les lacunes légales 1092
et réglementaires identifiées en termes de cybersécurité auprès des infrastructures critiques d'une part et au sein de l'activité des prestataires de gestion de cyberincidents d'autres part. Plusieurs hypothèses peuvent être proposées ; chaque hypothèse s'accompagne d'avantages et de défis.

L'objectif est de présenter différentes alternatives en questionnant leur 1093
bien-fondé. Les questions portent également sur la possibilité, voire la nécessité, de combiner différentes hypothèses pour parvenir au cadre réglementaire le plus efficient. L'implémentation de telles propositions doit être cohérente dans l'ordre juridique et elle doit appréhender les différents enjeux gravitant dans le domaine. Les propositions à examiner doivent contribuer à l'amélioration de la résilience des infrastructures critiques, en leur permettant de gérer au mieux les cyberincidents pouvant les impacter.

Les infrastructures critiques sont les premières responsables de leur 1094
cybersécurité. Partant, elles fondent le point de départ pour la réglementation de leur cybersécurité. Elles doivent être assujetties à des exigences minimales de cybersécurité pour être incitées à améliorer leur résilience.

Toutes les personnes concernées par la cybersécurité des infrastructures 1095
critiques doivent être responsabilisées. Cela implique que les prestataires de

cybersécurité et de gestion de cyberincidents doivent également faire l'objet d'incitations réglementaires pour apporter un soutien sécurisé aux infrastructures critiques. Cela implique également la mobilisation des ressources des autorités compétentes pour le soutien des infrastructures critiques, principalement GovCERT et l'OFCS.

1096 Finalement, la présente étude permet d'examiner comment les propositions formulées permettent d'appréhender certaines questions actuelles spécifiques et comment elles s'imbriqueraient avec d'autres réglementations dans des domaines connexes.

B. La responsabilisation des infrastructures critiques comme point de départ

1097 Le premier groupe de propositions a comme point d'ancrage les infrastructures critiques. L'objectif est d'examiner s'il est possible d'inciter les infrastructures critiques à augmenter leur cyberrésilience par la réglementation. Cette solution tient son origine dans le principe selon lequel chaque personne est responsable d'elle-même. Les infrastructures critiques exploitent des systèmes informatiques et utilisent ces systèmes pour traiter des informations et assurer les prestations qu'elles fournissent. Elles doivent être soumises à des incitations réglementaires pour garantir la cybersécurité en général, comme dans leurs prestations, leurs comportements d'achats et l'exploitation de systèmes informatiques leur permettant de traiter des informations dans le cadre de leurs prestations. Ces organisations sont particulièrement essentielles au fonctionnement de l'économie nationale ou au bien-être de la population[1794].

1098 La proposition réglementaire de la CSN consiste à maintenir une sorte de *statu quo,* à savoir en se contentant des réglementations actuellement en place et en développant la réglementation de façon dispersée lorsqu'un examen des besoins réglementaires conduit à la conclusion que des normes doivent être modifiées ou adoptées. Cette variante implique l'examen systématique de tous les besoins et de toutes les lacunes réglementaires[1795]. Comme nous le verrons[1796], cette option peut être problématique à plusieurs égards.

1099 Par conséquent, une alternative sera plus approfondie. Elle consiste en l'introduction d'exigences légales minimales de cybersécurité pour les infrastructures critiques[1797]. Il s'agit ici de déterminer quelle législation centralisée

1794 Dans un ordre d'idées similaire, cf. SALAMON, p. 79.

1795 CF, *CSN*, 2023, p. 21.

1796 Cf. *infra* N 1141 ss.

1797 Cf. *infra* N 1145 ss.

devrait être applicable à quel cercle d'infrastructures critiques et comment le cadre légal et le de droit souple peuvent et doivent coexister afin d'optimiser la mise en œuvre de la loi par les organisations concernées.

C. La réglementation des prestataires de soutien

Les prestataires de gestion de cyberincidents ne sont pas soumises à des exi- 1100
gences légales minimales de cybersécurité en droit suisse en tant que fournisseuses de services informatiques ou en tant que prestataires de sécurité Elles sont soumises à diverses réglementations, dispersées selon les activités qu'elles fournissent, la relation à leurs clientes, les informations qu'elles traitent ou encore leur caractère privé ou public[1798]. Les prestataires de gestion de cyberincidents peuvent agir, comme nous l'avons vu, à titre public comme à titre privé. Partant, une législation unique n'est *de facto* pas envisageable.

La pratique des prestataires de gestion de cyberincidents soulève des 1101
questions supplémentaires en comparaison avec les autres infrastructures critiques. En effet, non seulement la cybersécurité de leur infrastructure doit garantir un niveau approprié de cybersécurité, mais également leurs prestations. Il convient d'examiner si une réglementation applicable à l'ensemble des organisations actives dans le sous-secteur critique des services informatiques est envisageable, dans la mesure où les différentes organisations actives dans ce sous-secteur peuvent être confrontées à des défis et des enjeux de cybersécurité similaires. Cette réglementation permettrait d'introduire des exigences légales supplémentaires pour ces organisations. En outre, il convient de se demander si des exigences supplémentaires devraient être introduites et, si oui, lesquelles[1799]. Un cadre légal proactif s'appuyant sur une approche *ex ante* est préférable à ce qui existe actuellement entre les réglementations contractuelles, sectorielles ou spécifiques.

L'OFCS, comme son équipe d'intervention nationale et gouvernemen- 1102
tale, agit principalement sur la base de la LSI et de ses ordonnances. Au vu de sa position, il est judicieux d'examiner d'autres compétences qui devraient être légalement attribuées à l'OFCS. Un développement des bases légales en vigueur permettrait d'attribuer à l'OFCS de plus amples compétences en termes de soutien, de réglementation et de surveillance lorsqu'il en va de la cybersécurité des infrastructures critiques[1800].

1798 Cf. *supra* en particulier N 619 ss.

1799 Cf. *infra* notamment N 1301.

1800 Cf. *infra* N 1396 ss.

D. En résumé

1103 La première piste réglementaire analysée porte sur la responsabilité des infrastructures critiques pour leur cybersécurité. Elles sont les premières responsables de leur cybersécurité et elles doivent être soumises à des exigences proactives permettant de mieux appréhender les mesures qu'elles doivent mettre en place. Les hypothèses analysées dans ce cadre sont au nombre de deux. La première hypothèse est celle proposée dans la CSN de 2023. Elle implique l'examen en continu des besoins réglementaires et le comblement des lacunes observées le cas échéant. La seconde hypothèse consiste à introduire des exigences minimales légales de cybersécurité pour les infrastructures critiques.

1104 La seconde piste réglementaire porte sur l'activité des prestataires de gestion de cyberincidents. Concrètement, il s'agit d'analyser une possibilité d'introduire des exigences de cybersécurité applicables notamment aux prestataires de gestion de cyberincidents comme fournisseuses de services informatiques. L'examen doit aussi porter sur l'utilisation de la loi peut renforcer et améliorer le rôle de l'OFCS.

III. Une conclusion au chapitre 8

1105 La cybersécurité est centrale pour la société et la réglementation est nécessaire pour l'appréhender (I.A). Cette conclusion est admise en Suisse et sur le plan international. La réglementation permet de satisfaire certains enjeux de cybersécurité et elle permet d'inciter des assujetties à disposer de pratiques de cybersécurité et d'encadrer celles-ci (I.B). La réglementation de la cybersécurité doit être limitée (I.C). Elle s'articule principalement autour de la cybersécurité des infrastructures critiques et de la responsabilité des prestataires de gestion de cyberincidents.

1106 Premièrement et comme annoncé, l'introduction d'exigences minimales légales de cybersécurité est analysée selon deux alternatives (II.A). La première alternative est celle de continuer à réglementer de façon dispersée en analysant en continu les lacunes légales et en comblant peu à peu ces dernières. La seconde alternative étudiée est l'adoption d'exigences minimales transversales dans une loi centralisée ayant vocation à s'appliquer à un ensemble d'infrastructures critiques.

1107 Deuxièmement, des propositions législatives seront faites pour que la loi puisse mieux être utilisée comme incitation et comme cadre aux professions liées à la gestion de cyberincidents dans une perspective de cybersécurité.

L'OFCS, en tant qu'actrice étatique spécifique dans ce contexte, peut également bénéficier d'améliorations législatives (II.B).

Chapitre 9 : la réglementation de la cybersécurité des infrastructures critiques

Préambule au chapitre 9

Des bases légales pour la cybersécurité des infrastructures critiques sont en voie de développement en Suisse. Comme les lacunes observées permettent de l'illustrer, la réglementation est insuffisante et doit être plus étoffée. Deux pistes réglementaires principales sont à examiner. 1108

La première est celle préconisée dans la CSN (I.A). Elle consiste en l'examen systématique des besoins réglementaires pour adopter les normes nécessaires. Elle s'inscrit dans l'adoption en cours de normes servant à imposer des exigences minimales à des cercles d'infrastructures critiques (I.B). Cette première piste doit prendre en compte les lacunes précédemment identifiées pour adopter de nouvelles bases légales et de nouvelles normes (I.C et D). Comme nous le verrons, cette option permet de poursuivre l'élaboration d'un cadre réglementaire selon ce qui est en train d'être fait, tout en respectant l'autonomie sectorielle et le rôle subsidiaire de l'État et de la Confédération dans la réglementation de la cybersécurité pour les infrastructures critiques. En revanche, cette alternative peut soulever des questions de facilité, de durée et de cohérence (I.E). 1109

La seconde piste réglementaire consiste en l'introduction d'exigences minimales légales applicables aux infrastructures critiques (II.A). Cette alternative suppose l'adoption d'une base légale centralisée qui prévoit des exigences minimales à un cercle étendu d'infrastructures critiques. Une réglementation centralisée suppose la compétence législative de la Confédération (II.B). Elle peut être suivie tout en respectant l'autonomie sectorielle et le principe de subsidiarité. La LSI sert de base légale adéquate pour introduire de telles exigences (II.C). Le catalogue de mesures prévu par la loi sert de base appropriée, bien que quelques précisions puissent être amenées (II.D). Il est important dans cette seconde approche de mobiliser les ressources des autorités compétentes pour que la loi puisse être mise en œuvre par les organisations assujetties. Cette alternative est préférable à celle suivie par la CSN en raison de la nécessité d'adopter un cadre légal transversal, de la facilité légistique qu'une telle piste implique et pour des raisons de cohérence. Elle permettrait d'atteindre un niveau supérieur et harmonisé de cyberrésilience des infrastructures critiques en Suisse (II.E). 1110

I. La réglementation ponctuelle

A. L'alternative de la Cyberstratégie nationale

1111 La réglementation de la cybersécurité est actuellement en développement, de façon plus ou moins générale et pour des cercles définis d'organisations. La réglementation se développe de façon disparate et les besoins réglementaires sont évalués par secteur, par technologie ou par question spécifique. Le CF préconise cette orientation dans la CSN 2023. La CSN prévoit qu'« il convient d'examiner en tout temps où il serait nécessaire de mettre en place des bases légales »[1801].

1112 C'est pour cette raison principalement qu'il convient d'analyser dans la présente étude les questions qui se poseraient avec l'implémentation d'une telle variante. Il convient d'en comprendre les avantages et les inconvénients. Il est effectivement important de parcourir la variante choisie par les autorités avant d'examiner si une autre solution, peut-être plus complète et globale, est préférable.

B. Un résumé de la réglementation existante

1. Les bases légales

1113 Certains sous-secteurs critiques se dotent de bases légales pour appréhender la cybersécurité. Il en va de la sorte pour l'administration fédérale par le biais des art. 6 ss LSI, pour l'approvisionnement en électricité avec l'art. 8*a* de la Loi fédérale sur l'approvisionnement en électricité (LApEl) et l'art. 5*a* de l'Ordonnance sur l'approvisionnement en électricité révisée (OApEl). Il en va de la sorte également pour les fournisseuses d'accès à Internet conformément à l'art. 96*a* l'Ordonnance sur les services de télécommunication (OST) ou comme on peut le voir à l'art. 74 de l'Ordonnance sur les dispositifs médicaux (ODim), qui prévoit expressément que la cybersécurité doit être assurée par les établissements de santé pour protéger les dispositifs connectés à des réseaux[1802]. Ces dispositions illustrent des exemples de sous-secteurs critiques pour lesquels les autorités compétentes ont admis une nécessité de légiférer. Les secteurs et sous-secteurs critiques concernés sont l'énergie, de la santé, les services financiers ou encore l'information et de la communication[1803].

1801 CF, *CSN*, 2023, p. 21.

1802 Cf. *supra* N 382 ss, 414 ss, 455 ss et 495 ss. D'autres bases légales prévoient des considérations de cybersécurité à l'instar de l'art. 29 al. 2 LFINMA, qui implique une obligation d'annonce de cyberattaques à la FINMA, cf. *supra* N 447.

1803 Cf. *supra* N 1033 ss ; Interpellation 22.3749 « Faut-il différencier entre les secteurs économiques sous l'angle des exigences en matière de cybersécurité » déposée le 16 juin 2022 par Gherard Andrey, Avis du CF du 24.08.2022.

Pour le reste des sous-secteurs critiques, la législation suisse a été en grande partie adoptée avant que des considérations technologiques soient prises en compte. Il n'est pas exclu que certaines lois et ordonnances en vigueur visant la sécurité puissent s'appliquer de manière analogique à la cybersécurité, mais nous ne saurions en tirer une conclusion généralisée[1804]. Les bases légales pertinentes n'ont pas été adoptées en vue de s'appliquer expressément à la cybersécurité, ce qui peut soulever certaines questions de prévisibilité du droit pour les assujetties, ainsi que certaines questions relatives à l'adéquation des dispositions applicables à des considérations de cybersécurité. 1114

2. Les réglementations non contraignantes

L'État encourage l'industrie à s'auto-réglementer, ce qui transparaît dans certains secteurs et sous-secteurs critiques[1805]. Les organisations actives dans l'approvisionnement économique du pays peuvent aujourd'hui s'appuyer d'une part sur la norme minimale pour améliorer la résilience informatique adoptée par l'Office fédéral pour l'approvisionnement économique du pays (OFAE). Elles peuvent d'autre part s'appuyer sur des normes plus spécifiques selon qu'elles fournissent des prestations dans l'élimination des déchets, dans les eaux usées, dans les transports publics, ou dans l'approvisionnement en électricité, en eau, en denrées alimentaires, en chauffage et froid à distance ou en gaz. 1115

Certains autres secteurs et sous-secteurs critiques comptent également sur des réglementations non contraignantes permettant de les guider dans la sécurité des informations que les exploitantes traitent et dans la sécurité de leurs systèmes informatiques. Tel est le cas pour certaines organisations du secteur critique de la santé qui disposent de recommandations de différentes autorités et organisations professionnelles[1806]. 1116

C. L'évolution à venir

1. La nécessité de se pencher sur toutes les infrastructures critiques

Certains secteurs et sous-secteurs critiques disposent déjà d'une réglementation plus ou moins contraignante incitant les organisations assujetties à atteindre un certain niveau de cybersécurité. Les normes applicables ont pour conséquence la mise en place auprès d'infrastructures critiques de mesures permettant d'assurer quelques aspects de la cybersécurité et de la gestion 1117

1804 Cf. à titre exemplatif *supra* N 434 ss pour le secteur critique de l'élimination.

1805 Sur l'incitation par l'État à l'auto-réglementation, voir FLÜCKIGER, p. 359 ss.

1806 Cf. *supra* N 463 ss.

des cyberincidents qui les affectent. Les cercles d'assujetties et les exigences prévues par les différents instruments sont généralement limitées. Il est donc important de se demander si ces instruments devraient être adaptés en fonction d'un cercle plus large d'organisations, si les exigences devraient être développées et si ces instruments devraient revêtir un caractère contraignant. En outre, ces instruments doivent s'adapter aux évolutions à venir.

1118 De nombreux secteurs et sous-secteurs critiques n'ont pas introduit d'exigences minimales, ce qui implique un déficit d'incitation réglementaire pour que bon nombre d'infrastructures critiques gèrent mieux leur cybersécurité et les cyberincidents qui les affectent. Cette solution n'est de loin pas optimale, dans la mesure où certaines infrastructures critiques n'ont pas implémenté de mesures suffisantes, ce qui peut avoir d'importantes répercussions lors de la survenance de cyberincidents.

1119 En raison du manque de clarté quant à la définition d'infrastructure critique, de la diversité et de la dispersion des normes, il peut être difficile pour les organisations de savoir si elles sont critiques ou non, si elles sont assujetties à des exigences de cybersécurité et, le cas échéant, auxquelles. Partant, la loi doit revêtir un niveau accru de clarté.

2. Les changements en cours

1120 La réglementation de la cybersécurité au sein des secteurs et sous-secteurs critiques est en cours de développement de manière fragmentée. L'approche de la CSN conserve cette logique, en prévoyant de déterminer en tout temps où il serait nécessaire de mettre en place des bases légales[1807]. Il convient, selon cette approche, d'examiner constamment les besoins et la réglementation de tous les secteurs et sous-secteurs critiques afin de savoir exactement quelles lacunes sont à déplorer et quelles normes supplémentaires devraient être adoptées. Il est dans cette optique important d'examiner en tout temps également les technologies et questions qui devraient être réglementées[1808].

1121 C'est dans cet ordre d'idées que la législation pour la cybersécurité dans l'approvisionnement en électricité est en cours de révision[1809]. En outre, l'Office fédéral de la communication (OFCOM) réfléchit aux exigences s'imposant dans le contexte de l'informatique en nuage[1810]. Il convient d'attendre de voir les secteurs ou technologies dont les autorités vont ensuite examiner

1807 CF, *CSN*, 2023, p. 21. La CSN 2023 est appelée à être réexaminée en 2028, soit 5 ans après sa publication, CF, *CSN*, 2023, p. 35.

1808 CF, *CSN*, 2023, p. 21.

1809 Cf. *supra* N 417 ss.

1810 CF, *CSN*, 2023, p. 21.

les lacunes. L'on peut espérer que les besoins de certains sous-secteurs soient rapidement examinés[1811].

D. La mise en œuvre

1. La nécessité pour les secteurs de définir les champs d'application

Il est important que le cercle d'assujetties aux différentes exigences minimales de cybersécurité soit clairement identifiable. Il n'existe aujourd'hui pas de définition uniforme de la notion d'infrastructure critique. À ce sujet, la variante de la réglementation sectorielle poursuivie par le CF ouvre deux possibilités. Premièrement, il est possible de laisser la question de la définition d'infrastructure critique ouverte et de laisser aux différents secteurs et sous-secteurs critiques le soin de définir quelles organisations sont soumises aux exigences sectorielles ou sous-sectorielles. Deuxièmement, il est envisageable de se baser sur une définition centrale de la notion d'infrastructure critique[1812], tout en laissant le soin aux entités sectoriellement compétentes de définir si toutes les infrastructures leur étant soumises devraient mettre en place des mesures minimales de cybersécurité selon la réglementation applicable. 1122

Il semble en tout cas cohérent de laisser aux organismes sectoriels compétents le soin de définir le cercle d'organisations soumises aux exigences minimales sectorielles de cybersécurité. En effet, les autorités compétentes et associations professionnelles sectorielles sont plus à même de connaître les organisations devant implémenter diverses mesures de cybersécurité en leur sein. Elles connaissent par ailleurs les spécificités techniques auxquelles sont confrontées les organisations leur étant soumises. 1123

Bien qu'en pratique cette variante revête un intérêt certain et une logique certaine, nous pourrions nous poser la question générale du bien-fondé à ne pas disposer d'une définition plus claire de la notion d'infrastructure critique en Suisse. Dans la mesure où les exigences sont sectorielles dans l'approche suivie par la CSN, il n'est pas nécessaire de réfléchir à une définition plus claire de la notion d'infrastructure critique[1813]. Il est surtout important que les 1124

1811 Par exemple pour le sous-secteur critique des services informatiques suite aux différentes cyberattaques ayant ciblé des prestataires informatiques pour la Confédération, dans la mesure où une enquête administrative est en cours, cf. OFCS, *Rapport concernant les analyses de données effectuées après la cyberattaque contre l'entreprise Xplain,* 2024, p. 3 ; NCSC, *Cyberattaque contre l'entreprise Concevis: l'administration fédérale est également concernée*.

1812 Il s'agit ici de se demander si une définition plus claire que celle de l'art. 5 litt. c LSI serait préférable, cf. *supra* N 74.

1813 Pour une proposition de définition légale d'infrastructure critique, cf. *infra* N 1211.

exigences sectorielles et sous-sectorielles s'appliquent à des cercles définis d'infrastructures critiques et que les autorités compétentes s'assurent que toutes les organisations devant être soumises aux exigences le soient effectivement.

1125 Indépendamment de la notion d'infrastructure critique choisie, il est important de laisser la liberté pour les différents secteurs et sous-secteurs critiques de décider qui sont les assujetties des différentes exigences de cybersécurité, tout en gardant à l'esprit que l'objectif est que les infrastructures critiques soient soumises à des exigences minimales permettant un niveau satisfaisant de cyberrésilience compte tenu de leur niveau de criticité, de leur taille et d'autres facteurs similaires.

1126 Mieux définir la notion d'infrastructures critiques revêt une logique juridique et politique. En revanche, une telle définition constitue une ingérence dans les compétences des organisations sectorielles. L'importance de la définition d'infrastructure critique dans le présent contexte vise surtout le champ d'application des différentes exigences sectorielles introduites. Selon cette approche, il n'est pas forcément nécessaire de clarifier la notion d'infrastructure critique pour que les bases légales prévoient le cercle d'organisations assujetties. Chaque base légale a en effet son champ d'application, raison pour laquelle la définition de la notion d'infrastructure critique n'a pas besoin d'être tranchée à ce stade et il est important surtout que les normes sectorielles prévoient un champ d'application défini.

2. Les exigences minimales

1127 Les secteurs et sous-secteurs critiques sont par essence différents. Ce constat implique qu'ils ne nécessitent pas forcément le même niveau de réglementation ou les mêmes spécificités au niveau réglementaire. Il faut d'abord analyser la criticité et la vulnérabilité d'un sous-secteur. Dans le cadre de cette analyse, il faut également tenir compte de la dépendance des infrastructures critiques concernées vis-à-vis des différentes ressources, de même que celles d'autres groupes cibles sur ces infrastructures analysées[1814]. Il faut en outre comprendre la structure des différents secteurs et sous-secteurs critiques, à savoir si les actrices actives dans le sous-secteur peuvent se soutenir mutuellement, s'il existe une seule organisation fournissant les prestations principales ou si plusieurs organisations se partagent les prestations offertes, ou encore comment la répartition géographique est faite au sein du sous-secteur[1815].

1814 OFPP, *Protection de la population 27,* 2017, p. 15.

1815 Par exemple, le sous-secteur critique des télécommunications compte quelques organisations principales, cf. OFPP, *Beschreibung der Teilsektoren Kritischer Infrastrukturen in der Schweiz – Telekommunikation,* 2010, p. 1. Le sous-secteur de l'approvisionnement

Il faut ensuite s'assurer des besoins permettant d'assurer la cybersécurité qui nécessitent d'être appréhendés par la réglementation, en portant une attention particulière sur les mesures techniques et opérationnelles, les technologies[1816], les équipements[1817] et les prestations et services de cybersécurité[1818]. Il est possible de s'appuyer, pour réglementer les différents sous-secteurs, sur les bases légales et normes existantes pour certains soussecteurs déjà réglementés, tout en réfléchissant aux enjeux et défis spécifiques à chaque nouveau sous-secteur à réglementer. Les réglementations doivent en effet être spécifiques, mais peuvent s'inspirer, voire renvoyer, à d'autres bases légales (comme prévu à l'art. 2 al. 5 *in fine* LSI2)[1819]. La suite de la présente étude montrera le type d'exigences minimales qui seraient pertinentes pour l'ensemble des infrastructures critiques, dans la mesure où certaines exigences minimales peuvent être imposées à aux infrastructures critiques de façon transversale[1820], alors que certaines mesures devraient être spécifiques à certaines organisations. L'examen de solutions réglementaires spécifiques pour chaque sous-secteur dépasse le champ de la présente étude[1821]. 1128

La réglementation des différents sous-secteurs n'étant pas toujours contraignante, les autorités réglementaires compétentes doivent systématiquement réfléchir à la forme de la réglementation à adopter pour que celle-ci puisse constituer une incitation appropriée. 1129

3. Le contrôle de la conformité aux réglementations

Dans la mesure où la réglementation se fait sectoriellement, la question du contrôle de la conformité aux exigences sectorielles se pose. Il faut savoir qui surveille le respect des obligations prévues sectoriellement et par quels mécanismes. 1130

en électricité inclut quelques organisations majeures et une série d'organisations plus ou moins importantes régionalement, cf. OFPP, *Factsheet zum kritischen Teilsektor Stromversorgung*, 2012, p. 1.

1816 Les technologies regroupent typiquement la cryptographie, les technologies permettant les transmissions sur réseau ou les technologies de stockage, de traitement, d'analyse de données ou de cybermenaces, SALAMON, p. 196.

1817 Dont les équipements permettant la transmission sur le réseau, l'accès physique, les fonctions d'authentification ou encore les équipements industriels (dont les capteurs), les pare-feux ou les produits de détection de cyberattaques, SALAMON, p. 196 s.

1818 SALAMON, p. 196 s.

1819 FF 2017 2765, p. 2825.

1820 Cf. *infra* N 1217 ss.

1821 Pour un résumé empreint d'exemples de lacunes observées, cf. *supra* N 1052 ss. Par ailleurs, le contenu d'exigences minimales transversales étant analysé ci-après, il peut servir d'inspiration pour divers sous-secteurs critiques.

1131 Dans une optique sectorielle, cette responsabilité peut logiquement être confiée à des autorités de surveillance sectorielles, qui connaissent les spécificités des organisations sur qui elles disposent déjà d'une certaine autorité et avec qui une collaboration existe déjà.

1132 Il est toutefois nécessaire de disposer de mécanismes de coopération entre les autorités de surveillance et l'OFCS. En effet, bien que les autorités de surveillance sectorielles connaissent les spécificités ayant trait aux différents secteurs et sous-secteurs, l'OFCS détient des connaissances plus étendues en matière de cybersécurité, raison pour laquelle il doit, d'une façon ou d'une autre, être impliqué dans les échanges avec les autorités de surveillance. Ce mécanisme doit être soutenu par l'introduction de la base légale suffisante. La LSI sert de fondement pour l'activité de l'OFCS et doit constituer la base légale pour ces échanges.

1133 Le rôle d'autorité d'application de la loi ne doit pas revenir à l'OFCS dans l'hypothèse de la réglementation ponctuelle. L'OFCS est l'autorité principale pour la cybersécurité en Suisse et détient à ce titre les connaissances de cybersécurité pour veiller à ce que les différentes organisations respectent les exigences minimales auxquelles elles sont soumises. Malgré tout, il n'a pas connaissance de l'ensemble des spécificités sectorielles. Si les réglementations sont uniquement sectorielles, il deviendrait complexe d'attendre la surveillance d'une autorité qui n'est pas davantage impliquée en amont dans le processus réglementaire[1822]. Il serait donc nécessaire d'impliquer l'OFCS dans le processus réglementaire de toutes les bases légales adoptées[1823].

1134 Les mécanismes de contrôle que les autorités peuvent utiliser ou, en d'autres termes, leurs compétences en tant qu'autorités d'application de la loi, doivent être décidés. Par exemple, si certaines bases légales attribuent à une autorité de surveillance des compétences d'enquête ou des compétences relatives à la réception d'annonce ou à la reconnaissance de certifications, les bases légales doivent les prévoir. Les éventuelles sanctions en cas de non-respect des exigences de cybersécurité doivent également figurer dans les lois.

1822 D'autres autorités de surveillance ne disposent pas de connaissances sectorielles, à l'instar de la PFPDT, mais celles-ci veillent généralement au respect par les assujetties d'une ou de plusieurs lois centrales et non pas à une multitude de lois exclusivement sectorielles.

1823 L'art. 10 P-OCyS prévoit justement que l'OFCS soutient les autorités fédérales et cantonales dans le développement ainsi que dans la mise en œuvre des réglementations de cybersécurité, ce qui risque d'entraîner une charge importante de travail pour l'office fédéral.

E. Une conclusion

1. En résumé

L'examen et l'adoption de réglementations ponctuelles composent une méthode cohérente avec l'approche du CF dans la CSN de 2023. En outre, la réglementation par comblement des lacunes ponctuelles est reconnue par les autorités dans différents sous-secteurs et a déjà débuté, par l'ajout de bases légales supplémentaires ou de normes non contraignantes dans certains sous-secteurs critiques. 1135

Les besoins réglementaires doivent être constamment évalués, en gardant à l'esprit que l'introduction d'exigences minimales de cybersécurité devient pressante pour certains sous-secteurs actuellement sous-réglementés. 1136

Les exigences concrètes à adopter dépendent des sous-secteurs et des organisations concernées, et de leurs spécificités. Le caractère contraignant ou non contraignant doit également être décidé, notamment en fonction de l'incitation souhaitée. Les autorités et mécanismes de contrôle d'application des réglementations doivent également être décidés. 1137

2. Les avantages

Cette approche permet d'éviter une ingérence importante dans l'autoréglementation favorisée jusqu'à présent. Les entités sectoriellement compétentes étant en principe impliquées dans les processus de réglementation, une autonomie sectorielle est garantie[1824]. Il en va de même pour le fédéralisme, dans la mesure où chaque canton demeure compétent pour adopter les bases légales applicables aux organisations soumises à la compétence législative cantonale[1825]. L'autonomie sectorielle et le fédéralisme sont primordiaux pour la réglementation de secteurs et sous-secteurs critiques. 1138

Les spécificités de chaque secteur et sous-secteur sont prises en compte dans la mesure où l'ensemble de la réglementation n'est pas unifié. Les secteurs et sous-secteurs peuvent par ce biais adopter des réglementations adaptées à leurs besoins, à leurs technologies et à leur importance pratique. 1139

L'ordre juridique suisse conserve par cette approche une certaine cohérence et continue de se développer comme la Confédération le souhaite, à savoir en examinant où, sectoriellement, les besoins de réglementation résident[1826]. 1140

1824 OFPP, *Protection de la population 27*, 2017, p. 15. Sur la question de la compétence législative de la Confédération et de l'autoréglementation, cf. *infra* N 1168 ss.

1825 Pour une analyse de la compétence législative de la Confédération en lien avec le fédéralisme, cf. *infra* N 1149 ss.

1826 CF, *CSN*, 2023, p. 21 ; FF 2017 2765, p. 2800.

3. Les problèmes

1141 Une réglementation dispersée engendre un risque non négligeable que certaines organisations n'atteignent pas un niveau suffisant de cybersécurité. Cette piste réglementaire implique un partage complexe des compétences entre les entités compétentes sectoriellement et est déjà critiquée dans le contexte de la protection générale des infrastructures critiques en Suisse[1827]. Cette approche n'est pas optimale pour aboutir à une réglementation harmonisée. Les lacunes actuelles dans le cadre légal suisse sont trop importantes pour que l'on se limite à agir par un comblement de lacunes ponctuel. Il n'est pas exclu que des organisations actives dans un sous-secteur passent entre les mailles du filet. C'est à l'heure actuelle le cas pour les fournisseuses de services informatiques qui ne sont pas soumises à des bases légales pour leur activité, à l'inverse de nombreuses autres infrastructures critiques.

1142 En outre, le processus d'examen constant de potentielles lacunes et des besoins de chaque sous-secteur semble particulièrement long et fastidieux. À titre d'exemple, le sous-secteur critique de l'approvisionnement en électricité devrait compter une modification de la LApEl et de l'OApEl entre 2024 et 2025, alors que l'examen avait commencé avant 2021, date à laquelle l'Office fédéral de l'énergie (OFEN) avait rendu son rapport attestant d'un besoin supplémentaire de réglementer la cybersécurité dans le sous-secteur[1828]. Cet exercice serait allégé en cas d'adoption centralisée d'exigences minimales légales. Les technologies évoluant rapidement, à l'inverse des processus législatifs, raison pour laquelle cette méthode est synonyme de perte de temps et d'efficience. Il est important de garder à l'esprit la nécessité d'améliorer le niveau global de cyberrésilience actuel auprès des infrastructures critiques.

1143 Le fait que de nombreux instruments réglementaires s'appliquent aux organisations peut avoir pour conséquence que celles-ci ne savent pas à quelles exigences elles sont soumises. En d'autres termes, le manque de clarté existant à ce jour risque d'être renforcé si la réglementation continue d'être dispersée.

1144 Finalement, bien que les autorités sectorielles détiennent des connaissances sur les spécificités de leur secteur, augmenter et diversifier leurs compétences en ajoutant des compétences de cybersécurité pour contrôler la correcte application de la réglementation serait difficile à mettre en œuvre dépendant des secteurs et sous-secteurs critiques.

1827 Cf. à titre exemplatif Cff, *Audit de la protection des infrastructures critiques,* 2023, 21.

1828 Cf. *supra* N 415 ; DETEC, *Rapport explicatif concernant l'avant-projet relatif à la révision de mai 2024 de l'ordonnance sur l'approvisionnement en électricité,* 2023, p. 1 ; OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »,* 2021, p. 24 et 131.

II. La création d'une législation centralisée

A. La ratio legis

Il est maintenant établi que le niveau de résilience des infrastructures critiques en Suisse doit s'améliorer. Cette amélioration passe par en premier lieu par l'introduction d'exigences minimales de cybersécurité afin de prévenir, détecter et réagir aux cyberincidents. Une obligation de signaler les cyberattaques existe déjà aux art. 74*a* ss LSI2, mais elle n'est pas suffisante pour assurer la cybersécurité. Le cadre légal prévoit en premier lieu des obligations d'annonce. En revanche, les lois introduisant des exigences de cybersécurité sont plus rares. Elles ne se limitent pas à la communication d'informations aux autorités, mais impliquent des démarches administratives, physiques et techniques pour assurer la cybersécurité[1829]. 1145

La solution préconisée actuellement par le CF dans le cadre de la CSN est susceptible de ne pas satisfaire tous les enjeux en présence ou de surmonter tous les défis existants[1830]. Le niveau de cybersécurité assuré au sein des différents secteurs et sous-secteurs critiques est variable, ce qui implique, comme nous avons pu le voir[1831], qu'au moins une partie des infrastructures critiques ne sont pas soumises à des exigences de cybersécurité suffisantes. Cette disparité risque d'être renforcée par le développement d'une réglementation éparse malgré une possible augmentation du niveau auprès de certaines organisations[1832]. La réglementation sectorielle pose également le problème de sa rapidité d'adaptation à l'évolution des technologies. Par ailleurs, la réglementation décentralisée et fragmentée soulève des questions de lisibilité, de prévisibilité et de sécurité juridique pour les infrastructures critiques ainsi que des questions de confiance de la population, dans la mesure où il est difficile pour tous les groupes cibles de savoir exactement quel est le cadre réglementaire leur étant applicable. Finalement, la surveillance par les différentes autorités sectorielles du respect des obligations par les assujetties peut être compliquée, dans la mesure où celles-ci ne disposent pas forcément de compétences en matière de cybersécurité. 1146

1829 SOLOVE/HARTZOG, p. 47 ss.

1830 Par ailleurs, plusieurs participantes à la consultation de la révision de la LSI pour introduire une obligation de signaler les cyberattaques ont proposé l'introduction de normes minimales sur la cybersécurité des infrastructures critiques pour mieux assurer la prévention des cyberincidents, FF 2023 84, p. 12.

1831 Cf. *supra* N 1052 ss.

1832 Cf. ETHOS, *Étude Ethos – Responsabilité numérique des entreprises du SMI Expanded*, 2022, p. 19 ; ETHOS, *Étude Ethos – Responsabilité numérique des entreprises du SMI Expanded*, 2023, p. 8 et 23.

1147 Bien que chaque infrastructure critique soit confrontée à une réalité spécifique et à un niveau de criticité lui étant propre, il est pertinent d'envisager une réglementation transversale, du moins pour un premier niveau harmonisé et général d'exigences minimales pour les infrastructures critiques. Une telle réglementation permet d'une part de réduire la fragmentation actuelle des dispositions en matière de cybersécurité et d'autre part d'assurer d'un niveau minimal transversal de cybersécurité auprès de ces organisations essentielles au bien-être de la population, au fonctionnement de la société ou à l'économie nationale[1833].

1148 Si l'on se limite aux infrastructures critiques, l'unité matérielle de la loi justifie une réglementation centrale. En effet, un niveau minimal harmonisé serait naturellement bénéfique en Suisse, dans la mesure où la problématique d'exigences minimales de cybersécurité se pose en partie pour l'ensemble des infrastructures critiques ; il ne s'agit pas de problématiques isolées. À cet effet, l'introduction d'exigences minimales au sein d'une base légale harmonisée est adéquate, à condition que l'on n'empêche pas l'adoption d'exigences spécifiques supplémentaires[1834]. En effet, les disparités et les spécificités sectorielles ne peuvent pas être niées, raison pour laquelle il faut un cadre réglementaire complet.

B. La compétence législative fédérale

1. Le principe de subsidiarité

1149 Le principe de subsidiarité découle de l'art. 5*a* Constitution fédérale (Cst.). Ce principe a une portée principalement verticale et il décentralise l'exécution des tâches au niveau le plus bas possible, afin de favoriser la souveraineté des entités concernées, avec un égard quant au but recherché et à l'efficience attendue[1835]. Parmi ces tâches figure la réglementation des différents domaines incombant à l'État. La Confédération peut légiférer uniquement lorsque la Constitution lui en attribue la compétence et dans les cas où les cantons ont délégué leur compétence, ces derniers disposant des compétences résiduelles (art. 3, 5*a* et 42 ss Cst.).

1150 De manière plus horizontale et limitée, l'État doit favoriser, lorsque c'est possible, l'autoréglementation au sein des différents secteurs. La liberté éco-

1833 De la même manière que ce qui a été recherché dans l'UE avec la Directive SRI et sa seconde version la Directive SRI2, cf. c. 22 Directive SRI2.

1834 OFJ, *Guide de législation*, 2019, N 597 s. La Confédération use déjà de ce mécanisme, avec des lois telles que la LHID dans lesquelles il laisse le soin aux cantons de fixer des modalités ou prévoir des règles plus spécifiques.

1835 CR Cst.-BELLANGER, art. 5*a* N 36.

nomique implique en vertu principalement de l'art. 94 Cst. que l'économie est, dans la mesure du possible, la principale responsable pour se gérer et que l'État doit respecter et sauvegarder cette liberté économique.

2. Le respect de l'autonomie cantonale

a. Le principe de subsidiarité dans la Constitution

La répartition des tâches entre la Confédération et les cantons est centrale en Suisse. Le principe de subsidiarité (art. 5*a* Cst.) signifie à cet égard que les cantons sont souverains, sous réserve que la Constitution limite leurs compétences. En d'autres termes, ils exercent leurs compétences tant que ces dernières ne sont pas déléguées à la Confédération (art. 3 Cst.). Ils disposent d'une compétence résiduelle et la Confédération dispose *a contrario* uniquement de compétences d'attribution, lui permettant notamment de disposer de compétences de réglementation et de contrôle dans le respect du principe de subsidiarité[1836]. 1151

Les art. 42 à 135 Cst., et plus précisément les art. 42 à 43*a*, font écho à l'art. 3 Cst. et consistent en une expression du principe de subsidiarité pour la Confédération en faveur des cantons. L'art. 42 Cst. limite les tâches que la Confédération accomplit à celles fixées par la Constitution[1837]. En outre, elle n'assume que les tâches qui excèdent les possibilités des cantons ou qui nécessitent une réglementation uniforme (art. 43*a* Cst.). En d'autres termes, la Confédération ne se charge d'une tâche ou n'y prend part que si elle ne peut pas être accomplie plus efficacement par les cantons ou qu'une solution uniforme est nécessaire au niveau fédéral[1838]. 1152

b. Les normes attributives de compétence actuellement utilisées

Compte tenu de ce qui précède, reste à déterminer si la Constitution fédérale attribue la compétence à la Confédération de légiférer en matière de cybersécurité des infrastructures critiques. À défaut, il n'est pas possible d'envisager une réglementation centralisée au niveau fédéral pour tous les secteurs critiques confondus. Cette question de rapport vertical entre les communes, les cantons et la Confédération est pertinente, dans la mesure où plusieurs sous-secteurs critiques ne sont par principe pas de la compétence législative de la Confédération. Il en va typiquement de la sorte pour les sous-secteurs 1153

1836 OFJ, *Guide de législation*, 2019, N 641 s. ; BSK BV-BIAGGINI, art. 5*a* N 2 et 21 ; CR Cst.-MARTENET, art. 3 N 7.

1837 AFF, *Fédéralisme/Subsidiarité « D'où vient la Suisse ? »*, 2004, p. 2 ; OFJ, *Guide de législation*, 2019, N 634 ; CR Cst.BELLANGER, art. 42 N 3.

1838 CR Cst.-BELLANGER, art. 5*a* N 13 et 18 ; MONTAVON, p. 53.

critiques comme les établissements médico-hospitaliers cantonaux, les administrations cantonales et communales ou encore les universités et hautes écoles cantonales. Il faut s'assurer que la Confédération ne viole pas le principe de subsidiarité dans l'hypothèse où elle légifère pour imposer à l'ensemble des secteurs et soussecteurs critiques des exigences minimales de cybersécurité.

1154 Pour répondre à la question de l'existence d'un fondement constitutionnel pour la compétence législative de la Confédération, il convient de chercher si une norme constitutionnelle attributive de compétence à la Confédération existe. La LSI, source principale pour la cybersécurité à l'échelle de la Confédération et applicable en partie aux infrastructures critiques, se fonde sur les art. 54 (affaires étrangères), art. 60 (organisation, instruction et équipement de l'armée) et art. 101 s. Cst. (politique économique extérieure et approvisionnement du pays). Ces dispositions constitutionnelles ne concernent pas toutes les dispositions de la LSI pour les infrastructures critiques (cf. art. 74 ss LSI), mais leur choix se tient en raison des différentes ordonnances que reprend la LSI[1839].

1155 La Confédération ne pourrait pas adopter légalement des exigences minimales de cybersécurité pour les infrastructures critiques en se fondant sur l'art. 54 Cst., dans la mesure où les affaires étrangères concernent principalement les relations entre la Suisse et d'autres sujets de droit international, ce qui s'éloigne des exigences minimales de cybersécurité pour les infrastructures critiques en Suisse[1840]. Le problème est identique avec l'art. 101 Cst., dès lors qu'il sert uniquement à sauvegarder les intérêts des entreprises suisses à l'étranger et ne concerne pas les prestations fournies par les infrastructures critiques en Suisse, ce qui est principalement recherché par d'introduction d'exigences minimales contraignantes pour assurer la cybersécurité de ces dernières[1841]. L'art. 60 Cst. ne pourrait pas non plus servir de base pour ces compétences car cette disposition attribue des compétences à la Confédération pour l'armée. La disposition pourrait au maximum permettre l'adoption au niveau fédéral d'exigences minimales pour le sous-secteur critique de l'armée[1842].

1156 L'art. 102 Cst., relatif à l'approvisionnement du pays, est en revanche plus intéressant dans la mesure où il permet à la Confédération de prendre des mesures préventives pour assurer l'approvisionnement de la Suisse face à une menace de force ou une pénurie grave à laquelle l'économie n'est pas en

1839 Cf. à titre exemplatif l'aOPri ou l'OCSP.

1840 CR Cst.-MAROONIAN/KOLB, art. 54 N 14.

1841 CR Cst.-MAROONIAN/KOLB, art. 54 N 38 ; CR Cst.-ZIEGLER, art. 101 N 5. Il faut en effet également tenir compte des aspects internes à la Suisse.

1842 CR Cst.-LUBISHTANI, art. 60 N 11.

mesure de remédier seule. Ces mesures pourraient être applicables aux secteurs critiques faisant également partie de l'approvisionnement, à l'instar de l'énergie ou l'alimentation (cf. art. 4 de la Loi sur l'approvisionnement du pays, LAP)[1843]. En revanche, elles ne concerneraient pas l'ensemble des infrastructures critiques actives en Suisse, se limitant aux secteurs critiques présentant un lien avec l'approvisionnement du pays[1844]. Cette solution se limiterait en outre à permettre à la Confédération de réglementer la cybersécurité en cas de graves menaces.

1157 La révision de la LSI a permis à la Confédération d'utiliser ses compétences législatives pour introduire l'obligation de signalement pour les cyberattaques contre les infrastructures critiques. L'obligation de signaler les cyberattaques se fonde sur les compétences « inhérentes » de la Confédération en termes de sécurité intérieure et extérieure. La Confédération s'est appuyée pour ce faire non pas sur l'art. 57 Cst., mais sur l'art. 173 Cst., artifice permettant de justifier les compétences de la Confédération sans base constitutionnelle explicite[1845].

1158 Compte tenu des fondements constitutionnels de la LSI, il est discutable de se servir des fondements constitutionnels susmentionnés pour introduire des exigences minimales de cybersécurité applicables aux infrastructures critiques. En effet, il est impossible, selon la position défendue par la présente étude, de se limiter à ces normes attributives de compétence. Il serait en outre préférable de ne pas fonder la compétence législative de la Confédération sur un artifice de compétence inhérente. Il convient de s'arrêter sur l'art. 57 Cst., dont le titre marginal est expressément la sécurité.

c. La sécurité comme fondement constitutionnel supplémentaire

(i) La notion de sécurité et la portée de l'art. 57 Cst.

1159 La base constitutionnelle des compétences en matière de sécurité est l'art. 57 Cst., qui attribue des compétences à la Confédération et aux cantons pour les questions relatives à la sécurité du pays et à la protection de la population[1846]. L'art. 57 al. 1 Cst. dispose que la Confédération, avec les cantons, « pourvoie »

1843 BSK BV-OESCH/RUFF, art. 60 N 3 ss ; CR Cst.-ZIEGLER, art. 102 N 3 s.

1844 Des sous-secteurs critiques tels que ceux des soins médicaux, des services financiers ou encore des organisations d'urgence ne seraient typiquement pas visés. En revanche, un lien entre l'art. 102 Cst. peut être créé avec l'art. 76 Cst. pour les eaux, l'art. 91 pour le transport d'énergie ou encore avec l'art. 92 pour les services postaux et télécommunications, BSK BV-OESCH/RUFF, art. 102 N 6.

1845 FF 2023 84, p. 60.

1846 OFJ, *Guide de législation*, 2019, N 655 ; BSK BV.BIAGGINI, art. 42 N 37 et 39 ; WEBER/WILLI, p. 146.

à la sécurité du pays et à la protection de la population[1847]. L'art. 57 al. 2 Cst. prévoit que les cantons et la Confédération coordonnent leurs efforts en matière de sécurité intérieure. La sécurité est une tâche fondamentale et essentielle de l'État ; c'est à lui qu'incombe la protection des institutions, la défense de la société et des individus contre les menaces importantes[1848].

1160 La question de savoir si l'art. 57 Cst. contient à ses al. 1 ou 2 des normes attributives de compétence est débattue. Il s'agit davantage d'une norme se référant au partage de compétences d'autres dispositions constitutionnelles[1849]. La question du caractère attributif de l'art. 57 Cst. se pose principalement si l'on estime qu'une nouvelle loi doit être adoptée pour prévoir les exigences minimales de cybersécurité pour les infrastructures critiques, dans la mesure où il n'existe pas, à notre connaissance, de loi basée uniquement sur l'art. 57 Cst. La présente étude préconise en revanche la LSI comme loi pour abriter ces exigences. La loi se fonde déjà sur d'autres dispositions constitutionnelles, raison pour laquelle il n'est pas nécessaire de trancher cette controverse. L'art. 57 Cst. viendrait en soutien aux autres fondements constitutionnels, permettant une meilleure appréhension et un choix de fondements constitutionnels plus juste et complet pour l'introduction de ces exigences. Comme exemple à titre comparatif, la Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI), sur laquelle se base l'Ordonnance sur les cyberrisques (aOPCy abrogée à l'entrée en vigueur de la LSI en vertu de l'annexe 2 de l'OSI), se fonde notamment sur les art. 54 et 57 Cst.

1161 La notion de sécurité de l'art. 57 Cst. est multidimensionnelle, controversée et évolutive[1850]. La portée de la notion s'ouvre peu à peu et l'on peut se demander s'il est possible d'inclure dans la notion de sécurité de l'art. 57 Cst. la cybersécurité des infrastructures critiques. Le maintien de la sécurité du pays et de sa population doit permettre de garantir les règles fondamentales de la coexistence pacifique, protéger les institutions, défendre la société et

1847 CR Cst.-BELLANGER, art. 42 N 37. Dans le même sens, CR Cst.-BLEICKER, art. 57 N 43.

1848 OFJ, *Guide de législation*, 2019, N 640 ; BSK BV-DIGGELMANN/ALTWICKER, art. 57 N 27 ; CR Cst.-BLEICKER, art. 57 N 17 ; MOECKLI, N 8.

1849 AUBERT, MOECKLI et DIGGLEMAN/ALTWICKER notamment considèrent que l'art. 57 Cst. ne constitue pas une norme attributive de compétence et ce bien que plusieurs lois se fondent sur cette disposition constitutionnelle, PC Cst.-AUBERT, N 1 ; BSK BV-DIGGLEMAN/ALTWICKER, art. 57 N 23 ; MOECKLI, N 9. BLEICKER confère à l'art. 57 al. 1 Cst. un caractère programmatique qui signifie qu'il conduit l'autorité qui légifère, notamment sur le plan fédéral, à prendre les mesures y compris les mesures législatives pour réaliser les objectifs de sécurité du pays et de protection des personnes, CR Cst.-BLEICKER, art. 57 N 43.

1850 Sur la controverse, cf. notamment BSK BV-DIGGELMANN/ALTWICKER, art. 57 N 9 et 16 ; MOECKLI, N 1.

les individus contre les menaces élémentaires (de type terrorisme ou criminalité organisée) et empêcher les crises sociales. Les infrastructures critiques sont vulnérables et elles sont associées aux risques liés aux troubles menaçant l'ordre et la paix publiques[1851]. Au vu de l'importance de protéger les infrastructures critiques pour les objectifs de sécurité et comme l'a démontré la présente étude[1852], la réglementation de la cybersécurité de ces organisations est étroitement liée à l'objectif susmentionné malgré le manque de clarté de l'art. 57 Cst. quant aux pouvoirs de la Confédération[1853]. Le CF a par ailleurs admis en 2018 que la protection des infrastructures critiques tombait dans le mandat constitutionnel imposant à l'État d'assurer la sécurité du pays[1854]. La protection des infrastructures critiques comprend leur cybersécurité lorsqu'elles sont d'importance nationale. La notion de sécurité de l'art. 57 Cst. ne doit donc pas se limiter aux traditionnelles activités de police, de douane, de renseignement, d'armée et de protection civile[1855]. Cependant, un courant doctrinal semble soulever une limite de la sécurité à ces activités[1856].

Compte tenu des controverses au sujet de la notion même de sécurité et 1162
du caractère attributif de compétences de l'art. 57 Cst., l'on pourrait se demander si un nouveau fondement devrait être créé pour la cybersécurité hors du cadre de la défense ou de la poursuite pénale de la cybercriminalité. Une interprétation plus extensive de la notion de sécurité au sens de l'art. 57 Cst. serait plus simple. Cela étant, le CF a soulevé que la Constitution n'attribuait pas, dans le contexte des mesures de police de sécurité, la compétence à la Confédération en matière de protection de l'État, bien que la jurisprudence et la doctrine lui aient reconnu le pouvoir d'adopter, en vertu de sa compétence inhérente, des mesures lui permettant de parer aux menaces contre l'État. Il a estimé qu'il serait utile de créer une disposition constitutionnelle fondant justement le mandat de protection découlant de la compétence inhérente de la Confédération et que les limites du pouvoir de celle-ci devraient être

1851 CR Cst.-BLEICKER, art. 57 N 17 et 34. La sécurité du pays s'étend effectivement aussi aux institutions de la collectivité publique nécessaires à cette sécurité, BSK BV-DIGGELMANN/ALTWICKER, art. 57 N 14.

1852 Cf. notamment *supra* N 78 s.

1853 CR Cst.-BLEICKER, art. 57 N 36 et références citées.

1854 CF, *SNPC 2018-2022*, 2018, p. 15. Une controverse existe au sujet de la scission entre sécurité extérieure et intérieure, pour plus d'information à CR Cst.-BLEICKER, art. 57 N 37 ss.

1855 L'attribution des compétences en matière de sécurité à la Confédération concerne en effet principalement la sécurité nationale, dont fait partie la défense nationale, mais sans y être limitée, ce que l'on peut comprendre de BSK BV-DIGGELMANN/ALTWICKER, art. 57 N 25.

1856 Cf. notamment BSK BV-DIGGELMANN/ALTWICKER, art. 57 N 27 ss ; MOECKLI, N 43 ss.

définies[1857]. Le Parlement fédéral n'a pas donné suite à cette proposition d'une modification de la Constitution[1858]. La présente étude laisse ouverte la question relative à la nécessité d'une nouvelle disposition constitutionnelle (liée à la question du caractère attributif de l'art. 57 Cst.). Toutefois, l'art. 57 Cst. pourrait servir de fondement constitutionnel supplémentaire pour la loi hébergeant les exigences minimales de cybersécurité applicables aux infrastructures critiques. Si un nouveau fondement constitutionnel permettant l'adoption par la Confédération de mesures de sécurité venait à être adopté, la cybersécurité auprès des infrastructures critiques devrait être intégrée aux réflexions sur l'étendue des pouvoirs que cette nouvelle disposition attribuerait à la Confédération. En parallèle, il n'est pas exclu qu'une nouvelle disposition constitutionnelle doive être adoptée au vu des développements technologiques et de la nécessité de les réglementer. Cette question sort cependant du cadre de la présente étude.

(ii) La sécurité et la subsidiarité

1163 La nature de la distribution des compétences entre la Confédération et les cantons posée à l'art. 57 Cst. diffère selon les aspects de la sécurité concernés. La disposition n'ayant pas été adoptée avec la finalité de s'appliquer à la cybersécurité des infrastructures critiques, il faut s'assurer qu'une législation centralisée adoptée par la Confédération ne violerait par le principe de subsidiarité. Cette interprétation de la norme doit être effectuée à l'aune de l'art. 43*a* al. 1 Cst., qui consiste en une maxime institutionnelle guidant l'interprétation des normes de compétence en requérant que la Confédération exerce des tâches qui nécessitent une réglementation fédérale uniforme (ou qui excèdent les possibilités des cantons)[1859].

1164 La condition des tâches excédant les possibilités des cantons est généralement évoquée lorsque les réglementations cantonales conduisent à des situations injustes pour la population. Tel pourrait être le cas, par exemple, si un canton compétent pour réglementer un secteur ou un sous-secteur critique n'impose pas les mêmes exigences qu'un canton voisin. Bien que l'excès des possibilités des cantons soit repris dans l'exigence d'une réglementation uniforme et a donc une portée moindre, il sied de relever que la cybersécurité est

1857 FF 2012 4161, p. 4294. Position semblant être partagée par MOECKLI, N 52.

1858 BO CN 2013 891.

1859 BSK BV-BIAGGINI, art. 43 N 13. En d'autres termes, l'art. 43*a* al. 1 Cst. invite les autorités à s'interroger sur la compatibilité d'un transfert de compétence à la Confédération en vue d'obtenir la solution la plus conforme à l'exigence constitutionnelle, CR Cst.-BELLANGER, art. 43*a* N 14 et 16. Au sujet des circonstances justifiant l'attribution d'une compétence législative à la Confédération : OFJ, *Guide de législation*, 2019, N 646.

aujourd'hui globalement peu réglementée à l'échelle cantonale et qu'il peut être particulièrement difficile pour les cantons d'imposer des exigences minimales de cybersécurité à tout un cercle d'organisations entrant dans leurs compétences[1860].

1165 Dans le cas d'une réglementation fédérale en raison de la nécessité d'une réglementation uniforme au sein de la Confédération, les autorités politiques doivent évaluer si, en fonction du domaine et des buts poursuivis, un besoin d'application homogène du droit fédéral existe et justifie une réglementation uniforme ou s'il est possible de laisser aux cantons une marge de manœuvre plus étendue pour permettre une diversité[1861]. Dès lors que de nombreuses infrastructures critiques échappent à la compétence législative des cantons, il faut admettre que la cybersécurité d'organisations essentielles à la population, à la société et à l'économie nationale doit être réglementée de façon uniforme. La similitude des questions face aux cybermenaces entre les différentes organisations vient souligner cette conclusion.

1166 Que l'on cherche à justifier la compétence législative de la Confédération par la nécessité d'une réglementation fédérale uniforme ou par l'excès des possibilités des cantons, il convient d'admettre que la Confédération devrait être habilitée à exercer cette tâche sans compromettre les compétences des cantons ou le principe de subsidiarité. Il semble aujourd'hui nécessaire de prévoir une réglementation harmonisée pour l'ensemble des secteurs et pour assurer une cohésion au niveau national, ce qui d'une part justifie la réglementation fédérale uniforme et, d'autre part, excède les possibilités des cantons.

1167 Bien que la Confédération doive être habilitée à légiférer en la matière sans porter atteinte au principe de subsidiarité, il faut, pour respecter ce principe, continuer à permettre aux cantons imposant un niveau plus élevé d'exigences de faire primer leur réglementation dans leur domaine de compétence, comme cela est déjà prévu lorsque les cantons traitent des informations de la Confédération ou qu'ils utilisent ses systèmes informatiques (art. 3 al. 2 LSI)[1862]. L'existence de l'art. 57 al. 2 Cst. implique que la Confédération doit surtout créer les conditions de base favorables pour les cantons, notamment sur le plan législatif, et assurer la coordination, l'information et le soutien dans le domaine d'exécution[1863]. Cet argument plaide non pas pour une réglementation unique

1860 CR Cst.-BELLANGER, art. 43*a* N 22.

1861 CR Cst.-BELLANGER, art. 43*a* N 20. Il est important d'éviter les conflits, positifs ou négatifs de compétences intercantonales, TF, 1P.426/2003 du 21 avril 2004, c. 2.7.4 ; CR Cst.-BELLANGER, art. 43*a* N 21.

1862 FF 2017 2765, p. 2787 s.

1863 CR Cst.-BLEICKER, art. 57 N 51. En termes de coordination et de soutien, passer par des mécanismes centralisés faciliterait entre autres grandement l'échange d'information et la coopération intercantonale et intersectorielle.

et centrale, mais bien plus pour un cadre mixte, composé d'une législation centrale et d'une possible réglementation décentralisée. En effet, les cantons doivent conserver la faculté de légiférer dans les domaines soumis à leur compétence (en lien notamment avec les administrations cantonales et communales, les universités et hautes écoles, les hôpitaux cantonaux et ainsi de suite). Pour ce faire, la loi fédérale doit prévoir que ses exigences minimales ne s'appliquent pas lorsque le droit cantonal pose des exigences plus élevées.

3. Le respect d'une autonomie sectorielle ?

1168 Le principe de subsidiarité produit principalement des effets verticaux entre la Confédération, les cantons et les communes. Partant, aucun droit à l'autoréglementation ne découle de ce principe et la Constitution ne règle pas en tant que telles les relations entre l'État et les individus. Aujourd'hui, certains secteurs et sous-secteurs critiques se sont dotés de réglementations souples afin d'assurer un niveau minimal de cybersécurité. Ces pratiques n'impactent pas la compétence de la Confédération de réglementer ce domaine. Au contraire, cette dernière est légitimée à réglementer la cybersécurité auprès des infrastructures critiques en Suisse.

1169 La question de l'existence d'une dimension horizontale au principe de subsidiarité selon l'art. 5*a* Cst. est controversée[1864]. La non-intervention de l'État dans l'activité privée doit être appréciée à la lumière de l'art. 6 Cst., selon lequel chaque personne est responsable d'elle-même et de contribuer selon ses forces à l'accomplissement des tâches de l'État et de la société[1865]. La déréglementation et la privatisation sont les bienvenues dans cette perspective. En termes de réglementation, le pouvoir législatif peut associer le secteur privé à la mise en œuvre de la législation fédérale par le biais de l'autoréglementation[1866].

1170 Le principe de subsidiarité devrait inciter le pouvoir législatif à favoriser l'autoréglementation si elle peut lui aménager un espace, à condition qu'elle soit compatible avec l'intérêt public[1867]. Cela implique que lorsque la Confédération est compétente, elle doit prendre en compte les autorités et organisations impactées et les associer, dans la mesure du possible, à la réglementation de leurs secteurs et sous-secteurs. Cela permet le respect de la liberté

1864 BSK BV-BIAGGINI considère que le fait de savoir si l'État doit agir ou laisser une tâche aux individus ou à la société ne fait pas l'objet du principe de subsidiarité à l'art. 5*a* Cst., cf. BSK BV-BIAGGINI, art. 5*a* N 16. AUBERT, estime au contraire que la question de la dérégulation découle davantage de la proportionnalité de l'intervention de l'État, AUBERT, p. 5.

1865 BSK BV-BIAGGINI, art. 5*a* N 19.

1866 CR Cst.-BELLANGER, art. 5*a* N 32, 34 et 36.

1867 CR Cst.-BELLANGER, art. 5*a* N 37.

économique (art. 94 Cst.). La Confédération ne doit pas surréglementer afin de maintenir un environnement propice au secteur de l'économie privée (art. 94 al. 3 Cst.). Dans la variante d'une réglementation unique et centrale, la prise en compte des personnes impactées impliquerait typiquement leur consultation à différentes étapes du processus législatif.

1171 Le CF estime que la responsabilité de l'État de protéger les infrastructures critiques conformément à son mandat constitutionnel de garantie de la sécurité du pays est subsidiaire à celle de l'économie[1868]. L'État ne peut user de sa compétence que dans la mesure où le secteur privé n'y parvient pas. L'OFEN avait conclu à l'existence de cette situation pour l'approvisionnement en électricité. L'Office avait estimé que les organisations appliquant les normes minimales et la réglementation déléguée à l'Association des entreprises électriques suisses (AES) ne disposaient pas d'un niveau de cybersécurité rassurant, malgré la réglementation de certaines pratiques[1869]. C'est pourquoi les bases légales ont dû être révisées. Nous pouvons sans trop de risques tirer comme conclusion que les autres secteurs et sous-secteurs critiques, pour la plupart moins réglementés que l'approvisionnement en électricité, ne peuvent pas assurer l'intérêt public que représente la sécurité de leurs prestations critiques à la population et à la société.

1172 L'adoption d'exigences minimales de cybersécurité au niveau de la Confédération devrait donc être admise. Encore faut-il que les secteurs économiques demeurent en mesure d'adopter des exigences plus détaillées, plus spécifiques ou plus élevées afin de garantir le respect de l'autonomie et de la responsabilité principale du secteur économique.

C. La forme de la législation centrale

1. La nécessité de disposer d'une loi fédérale

1173 L'adoption d'une loi est nécessaire. La limitation à l'élaboration d'une ordonnance ou au recours à des instruments de droit souple n'est pas adéquate. Comme nous le verrons, la Constitution exige que les dispositions importantes fixant des règles de droit soient édictées sous la forme d'une loi fédérale (art. 164 al. 1 Cst.). Partant, la simple adoption d'une ordonnance, comme l'aOPCy, n'est pas admissible. En effet, son fondement légal était la LMSI et la loi ne

1868 CF, *CSN*, 2023, p. 12 ; CF, *SNPC 2018-2022*, 2018, p. 15. Pour un autre exemple consacré cette fois dans la loi, l'art. 102 Cst. et l'art. 3 LAP prévoient que l'approvisionnement du pays est principalement de la responsabilité du secteur économique, CR Cst.-ZIEGLER, art. 102 N 5.

1869 Cf. notamment OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »*, 2021, p. 73 ss.

prévoyait pas d'exigences minimales de cybersécurité visant les infrastructures critiques.

1174 De la même manière, la limitation à des actes non contraignants n'est pas suffisante, comme l'OFEN l'a constaté pour le sous-secteur critique de l'approvisionnement en électricité[1870]. Le niveau de cybersécurité assuré par différentes infrastructures critiques est insuffisant et il existe d'importantes disparités entre les différentes organisations. Comme cela a été analysé dans l'alternative poursuivie par la CSN[1871], agir par secteur et sous-secteur critiques ne permet que difficilement d'assurer un niveau homogène et suffisant de cybersécurité, peu importe les types d'instruments réglementaires adoptés. En outre, de nombreuses organisations ne comprennent pas les réglementations auxquelles elles sont soumises, ce qui va en faveur d'une législation centralisée pour garantir la lisibilité que l'adoption de nombreux instruments non contraignants ne semble pas permettre. Finalement, la voie que compte poursuivre le CF, visant à examiner en tout temps où il serait nécessaire de créer des bases légales, ne semble pas suffisantes au vu de la vitesse de modification des législations et du manque d'harmonisation minimale susmentionné qui en découlerait.

1175 « Toutes les dispositions importantes qui fixent des règles de droit[1872] doivent être édictées sous la forme d'une loi fédérale »[1873], comme le dicte l'art. 164 al. 1 Cst. La notion de disposition importante se rapporte notamment à l'effet juridique de la disposition sur les assujetties en termes d'états de fait visé ou de conséquences d'application. Parmi les critères permettant de qualifier une disposition d'« importante » figurent le nombre important de sujets de droit concernés, la forte influence sur les droits des personnes concernées, les conséquences financières considérables pour les individus ou encore le fait de trancher une question politique particulièrement décisive[1874].

1870 Cf. *supra* N 1171.

1871 Cf. *supra* N 1141 ss.

1872 Une règle de droit est une norme générale et abstraite, à savoir une disposition directement contraignante créant des droits, des obligations ou attribuant des compétences, s'adressant à un cercle de destinataires qui n'est pas défini de manière précise et visant un nombre indéterminé de situations concrètes, cf. art. 22 al. 4 LParl ; OFJ, *Guide de législation*, 2019, N 552.

1873 Adoptée par l'AF conformément aux art. 163 al. 1 Cst. et 22 al. 1 LParl, cf. notamment CR Cst.-MARTENET, art. 3 N 40.

1874 ATF 130 I 1, c. 3.4.2 ; CR Cst.-DUBEY, art. 164 N 21 ss. À titre d'exemple, le TF a reconnu sur le plan cantonal que la mise en place d'un *numerus clausus* par une université lors de l'admission d'étudiantes devait se faire en fonction de grandes lignes établies par le pouvoir législatif, dans la mesure où un tel procédé influe fortement sur les droits des personnes concernées, ATF 121 I 22, c. 4a.

En l'occurrence, l'introduction d'exigences minimales de cybersécurité aux infrastructures critiques est susceptible de concerner bon nombre d'organisations, d'exercer une influence sur leurs droits et d'engendrer des conséquences financières certaines. Nous pourrions même prétendre que la cybersécurité au sein des infrastructures critiques est une question politique particulièrement décisive du fait de l'importance qu'elle représente pour la résilience de la Suisse[1875].

Il n'est pas certain que tous les éléments susmentionnés arrivent à un niveau « important » au sens de l'art. 164 al. 1 Cst. Les grandes lignes de ces exigences doivent néanmoins dans tous les cas être fixées dans une loi fédérale. En effet, les dispositions fondamentales relatives aux droits et aux obligations des personnes doivent être prévues par une loi fédérale en vertu de l'art. 164 al. 1 litt. c Cst. La notion de « fondamentale » renvoie à l'idée que les dispositions fixant les grandes lignes des règles de droit (à savoir leur but, leur objet, leur étendue ou les grands principes de leur régime) doivent figurer dans une loi au sens formel[1876]. La portée de la notion de « droits et obligations des personnes » est débattue et la notion fait partie d'une liste controversée. Elle semble tout de même englober les grandes lignes des sanctions administratives[1877], ce qui nous laisse à penser que les grandes lignes d'exigences minimales faites à des entreprises devraient également tomber sous le coup de cette disposition et, par conséquent, nécessiter d'être réglementées dans une loi fédérale. Contrairement aux dispositions fondamentales relatives aux droits et aux obligations des personnes, les dispositions revêtant un niveau d'importance moindre peuvent figurer dans une ordonnance. Il ne faut pas non plus renoncer à toute réglementation non contraignante en complément, en raison de la capacité de ce type de réglementation à s'adapter rapidement et à approfondir les exigences concrètes, surtout dans des domaines comme la cybersécurité, qui évolue rapidement et qui présente encore un niveau certain de complexité pour de nombreuses organisations. 1176

2. Le choix de la loi fédérale

a. La loi sur la sécurité de l'information

Reste à déterminer si la LSI devrait contenir les exigences minimales de cybersécurité pour les infrastructures critiques ou non. Rappelons qu'elle poursuivait déjà initialement des objectifs de sécurité de l'information et de sécurité 1177

1875 Pour un exemple, cf. ATF 123 I 254, c. 2bb dans l'éducation ; CR Cst.-DUBEY, art. 164 N 22.

1876 CR Cst.-DUBEY, art. 164 N 31. À noter que la liste de l'art. 164 al. 1 Cst. fait l'objet de critiques, cf. CR Cst-DUBEY, art. 164 N 38 et références citées.

1877 BSK BV-WYTTENBACK/WYSS, art. 164 N 27.

informatique pour la Confédération (art. 1 al. 1 LSI ; art. 1 litt. a LSI2). Elle prévoit déjà les bases et les exigences relatives à la sécurité de l'information et à la sécurité des moyens informatiques applicables aux autorités et organisations de la Confédération (art. 2 et 6 ss LSI). La loi s'accompagne d'ordonnances concrétisant et détaillant les obligations légales.

1178 La LSI a été reconnue comme base légale adéquate, voire idéale pour introduire l'obligation de signaler les cyberattaques ciblant les infrastructures critiques[1878]. Un nouvel objectif a été ajouté à la loi, qui est celui d'accroître la capacité de résilience de la Suisse face aux cybermenaces (art. 1 al. 1 litt. b LSI2). La LSI est donc la loi principale pour la cybersécurité en Suisse.

1179 En termes d'obligations, la LSI comporte à ses art. 6 ss une liste d'exigences générales en matière de sécurité de l'information et de sécurité des moyens informatiques applicables à un cercle restreint d'infrastructures critiques (principalement les autorités et organisations de la Confédération, art. 2 s. LSI). Elle va introduire une obligation de signaler les cyberattaques pour certaines infrastructures critiques (art. 74*a* ss LSI2). Dans la mesure où l'obligation de signaler les cyberattaques est une première obligation de cybersécurité applicable aux infrastructures, la loi est idéale également pour l'introduction des exigences minimales de cybersécurité pour ces organisations.

1180 Les art. 6 à 10 LSI prévoient des obligations pour que l'administration fédérale respecte la sécurité de l'information et les art. 16 à 19 LSI sont consacrés à la sécurité des moyens informatiques utilisés par l'administration fédérale. L'art. 2 al. 5 LSI prévoit déjà le champ d'application à l'attention des infrastructures critiques. La disposition pourrait être envisagée comme suit : « les organisations de droit public ou de droit privé qui exploitent des infrastructures critiques sans être visées par les al. 1 à 3 sont soumises aux [art. 6 à 11, 16 à 19, aux] art. 73*a* à 79 [et à l'art. 81 LSI] ». Cette solution serait la plus simple à mettre en œuvre du point de vue législatif.

1181 Quelques questions doivent faire l'objet de réflexions. Premièrement, la LSI vise la garantie de la sécurité de l'information et pas de la cybersécurité. Les art. 16 à 19 LSI imposent néanmoins des obligations relatives à la sécurité des moyens informatiques, à savoir la sécurité informatique. Si l'on estime que la cybersécurité englobe la sécurité des informations traitées par le biais de systèmes informatiques et la sécurité informatique[1879], l'on doit admettre ce renvoi comme suffisant. Deuxièmement, il est nécessaire de se demander si les exigences prévues par la LSI sont suffisantes, adéquates ou trop poussées,

1878 FF 2023 84, p. 18.

1879 Cf. *supra* N 48.

question à laquelle nous chercherons à répondre plus tard[1880]. Troisièmement et comme cela a été précédemment démontré, la LSI ne se fonde pas sur les fondements constitutionnels adéquats pour justifier la compétence fédérale de légiférer sur ces exigences minimales. Ce n'est pas la première fois que le fondement constitutionnel d'une loi fédérale serait sujet à controverse ; l'ajout de bases constitutionnelles lors de la révision ou de l'adoption d'une loi est possible et a déjà eu lieu[1881]. L'art. 57 Cst. doit être ajouté dans les fondements constitutionnels de la LSI « en soutien » aux autres fondements déjà utilisés, sous réserve qu'une nouvelle disposition constitutionnelle soit adoptée et serve de fondement constitutionnel plus précis pour ce faire.

b. Une nouvelle loi ?

Il convient d'examiner si l'adoption d'une nouvelle loi, portant exclusivement 1182
sur les infrastructures critiques, serait opportune. L'adoption de cette loi permettrait tout d'abord d'éviter des confusions entre ce qui est attendu de l'administration fédérale et de ce qui est exigé des infrastructures critiques. Un tel procédé permettrait ensuite de ne pas compromettre les objectifs initialement poursuivis par la LSI en lien avec l'approvisionnement du pays, la défense ou encore la politique économique extérieure de la Suisse. Ce choix permettrait finalement de mieux tenir compte d'éventuelles spécificités concernant l'ensemble des infrastructures critiques. Cela étant, la question relative au fondement constitutionnel ne serait pas résolue, à savoir si l'art. 57 Cst. peut servir de fondement unique ou, si tel n'est pas le cas, une nouvelle disposition constitutionnelle devrait être à l'origine de la nouvelle loi[1882].

Cette nouvelle loi aurait une vocation similaire à celle de la Directive (UE) 1183
2022/2555 (Directive SRI2) de l'Union européenne (UE). La Directive SRI2 sert de fondement légal général pour la cybersécurité des infrastructures critiques. Elle impose les critères à prendre en considération par les États membres pour que les infrastructures critiques prennent des mesures appropriées et proportionnées pour assurer leur cybersécurité. La Directive SRI2, remplaçant la Directive (UE) 2016/1148 (Directive SRI), est l'acte principal en matière de cybersécurité auprès des infrastructures critiques dans l'UE. Elle cherche à assurer un niveau élevé et uniforme de sécurité des réseaux et des systèmes d'information. Plus précisément, elle vise le renforcement des capacités de cybersécurité dans chaque État membre, une coopération accrue dans l'UE. Elle

1880 Cf. *infra* N 1217 ss.

1881 Voir par exemple lors de la révision totale de la LPD, cf. FF 2017 6565, p. 6631 ; voir aussi la modification du préambule de la LCart, cf. FF 2002 1911, p. 1923 s. et 1939.

1882 Cf. *supra* N 1159 ss.

prévoit aussi l'implémentation de mesures de gestion des risques en matière de cybersécurité et des obligations de notification en cas de cyberincidents pour les « entités essentielles et importantes » (art. 21 ss Directive SRI2)[1883].

1184 En cas d'adoption d'une nouvelle loi, l'obligation de signaler les cyberattaques prévue aux art. 74*a* ss LSI2 devrait logiquement être déplacée dans la nouvelle loi prévoyant les exigences minimales de cybersécurité applicables aux infrastructures critiques définies[1884].

1185 L'ordre juridique suisse est largement fondé sur la neutralité technologique, selon laquelle la législation doit appréhender tant des situations réelles que virtuelles[1885]. Adopter une loi sur la cybersécurité reviendrait à remettre en question ce principe. Pour remédier à cette éventualité, il serait toujours envisageable d'adopter une loi visant à assurer la sécurité de l'information auprès des infrastructures critiques qui comprenne la sécurité informatique, à l'instar de ce qui est fait avec la LSI. La nouvelle loi présenterait de fortes similarités avec la LSI en prévoyant pour les infrastructures critiques des obligations similaires à celles imposées par la LSI à l'administration fédérale.

1186 Bien qu'une loi spécifique pour la cybersécurité auprès des infrastructures critiques puisse répondre à différents enjeux, la LSI est idéale par ce qu'elle prévoit et les objectifs qu'elle poursuit. En outre, l'utilisation de la LSI soulève moins de questions juridiques, permet de répondre aux enjeux et questionnements et est plus simple sur le plan légistique. Elle sera donc utilisée comme base de réflexion et pour la suite de la présente analyse.

3. La possibilité de compléter la loi

a. L'ordonnance du Conseil fédéral

1187 La loi doit être complétée par une ordonnance du CF qui permet de préciser la loi. L'ordonnance s'adapte et se modifie plus facilement en fonction des évolutions technologiques[1886]. La mise en œuvre par la Confédération se justifie

1883 OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »,* 2021, p. 50 ; SALAMON, p. 240 s. La notion d'entités essentielles et importantes de l'art. 3 Directive SRI2 se rapproche de ce qui pourrait être considéré comme des infrastructures critiques en Suisse.

1884 Il conviendrait en effet de modifier la LSI en abrogeant en tout cas les dispositions des art. 74*a* ss LSI2 pour les déplacer dans la nouvelle loi, ChF, *DTL,* 2013, N 271, tout en tenant compte des critiques que l'on peut émettre au sujet de la loi, à commencer par la limitation aux cyberattaques et non pas aux cyberincidents d'une certaine gravité ou par la question du champ d'application personnel qui devrait être plus clair, MEYER/MÉTILLE, *Loi fédérale sur la sécurité de l'information : version 2.0,* 2022, N 47. À noter que la même orientation a été prise par la Directive SRI2, cf. art. 21 et 23 Directive SRI2.

1885 Pour une analyse du principe de neutralité technologique, voir BARBEY, en particulier p. 4 et 16 ; MONTAVON, p. 98 ss.

1886 BSK BV-WYTTENBACH/WYSS, art. 164 N 11.

typiquement dans les cas où une réglementation uniforme est nécessaire. L'art. 182 al. 2 Cst. (et l'art. 9 LOGA) attribue au CF la compétence de mettre en œuvre la législation fédérale[1887]. Les ordonnances que peut adopter le pouvoir exécutif pour mettre en œuvre les lois fédérales doivent se rapporter à la matière de la loi et s'inscrire dans le cadre de la finalité de ces dernières[1888].

Le pouvoir exécutif dispose d'une importante marge de manœuvre lorsqu'il s'agit de choisir s'il faut adopter une ou plusieurs ordonnances[1889]. Même s'il est plus libre que l'Assemblée fédérale (AF), l'exigence d'unité matérielle s'applique également aux instruments qu'il adopte. Il faut donc savoir si l'adoption d'une ordonnance suffit ou si l'adoption de plusieurs ordonnances distinctes se basant sur la même loi constitue un choix plus judicieux[1890]. 1188

La LSI dispose déjà de son ordonnance. L'Ordonnance sur la sécurité de l'information (OSI) doit être complétée par des précisions supplémentaires à la suite de l'introduction d'exigences de cybersécurité pour les infrastructures critiques. En outre, le projet d'Ordonnance sur la cybersécurité (P-OCyS) devient central dans ce contexte. De plus amples réflexions se poseraient davantage en cas d'adoption d'une nouvelle loi. 1189

À noter que l'ordonnance doit revêtir un niveau de densité normative suffisante. Pour ce faire, une ordonnance doit garantir une application uniforme du droit fédéral et respecter la marge de manœuvre des autorités d'exécution. En outre, dans le cas présent, elle doit vraisemblablement préciser certains concepts juridiques indéterminés. Sa densité normative est plus forte que celle de la loi dans la mesure où elle lui est plus détaillée et technique[1891]. Elle doit également veiller à laisser suffisamment de marge d'appréciation aux cantons, susceptibles d'être concernés par la réglementation[1892]. 1190

b. Une ordonnance de l'Office fédéral de la cybersécurité ?

Outre l'ordonnance du CF, il existe plusieurs ordonnances, législatives ou administratives, permettant de faciliter pour les assujetties la mise en œuvre d'une loi complète et susceptible de soulever des questions techniques ou organisationnelles. 1191

1887 OFJ, *Guide de legislation,* 2019, N 1077 ; BSK BV-KÜNZLI, art. 182 N 19 ; CR Cst.-DUBEY, art. 164 N 17.

1888 CR Cst.-MOOR, art. 182 N 16.

1889 OFJ, *Guide de législation,* 2019, N 383.

1890 OFJ, *Guide de législation,* 2019, 2019, N 599 s.

1891 BSK BV- WYTTENBACH/WYSS, art. 164 N 20.

1892 OFJ, *Guide de législation,* 2019, N 390 ss et 593.

1192 Le CF peut déléguer aux départements la compétence d'adopter des règles de droit en tenant compte de l'importance de la norme envisagée (art. 48 al. 1 LOGA)[1893]. Sur ce fondement, les départements peuvent adopter des ordonnances pour tenir compte des spécificités sectorielles.

1193 L'on pourrait concevoir une délégation au Département fédéral de la défense, de la protection de la population et des sports (DDPS) pour l'adoption d'ordonnances plus concrètes en raison de ses nouvelles compétences[1894]. Cela étant, le nouvel OFCS constitue l'autorité la plus compétente pour adopter des actes d'exécution. L'OFCS doit avoir la compétence d'adopter d'une part une ordonnance législative et, d'autre part, des directives (contraignantes et non contraignantes) d'application de la loi[1895]. Le nouvel office est effectivement l'autorité disposant des principales compétences pour édicter des normes techniques et organisationnelles pour guider la mise en œuvre et l'exécution de la législation auprès des assujetties[1896]. Il peut intervenir en édictant des lignes directrices non contraignantes comme des prescriptions obligatoires.

1194 Contrairement aux ordonnances adoptées par des départements, le CF peut procéder à la sous-délégation aux offices ou aux groupements de l'administration uniquement si la loi fédérale le prévoit (art. 48 al. 2 LOGA)[1897]. Bien que la sous-délégation aux offices ou aux groupements de l'administration soit plus compliquée que la délégation aux départements (dès lors que la loi doit le prévoir), le CF peut déléguer sa compétence à un office compétent si ce dernier dispose de compétences plus étendues pour régler certaines spécificités.

1195 À l'heure actuelle, la LSI donne compétence aux autorités soumises à la loi d'édicter les dispositions d'exécution (art. 84 al. 1 LSI). Cela étant, il serait judicieux de prévoir, avec la centralisation de la législation et pour des questions délimitées, que le CF est compétent pour concrétiser certaines dispositions

1893 OFJ, *Guide de législation,* 2019, N 729 ; BSK BV-KÜNZLI, art. 182 N 7 ; CR Cst-MOOR, art. 182 N 29.

1894 Sur la réorganisation de la cybersécurité au sein de la Confédération, cf. *supra* N 225 ss et 700 ss.

1895 Les dispositions de l'OSI dans sa version actuelle arrêtent les compétences de l'OFCS pour la sécurité de l'information au sein de la Confédération mais pas en lien avec la cybersécurité des infrastructures critiques. Cela étant, la NCSC étant transformé en OFCS et ce dernier restant compétent pour recevoir les signalements des cyberincidents, l'on peut supposer qu'il continuera à détenir ces compétences outre ce qui est prévu aux art. 73*a* ss LSI 2 et 15*a* Org-DDPS, cf. SG-DDPS, *Législation d'exécution relative à la LSI, Explications,* 2023, p. 6.

1896 Et ce bien que le service spécialisé de la Confédération pour la sécurité de l'information reprenne d'ici 2025 les compétences du NCSC en ce qui concerne l'adoption de directives pour la sécurité de l'information et la sécurité des moyens informatiques de la Confédération, cf. *supra* N 781.

1897 CR Cst.-MOOR, art. 182 N 29.

et qu'il peut déléguer cette compétence à l'OFCS, de façon similaire à ce que prévoit par exemple l'art. 62 al. 2 LTC avec une délégation du CF à l'OFCOM[1898]. L'art. 85 al. 2 LSI prévoit actuellement que le CF peut déléguer cette tâche en matière d'exigences et mesures standard non contraignantes. Dans la mesure où nous préconisons une solution centralisée au niveau de l'OFCS, la disposition devrait prévoir que le CF peut déléguer ses compétences d'adoption de dispositions d'exécution à l'OFCS, ce qui permettrait d'assurer une plus grande sécurité juridique. L'art. 85 LSI traitant uniquement des exigences et mesures standard non contraignantes, il serait préférable que l'art. 84 LSI, relatif aux dispositions d'exécution, confie une tâche de concrétisation des obligations au CF, qui peut déléguer cette compétence à l'OFCS.

Il est cohérent de centraliser ces compétences afin d'éviter que la loi ne doive octroyer la compétence à chaque office fédéral d'adopter des ordonnances. Les offices compétents pour les différents secteurs et sous-secteurs critiques sont régulièrement dépourvus de compétences poussées en cybersécurité. Une compétence sous-déléguée à chaque office sectoriellement compétent serait par ailleurs excessivement complexe à mettre en œuvre au niveau de la loi et au niveau de la pratique des autorités disposant de ressources limitées pour les questions spécifiques liées à la surveillance de la cybersécurité auprès des organisations de leur secteur. 1196

c. D'autres actes d'exécution

Des ordonnances administratives peuvent également être adoptées pour compléter des règles obligatoires par souci d'efficacité. Ces ordonnances ont vocation à s'adresser aux collaboratrices de l'administration en leur prescrivant comment exécuter leurs tâches. Elles n'ont pas force de loi et ne lient ni les administrées, ni les pouvoirs judiciaires ; leur caractère impératif varie en pratique[1899]. Elles peuvent permettre de renforcer la mise en œuvre du droit[1900]. Il ne faut pas se limiter à une réglementation centrale afin de ne pas exclure la compétence d'autorités sectoriellement compétentes d'adopter des ordonnances administratives pour guider l'exécution des normes contraignantes. Au vu de l'importance de respecter les différences intersectorielles et de pouvoir s'adapter en continu aux évolutions technologiques, il faut conserver les compétences de l'OFCS remplaçant le NCSC ainsi que les compétences 1197

1898 FF 2017 6185, p. 6264.

1899 Elles peuvent être impératives pour les autorités lorsqu'elles vont dans le sens de la loi et que leur violation revient à la violation d'une obligation légale, cf. ATF 142 II 182, c. 2.3.2 ; OA, *Enquête administrative « Fuite de données »,* 2024, N 234.

1900 FLÜCKIGER, p. 299.

des autres entités compétentes d'adopter des recommandations, normes minimales et ainsi de suite. Ces ordonnances administratives ne fondent pas directement, à l'inverse des lois et ordonnances législatives, des droits ou obligations contraignantes pour les sujets de droit et elles ne peuvent être directement contraignantes. Elles sont en l'occurrence orientées vers les personnes soumises à la législation pour orienter leur comportement *(ausengerichtete Richtlinien)*. La réglementation par le biais de directives, d'instructions ou de circulaires est admissible uniquement lorsqu'elle régit le comportement des destinataires de façon souple *(soft law)*[1901]. Ces directives, pour être contraignantes, doivent rester dans le cadre fixé par la loi qu'elle concrétise et restituer le sens exact de la loi[1902].

1198 Il nous semble important que l'OFCS puisse continuer d'adopter des directives applicables à l'administration fédérale, des instructions et communications (faisant suite à la pratique du NCSC). Il semblerait par ailleurs que, parmi les infrastructures critiques, bon nombre soient favorables à une réglementation souple, notamment par l'intervention du NCSC[1903]. Les mêmes questions se poseraient pour les autres autorités et les autres organismes actuellement compétents pour édicter de tels documents, à l'instar de l'OFAE avec sa Norme minimale pour améliorer la résilience informatique, ou des associations professionnelles ayant adopté sur cette base des normes et des manuels applicables à certains secteurs de l'approvisionnement du pays[1904].

1199 L'art. 85 LSI prévoit actuellement que le CF peut imposer des exigences standard en matière de sécurité et définir des mesures standard en matière d'organisation, de personnel et de construction, même sur le plan technique (art. 85 al. 1 LSI). Ces exigences et mesures ont valeur de recommandation, sous réserve d'être déclarées obligatoires par les autorités soumises à la loi (art. 85 al. 3 LSI).

1200 La compétence du CF d'adopter des exigences et des mesures peut être déléguée (art. 85 al. 2 LSI). Les art. 15 et 29 OSI démontrent que le CF a délégué cette compétence pour les autorités et organisations de la Confédération au service spécialisé de la Confédération pour la sécurité de l'information[1905]. Cette disposition permet à la nouvelle autorité d'adopter des directives générales

1901 OFJ, *Guide de législation*, 2019, N 557 ss ; ODERMATT, art. 22 ParlG N 24.

1902 ATF 131 V 42, c. 2.3 ; ATF 141 III 401, c. 4.2.2. Le tribunal n'est pas lié en tant que tel, mais il tient compte des ordonnances administratives et ne s'en éloigne pas sans motifs valables.

1903 KNIEPS et al., p. 23 et 25.

1904 Sur ces différents instruments, cf. notamment *supra* N 510 et 534 ss.

1905 Qui est le nouvel office reprenant les tâches du SG-DDPS et en partie du NCSC, SG-DDPS, *Législation d'exécution relative à la LSI, Explications*, 2023, p. 5.

et abstraites pour les autorités de l'art. 2 LSI. Outre les compétences d'élaborer des directives techniques qu'aurait dû conserver l'OFCS, l'OFCS devrait disposer des compétences pour adopter également des actes d'exécution, du moins non contraignants, pour guider les infrastructures critiques dans la mise en œuvre des exigences légales de cybersécurité.

Nous estimons qu'il n'est pas nécessaire que la loi précise ces délégations 1201
(contrairement à l'ordonnance qui devra être claire quant à la répartition des compétences), dans la mesure où une diversité d'autorité doit conserver ses compétences d'adoption d'actes de droit souple. En effet, dans un domaine tel que la cybersécurité, il est important de garder à l'esprit que l'autoréglementation est privilégiée depuis des années et que les différents secteurs et sous-secteurs critiques sont plus conscients de leurs spécificités que l'AF ou le CF. Certaines organisations utilisent des technologies spécifiques (à l'instar des compteurs intelligents) ou traitent des informations particulières. Il est important pour la bonne marche de la réglementation de prendre en compte les initiatives sectorielles, dont certaines sont déjà en place, afin de favoriser la prise en compte des secteurs concernés, les compétences des autorités sectorielles qui ont connaissance des spécificités propres aux différents secteurs et la position des cantons disposant de dispositions assurant un niveau égal ou plus élevé de cybersécurité[1906].

D. Le contenu de la législation

1. Une question de densité normative

Le contenu de la législation doit naturellement être décidé. Il s'agit principa- 1202
lement d'imposer des exigences minimales de cybersécurité dans la loi, en gardant à l'esprit qu'elle ne peut pas évoluer aussi rapidement que des ordonnances ou des normes non contraignantes. La loi doit prescrire les règles de droit générales et abstraites importantes, raison pour laquelle elle doit prévoir les conditions relatives aux obligations. Les compétences des autorités chargées de l'application de la loi, les voies de droits, les sanctions ou encore les dispositions transitoires doivent également y figurer[1907].

1906 Il faut maintenir l'implication d'autorités centrales et sectorielles, OFEN, *Rapport « Cyber-Sicherheit und Cyber Resilienz für die schweizer Stromversorgung »*, 2021, p. 61. Il est en revanche nécessaire à des fins de clarté que les autorités et organisations compétentes à l'instar des offices fédéraux partagent clairement les bases légales et les instruments de droit souple auprès des organisations actives dans les secteurs, notamment sur leur site Internet.

1907 OFJ, *Guide de législation*, 2019, N 581. Les dispositions finales ne seront pas approfondies dans la présente étude, soulevant d'autres questions s'éloignant du cadre de

1203 Il convient de porter une attention particulière à la densité normative. La densité normative découle du principe de la légalité de l'art. 5 al. 1 Cst. et implique que les dispositions d'une base légale doivent être suffisamment détaillées et spécifiques ou, en d'autres termes, claires et précises par rapport aux circonstances et au domaine[1908]. Pour estimer la densité normative nécessaire, il convient de prendre en considération divers facteurs, à l'instar du niveau de la norme, de l'importance du domaine concerné ou encore des besoins des destinataires concernant la sécurité du droit. La densité ne doit pas être trop forte, ce qui implique que la loi ne doit pas régler des situations qui pourraient être réglées à un niveau inférieur, régler des situations atypiques, répondre à des questions non pertinentes ou encore compléter le texte législatif par des motivations. Pour éviter une densité normative trop faible, la base légale ne doit pas se contenter d'énumérer des principes généraux sans apporter de solutions concrètes aux problèmes se posant ni laisser trop de questions ouvertes. Elle doit éclaircir les situations problématiques, répondre aux questions fondamentales et opérer des distinctions importantes.

1204 La loi fédérale doit contenir principalement des instructions de caractère général. Sa densité normative est plutôt faible en comparaison avec son ordonnance. Elle ne doit pas réglementer des situations qui pourraient être réglementées au niveau d'une ordonnance, mais ne doit pas non plus se limiter à énumérer des principes et obligations sans répondre aux problèmes[1909].

1205 Il n'est pas possible de traiter de l'ensemble d'une législation au sein de la présente étude. Il convient néanmoins de parcourir les défis juridiques majeurs de cette réglementation.

2. Le but, les définitions et le champ d'application

1206 La loi et son ordonnance doivent poursuivre des buts précis et elles doivent prévoir un champ d'application ainsi que des définitions[1910]. La disposition relative au but poursuivi par la loi doit naturellement faire état de la nécessité d'augmenter la cyberrésilience des infrastructures critiques en Suisse. Le futur art. 1 al. 1 litt. b LSI est suffisant en prévoyant que la loi vise à accroître la capacité de résilience de la Suisse face aux cybermenaces[1911].

l'analyse. À noter qu'il est en tout cas nécessaire pour les dispositions transitoires de prévoir notamment un délai de mise en conformité.

1908 OFJ, *Guide de législation*, 2019, N 592 ; CR Cst.-DUBEY, art. 5 N 46 ss.

1909 OFJ, *Guide de législation*, 2019, N 593 ss.

1910 OFJ, *Guide de législation*, 2019, N 613 ; ChF, *DTL*, 2013, N 30.

1911 FF 2023 84, p. 20 s.

La Suisse persiste à élaborer une législation technologiquement neutre, à savoir une législation permettant d'appréhender tant des situations réelles que virtuelles. Cela étant, la loi doit tout de même définir la notion de cybersécurité[1912]. La notion de cybersécurité figurait à l'art. 3 litt. a aOPCy et la LSI a vocation à être la loi principale pour la cybersécurité en Suisse. La LSI définit par ailleurs dans sa version révisée les notions de cyberincident, de cyberattaque et de cybermenaces (art. 5 litt. d, e et f LSI2). 1207

Parmi les autres définitions principales, la notion d'infrastructure critique est définie de façon opaque dans la LSI à l'heure actuelle (art. 5 litt. c LSI). La définition de l'art. 5 litt. c LSI comporte des notions indéterminées et des exemples. L'on doit donc se demander ce qui entre dans la notion d'infrastructure critique, ce qui permet dans un second temps de prévoir un champ d'application aux exigences minimales de cybersécurité. 1208

Le niveau de précision de la définition choisi entraîne plusieurs conséquences. Tout d'abord, l'exigence de clarté de la loi implique que les organisations doivent savoir si elles sont considérées comme critiques ou non. Ensuite, les infrastructures critiques ont droit au soutien matériel de l'OFCS (art. 73*a* al. 2 litt. e et art. 74 LSI2). Partant, une définition très large impliquerait que le nouvel OFCS devrait disposer de ressources très importantes pour être apte à leur venir en aide. Dans les faits, l'OFCS n'aurait probablement pas les ressources pour venir en aide à l'ensemble des organisations actives dans tous les sous-secteurs critiques[1913]. En revanche, il devrait disposer des ressources suffisantes pour soutenir le cercle d'infrastructures critiques plus restreint, par exemple les organisations de la liste de l'art. 74*b* LSI2. Finalement, le champ d'application des exigences minimales de cybersécurité doit être fixé en fonction de la définition d'une infrastructure critique. 1209

Quant à une redéfinition légale, il est possible de coller aux critères retenus dans la Stratégie de protection des infrastructures critiques (Stratégie PIC) et par l'OFPP dans son Inventaire PIC, à savoir que toute infrastructure active dans un sous-secteur critique doit être considérée comme une infrastructure critique[1914]. Une telle définition serait plus claire pour les organisations se demandant si elles sont considérées comme critiques ou non. Elle permettrait également de s'assurer qu'aucune organisation ne passe entre les mailles 1210

1912 Sur la notion de cybersécurité, cf. *supra* N 44.

1913 Le travail d'analyse mené par l'OFCS peut en effet être considérable et nécessiter des ressources majeures en termes de temps et de personnel, cf. OFCS, *Rapport concernant les analyses de données effectuées après la cyberattaque contre l'entreprise Xplain,* 2024, p. 7 et 11.

1914 Cf. *supra* N 74 ; FF 2023 1659, p. 7 ; OFPP, *Méthode d'élaboration de l'Inventaire PIC,* 2017, p. 5.

du filet. En revanche, la définition serait particulièrement large et couvrirait l'ensemble des organisations actives dans un sous-secteur critique, qui ne sont pas forcément toutes essentielles au bien-être de la population, au fonctionnement de la société civile, de l'économie ou de l'État. En outre, le soutien apporté par l'OFCS aux infrastructures critiques est plus important que celui fourni au reste de la population. Par conséquent, si de trop nombreuses organisations viennent à requérir l'aide de l'OFCS, les ressources de ce dernier pourraient être mises à mal pour soutenir des organisations qui ne sont pas toutes nécessaires à l'économie nationale ou au bien-être de la population[1915].

1211 L'art. 5 litt. c LSI doit être reformulé à plusieurs égards pour plus de clarté juridique. Premièrement, la disposition doit renvoyer au critère de sous-secteur critique de l'OFPP afin que la situation soit plus claire pour les organisations se demandant si elles sont ou non critiques. En revanche, la définition doit conserver la formulation « installations, processus et systèmes essentiels au fonctionnement de l'économie et au bien-être de la population ». Cette formulation permet d'exclure les organisations actives dans des sous-secteurs critiques qui ne présenterait pas de niveau de criticité. Deuxièmement, cette formulation doit être complétée d'une façon similaire à l'art. 6 al. 1 litt. a ch. 4 de la Loi sur le renseignement (LRens) par l'ajout de la formulation suivante : « infrastructures, installations, processus et systèmes essentiels au fonctionnement de la société, de l'économie et de l'État, ou au bien-être de la population » pour être moins limitative. En effet, certaines infrastructures critiques sont nécessaires au fonctionnement de la société et non uniquement au bien-être de la population ou à l'économie nationale, à l'instar des fournisseuses de services de télécommunication. Troisièmement, il est nécessaire que les organisations se demandant si elles sont critiques puissent requérir de l'OFPP une décision constatatoire. Cette décision pourrait émaner de l'OFCS, mais il existe probablement d'autres conséquences, non liées à la cybersécurité, découlant du statut d'infrastructure critique. La compétence d'établir l'Inventaire PIC revenant à l'OFPP, il est bien plus logique que ce dernier soit compétent pour émettre cette décision. Cette dernière permettrait à l'infrastructure critique de rejoindre le cercle fermé de clientes de l'OFCS, de bénéficier des échanges avec d'autres infrastructures critiques et des différentes mesures de soutien de l'art. 74a LSI2[1916]. Un mécanisme de décision constatatoire existe déjà à l'art. 74a al. 2 LSI2 ; il doit aussi exister pour que les organisations puissent

1915 Bien qu'il ne soit obligé de soutenir les infrastructures critiques que dans la gestion des cyberattaques signalées sur la base des art. 74*a* ss LSI2 (art. 74a al. 3 LSI2).

1916 Sur les décisions déclaratives ou constatatoires, cf. notamment DUBEY/ZUFFEREY, N 900 ss.

savoir si elles sont considérées comme des infrastructures critiques susceptibles de bénéficier du soutien prévu à l'art. 74 LSI2[1917]. L'art. 5 litt. c LSI devrait donc prévoir un premier alinéa comme suit : « infrastructure critique : les infrastructures, installations, processus et systèmes entrant dans un sous-secteur critique essentiels au fonctionnement de la société, de l'économie et de l'État, ou au bien-être de la population ». Un second alinéa devrait prévoir que l'OFPP, sur demande, renseigne et rend une décision su sujet de la qualité d'infrastructure critique d'une organisation.

Une fois la notion d'infrastructure critique clarifiée, le champ d'appli- 1212
cation peut être défini. Il doit naturellement être clair. En d'autres termes, il convient de savoir si les exigences minimales de la loi doivent s'appliquer à toutes les infrastructures critiques reconnues comme telles en vertu de l'art. 5 litt. c LSI selon la proposition de la présente étude, éventuellement en vertu d'une décision constatatoire de l'OFPP, ou si ces exigences doivent au contraire s'appliquer à un cercle restreint d'entre elles, se limitant par exemple aux organisations les plus importantes (selon le modèle de l'art. 74*b* LSI2).

Les exigences minimales de cybersécurité doivent s'appliquer aux orga- 1213
nisations listées à l'art. 74*b* LSI2, de la même manière que l'obligation de signaler les cyberattaques. Elles ne doivent pas s'appliquer à l'ensemble des infrastructures considérées comme critiques dans la mesure où certaines ne représentent pas de cyberrisques particuliers pour le bien-être de la population, ou pour le fonctionnement de la société ou de l'économie nationale. La loi et son ordonnance doivent donc lister les conditions à remplir pour être une organisation soumise aux obligations de la loi. Cette solution présente une certaine simplicité en permettant de reprendre la liste de l'art. 74*b* LSI2 qui impose l'obligation de signaler les cyberattaques à un cercle particulièrement important d'infrastructures critiques[1918]. En outre, le CF devrait conserver sa faculté d'exempter des organisations qui, prises individuellement, ne sont pas essentielles au bon fonctionnement de l'économie ou au bien-être de la population en raison de leur taille ou de leur contribution au secteur critique (art. 74*c* LSI2)[1919]. La loi doit également prévoir la possibilité pour une

1917 Il est en effet possible que certaines infrastructures critiques soient considérées comme des infrastructures critiques ayant le droit de bénéficier du soutien de l'OFCS mais sans être sujettes à des obligations telles que l'obligation de signaler les cyberattaques en vertu des art. 74*a* ss LSI2. Il pourrait en aller de la sorte pour les organisations exemptées par le CF sur la base de l'art. 74*c* LSI2.

1918 L'UE semble avoir adopté une ligne de conduite similaire pour désigner, selon les secteurs, les entreprises soumises à ces exigences minimales, cf. art. 2 et Annexes I et II Directive SRI2.

1919 FF 2023 84, p. 42.

organisation de se voir prononcer une décision constatatoire de la part de l'OFCS pour savoir si elle est soumise aux exigences minimales de cybersécurité, comme c'est déjà le cas à l'art. 74a al. 2 LSI2 pour l'obligation de signaler les cyberattaques.

1214 La liste de l'art. 74*b* devrait être revue à quelques égards. Principalement, la loi ne devrait pas limiter sa liste aux infrastructures critiques ayant leur siège en Suisse[1920]. La question se pose typiquement pour les fournisseuses et exploitantes d'informatique en nuage (art. 74*b* al. 1 litt. t LSI2). La situation, notamment en lien avec les entreprises offrant des services informatiques, peut être discutable au vu de la dépendance des organisations en Suisse à un petit nombre de prestataires d'informatique en nuage qui n'ont pas leur siège en Suisse[1921]. Une solution similaire à la théorie des effets en protection des données personnelles est préférable afin de bien pouvoir appréhender les enjeux et objectifs de sécurité en Suisse indépendamment du siège de l'organisation. Pour appréhender également les organisations ayant leur siège à l'étranger, mais offrant leurs prestations à l'intérieur du territoire helvétique, la LSI devrait concrètement prévoir que les exigences minimales de cybersécurité s'appliquent aux états de fait déployant des effets en Suisse (de façon similaire à l'art. 3 LPD). Elle ne doit dans tous les cas pas se limiter aux organisations ayant un siège en Suisse[1922].

1215 Sachant que les exigences proposées ci-dessous[1923] sont minimales, nous préconisons que l'ensemble des infrastructures critiques de l'art. 74*b* LSI2 soient soumises à ces exigences, avec la réserve susmentionnée et avec une réserve au profit des réglementations spéciales prévoyant un niveau plus élevé[1924]. Le principe de la primauté de la loi spéciale sur la loi générale *(lex specialis derogat generali)* continue de s'appliquer, ce qui implique que l'éventuelle loi sectorielle prime sur la réglementation centrale si elle prévoit des règles spéciales. Partant, la LSI doit prévoir en tant que loi centrale et à l'instar

1920 FF 2023 84, p. 42.

1921 CF, *CSN*, 2023, p. 7 ; FF 2023 84, p. 41.

1922 La théorie des effets de l'art. 74*b* al. 3 LSI2 est limitée par la condition du siège en Suisse, cf. FF 2023 84, p. 42.

1923 Cf. *infra* N 1217 ss.

1924 Pour des exemples de réglementation différenciée, voir les art. 17 s. LSI qui imposent à toutes les autorités soumises à la loi la conformité aux exigences de sécurité « Protection de base » avec des niveaux supplémentaires de mesures lorsque les violations risquent de nuire gravement ou considérablement aux intérêts de l'art. 1 al. 2 LSI. L'on peut également citer les art. 7 ss LB pour les banques d'importance systémique, les valeurs attendues pour les organisations actives dans l'approvisionnement en électricité au sens des annexes de la OApEl ou, au niveau européen, le *Digital Service Act* (DSA) qui prévoit différents niveaux d'obligations selon l'importance du service numérique.

de l'art. 2 de la Loi fédérale sur la protection de l'environnement (LPE) ou de l'art. 4 de la Loi fédérale sur la partie générale du droit des assurances sociales (LPGA) que les lois spéciales sont réservées. Cela pourrait se faire par le simple ajout d'un alinéa à l'art. 4 LSI, qui prévoit déjà la primauté de la Loi fédérale sur le principe de transparence dans l'administration (LTrans) sur la LSI (art. 4 al. 1 LSI2).

En parallèle, les sous-secteurs doivent déterminer les entités susceptibles d'être soumises à des réglementations souples spécifiques. Les organisations concernées doivent accepter d'être soumises, en raison de leur statut, de leur activité ou de la technologie à laquelle elles contribuent ou qu'elles utilisent, à des normes souples spécifiques, celles-ci n'étant par nature pas contraignantes. 1216

3. Les exigences minimales de cybersécurité

a. Le point de départ

La partie principale de la loi concerne les exigences minimales de cybersécurité pour les infrastructures critiques. Plus précisément, le cadre légal doit traiter des obligations des assujetties, des différentes procédures et des sanctions[1925]. En vertu de l'art. 164 al. 1 Cst., les dispositions « importantes » doivent figurer dans une loi au sens formel[1926], ce qui implique que la LSI doit contenir les dispositions principales relatives aux exigences minimales de cybersécurité, mais qu'elle ne doit pas en régler les moindres détails. En effet, les réglementations efficaces doivent être préférées à des prescriptions opérationnelles détaillées[1927]. La LSI contenant déjà des exigences minimales (applicables à un cercle restreint d'infrastructures critiques), nous allons parcourir les dispositions qui y figurent et examiner si d'autres dispositions sont nécessaires, que ce soit au niveau de la loi ou de l'ordonnance qui concrétise la loi. 1217

Si la loi fédérale suit une approche fondée sur le risque (qui est générale et appropriée), les obligations concrètes doivent figurer dans un instrument de droit. La loi peut prévoir des actes d'exécution, procéder par renvois ou encore contenir des annexes. Les éventuels changements principaux auront davantage à voir avec les ordonnances, les actes non contraignants adoptés par l'OFCS et, le cas échéant, par d'autres entités sectorielles pour certaines infrastructures critiques. 1218

La loi doit être axée sur les résultats que l'on vise, à l'instar de l'accès logique aux ressources essentielles plutôt que sur les modalités comme l'utilisation 1219

1925 OFJ, *Guide de législation*, N 613 et 840.

1926 Cf. *supra* N 1173 ss.

1927 CF, *CSN*, 2023, p. 21.

d'une authentification multifactorielle, afin de laisser une marge d'évolution et d'amélioration aux différentes actrices[1928]. Le droit suisse permet de prévoir les principes et objectifs dans une loi au sens formel et de concrétiser dans des ordonnances et des instruments de droit souple les exigences concrètes modifiables plus facilement au fil du temps.

1220 L'on passe généralement par des actes d'exécution pour concrétiser les obligations. La Constitution interdit au CF d'édicter les obligations générales en matière de cybersécurité dès lors qu'elles constitueraient des normes « importantes » en vertu de l'art. 164 al. 1 Cst. Elles doivent être prévues par une loi au sens formel[1929]. En revanche, l'art. 182 al. 2 Cst. attribue au CF la compétence de veiller à la mise en œuvre de la législation. La loi peut, pour des raisons de lisibilité, prévoir une disposition comme suit : « le Conseil fédéral édicte des dispositions sur les exigences minimales en matière de cybersécurité », à l'instar de ce qui est prévu à l'art. 8 al. 3 LPD. Une telle disposition est souhaitable mais elle n'est pas nécessaire. En effet, même si la loi ne confère pas de fonctions législatives expresses au CF, ce dernier dispose toujours de la compétence d'exécuter la législation en vertu de l'art. 182 al. 2 Cst. et, partant, d'adopter des ordonnances d'exécution[1930]. En outre, la loi devrait prévoir les compétences du nouvel office plus clairement pour assurer la sécurité et la prévisibilité juridiques.

1221 Les autres actes d'exécution possibles sont des ordonnances administratives non contraignantes. Il est important que les autorités compétentes puissent émettre des instructions ou des directives pour que les infrastructures critiques parviennent à mettre en œuvre leurs obligations. Ces directives présentent l'avantage de pouvoir être modifiées par l'autorité compétente rapidement pour s'adapter en continu de façon dynamique aux développements et avancées technologiques. La LSI attache déjà parfois un caractère contraignant à de telles directives. C'est typiquement ce qui est prévu à l'art. 18 al. 2 LSI, qui impose aux autorités soumises à la loi d'assurer le respect des exigences minimales de la catégorie de sécurité « protection de base » pour tous les moyens informatiques[1931].

1222 La prévisibilité du droit implique que les infrastructures critiques doivent savoir à quelles exigences minimales elles sont soumises en termes de cybersécurité et de gestion de cyberincidents. Pour rappel, la gestion d'incidents se

1928 UIT, *Guide pour l'élaboration d'une stratégie nationale de cybersécurité,* 2018, p. 44.

1929 CR Cst.-MOOR, art. 164 N 8 ; cf. *supra* N 1173 ss.

1930 ATF 142 II 182, c 2.3.1.

1931 Cf. à ce sujet NCSC, *Si001,* 2022.

découpe selon les quatre phases suivantes[1932] : la prévention ou préparation, la détection (d'événements mais surtout de cyberincidents), la réaction et les activités post-incidents. Certaines mesures doivent être implémentées tout au long de ces quatre phases, comme les diverses communications ou la documentation. Nous allons examiner quelles mesures doivent être prévues par la loi pour ces étapes et, plus superficiellement, par les ordonnances[1933], en distinguant entre les différents niveaux de réglementation et en laissant la porte ouverte à des actes d'exécution de droit souple.

b. La planification et la préparation

(i) L'approche fondée sur les risques et la planification

En termes de prévention ou de préparation, l'art. 6 al. 1 LSI impose d'évaluer 1223
les besoins de protection des informations. Les administrées doivent fixer les objectifs, les principes de gestion de risques et les conséquences d'une violation des prescriptions (art. 7 LSI). Elles doivent évaluer les risques pour pouvoir prendre les mesures pour éliminer les risques ou les ramener à un niveau acceptable (art. 8 LSI et 8 OSI).

Ces différentes mesures illustrent l'approche suivie par la LSI fondée sur 1224
les risques, qui permet à la loi de se limiter à poser le principe selon lequel les mesures doivent être prises et celles-ci doivent être adaptées aux risques[1934]. Cette orientation est à privilégier par rapport à une loi prévoyant chaque détail, dans la mesure où la loi ne peut pas anticiper toutes les circonstances auxquelles elle pourrait s'appliquer[1935]. À titre de comparaison, l'art. 21 par. 1 et 2 Directive SRI2 suit une approche similaire à l'approche suisse, en prévoyant que l'approche « tous risques » comprend au moins la gestion d'incidents, la sécurité des ressources humaines, les pratiques de base en matière de cyberhygiène ou encore la sécurité de la chaîne d'approvisionnement (art. 21 par. 2 Directive SRI2). La Directive SRI2 est plus détaillée que la LSI et impose que les mesures soient appropriées et proportionnelles, tout en tenant compte des risques, de l'état des connaissances, des normes s'il en existe, du coût et de la proportionnalité (estimée en fonction de l'exposition, de la taille de l'infrastructure et de la probabilité et de la gravité des incidents possibles), ce que le message de la LSI mentionne en partie[1936]. Une réflexion similaire doit être

1932 Si l'on se focalise sur les incidents et non pas sur les événements en général, cf. *supra* N 55.

1933 Schéma chronologique utilisé par différents standards internationaux ainsi que dans la présente étude, cf. *supra* N 90 et 291 ss.

1934 Pour la LSI, FF 2017 2765, p. 2830.

1935 Dans un ordre d'idées similaire, voir FLÜCKIGER, p. 94.

1936 FF 2017 2765, p. 2830.

suivie pour les infrastructures critiques dépassant le cercle limité des autorités et des organisations de la Confédération. Dans la mesure où la loi consacre une approche fondée sur les risques, l'étendue des mesures concrètement attendues pour chaque infrastructure critique dépend des risques auxquels elle est confrontée, ce qui permet d'éviter que certaines infrastructures critiques soient soumises à des obligations dépassant clairement leurs ressources.

1225 Alors que la LSI et l'OSI prévoient que les destinataires doivent fixer les objectifs, les principes de gestion de risques, les objets à protéger et ainsi de suite, elles ne prévoient pas spécifiquement que les mesures de sécurité doivent être documentées quelque part auprès des organisations, de façon équivalente à un règlement de traitement en protection des données personnelles (art. 5 s. OPDo). L'obligation d'établir un règlement de traitement de l'art. 5 OPDo permet de disposer d'informations notamment sur les mesures servant à garantir la sécurité des données (art. 5 OPDo). Ce règlement doit être régulièrement actualisé et mis à disposition de la conseillère à la protection des données[1937]. Il est important qu'en matière de sécurité de l'information, de cybersécurité et de sécurité informatique, les mesures soient documentées à des fins de garantie de la sécurité, de contrôle interne ou à des fins de preuve de conformité aux exigences légales. Partant, une obligation similaire devrait figurer dans la LSI (dans la mesure où il s'agit d'une obligation qui doit avoir un fondement légal). Elle doit imposer aux infrastructures critiques assujetties d'établir et de tenir un règlement pour les traitements informatisés comprenant, d'une façon similaire à ce qui est prévu à l'art. 5 OPDo, des informations sur l'organisation interne, sur les procédures de traitement et de contrôle des informations ainsi que sur les mesures visant à garantir la sécurité des moyens informatiques et des informations[1938]. L'obligation devrait si nécessaire être concrétisée dans l'ordonnance ou dans d'autres actes. La législation devrait également imposer l'élaboration d'une stratégie pour la cybersécurité pour organiser et assurer les responsabilités en termes de cybersécurité.

1937 PFPDT, *TOM,* 2024, p. 46. Voir par exemple le modèle de règlement de traitement mis à disposition par la PFPDT des personnes privées traitant des données personnelles, cf. PRÉPOSÉE FÉDÉRALE À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE, *Règlement de traitement des personnes privées*.

1938 L'OPDo fait référence à un règlement de traitement, mais il peut s'agir dans le cas présent d'un SGSI.

Schéma 19 : les ajouts proposés quant à l'approche fondée sur le risque et la planification

Réglementation actuelle

— Evaluation des besoins de protection des informations (art. 6 al. 1 LSI)
— Fixation des objectifs en matière de sécurité de l'information, des principes de gestion des risques et des conséquences d'une violation des prescriptions (art. 7 al. 2 LSI)
— Evaluation constante des risques et des mesures propres à éliminer les risques ou les ramener à un niveau acceptable (art. 8 LSI, 8 OSI)

Ajouts proposés

— Obligation de disposer d'un règlement de traitement
— Obligation d'adopter une stratégie relative à la sécurité de l'information et à la sécurité des moyens informatiques

(ii) Les responsabilités

En matière de responsabilités, les services de la Confédération doivent veiller à ce que la sécurité de l'information soit organisée, mise en œuvre et contrôlée conformément à l'état des connaissances scientifiques et techniques (art. 7 LSI). Elles doivent en outre garantir la sécurité des moyens informatiques qu'elles exploitent (art. 19 LSI). L'OSI précise à son art. 30 que les unités administratives doivent veiller à ce que les responsabilités pour la sécurité informatique soient définies opérationnellement dans les accords de projets ou dans les conventions de prestations avec des fournisseuses internes de prestations (art. 30 al. 1 OSI). 1226

L'art. 36 OSI a ajouté la notion de responsable de la sécurité de l'information en imposant ce rôle aux autorités telles que les unités administratives. L'art. 39 OSI fait de même en introduisant le rôle de responsable de la sécurité de l'information pour les départements, qui chapeaute à un niveau hiérarchique plus élevé la sécurité de l'information des départements fédéraux et de leurs unités administratives. La responsable assure typiquement la mise en place, l'exploitation, le contrôle et l'amélioration continue du SGSI ou décide des mesures nécessaires pour la formation et la sensibilisation (art. 36 al. 3 litt. a et c OSI). Elle prend également toutes les décisions exerçant une influence déterminante sur la sécurité de l'information dans son domaine de compétence, notamment en ce qui concerne l'organisation, les processus, l'acceptation des risques ou encore les objectifs de sécurité (art. 36 al. 3 litt. b OSI). Il est aujourd'hui important que toutes les infrastructures critiques soumises aux exigences disposent d'une ou plusieurs personnes compétentes pour chapeauter la sécurité de l'information, comme la sécurité informatique ou la cybersécurité. Partant, cette obligation devrait, tout comme les obligations susmentionnées, s'appliquer à l'ensemble des assujetties selon la proposition législative. 1227

1228 En outre, les autorités et organisations actuellement soumises à la LSI doivent désigner une préposée à la sécurité de l'information ainsi qu'une suppléante, qui conseillent et, sur mandat, dirigent l'organisation relative à la sécurité de l'information et la gestion des risques, vérifient le respect des prescriptions, proposent les mesures qui s'imposent et représentent le point de contact pour signaler sur une base volontaire les incidents dans le domaine de la sécurité de l'information au service spécialisé de la Confédération pour la sécurité de l'information (art. 81 LSI)[1939]. Dans la pratique actuelle, les personnes chargées de la cybersécurité disposent régulièrement d'autres compétences sans revêtir un rôle particulier, ce qui signifie que la cybersécurité est encore souvent exercée à titre accessoire[1940].

1229 Il faut, pour remédier à ce problème, imposer ce rôle aux infrastructures critiques, comme ce qui est prévu à l'art. 81 s. LSI pour l'administration fédérale (ou, d'une façon similaire, à l'art. 10 LPD avec l'institution d'une conseillère à la protection des données). L'institution d'une préposée pour les départements et pour les unités administratives poursuit notamment des objectifs de conseil et d'aide dans l'accomplissement des tâches et dans l'exécution des obligations en vertu de la LSI ou encore de respect des prescriptions relatives à la sécurité de l'information (art. 81 al. 2 LSI, 37 OSI pour les unités administratives et 40 OSI pour les départements). Au sein des unités administratives, les fonctions de la préposée à la sécurité de l'information sont principalement les suivantes : elle gère le système de gestion de la sécurité de l'information (SGSI) de l'unité administrative, sert de point de contact central et de conseil pour les questions relatives à la sécurité de l'information, veille à la mise en œuvre des directives en matière de sécurité de l'information, exerce une surveillance interne pour les questions ayant trait à ce domaine et coordonne la maîtrise des incidents et des vulnérabilités, ou encore rend compte chaque semestre à une responsable de la sécurité selon les art. 36 s. OSI[1941].

1230 Les fonctions de responsable de la sécurité de l'information et de préposée sont proches et il s'agit principalement de disposer d'une ou plusieurs personnes compétentes pour chapeauter la cybersécurité et la sécurité de l'information ainsi que gérer le SGSI, servir de point de contact et de conseil pour la cybersécurité et veiller à la mise en œuvre des exigences au sein des organisations. Ces rôles semblent pouvoir revenir à la même personne, par exemple pour une infrastructure critique de petite taille et de peu de ressources. Ce qui

1939 FF 2017 2765, p. 2875 s.

1940 C'est un problème qui touche toutes les organisations, cf. pour les PME, NCSC, *Rapport semestriel 2022/2*, 2023, p. 7.

1941 Il est d'ailleurs prévu que les préposées à la sécurité de l'information soient chargées de quelques compétences de gestion d'incidents.

importe c'est que les fonctions assimilées aux préposées et aux responsables de la cybersécurité existent au sein des infrastructures critiques.

Cette réflexion nous amène à nous interroger sur la nécessité d'imposer aux infrastructures critiques une obligation de disposer d'une prestataire de gestion de cyberincidents. Ce qui importe réellement porte sur les compétences desquelles il faut disposer pour gérer un cyberincident. Le recours à une prestataire en tant que telle déplace l'intérêt sur la forme que doivent prendre les compétences, ce qui est d'une moindre importance, au vu de la diversité d'intervenantes et de structures. Qu'une organisation décide d'engager à l'interne quelques personnes pour gérer les cyberincidents, de sous-traiter la gestion de cyberincidents à l'externe ou qu'elle décide de faire appel à un *Security Operation Centre* (SOC), une *Computer Security Incident Response Team* (CSIRT) externe ou un *Cyber Fusion Centre*[1942] n'a pas de réelle portée pratique, tant que suffisamment de personnes compétentes sont chargées des compétences susmentionnées. Le CF exprime par ailleurs dans son message que des compétences claires pour le traitement des incidents et des vulnérabilités doivent être attribuées, et que « le personnel impliqué, qu'il soit interne ou externe » doit être en mesure de réagir en cas d'incident pour limiter au maximum les conséquences dommageables de ce dernier[1943]. En outre, bien qu'imposer une responsabilité chapeautant les questions de sécurité de l'information nous semble cohérent, imposer légalement le recours à une prestataire de gestion de cyberincidents serait trop intrusif dans les pratiques, en particulier s'agissant d'une question qui est actuellement largement laissée à la discrétion de la pratique. Par conséquent, il n'est pas nécessaire que la législation consacre cette question. 1231

En revanche, les organisations assujetties doivent disposer de personnes compétentes pour gérer les cyberincidents[1944]. Un acte de droit souple peut toujours, pour le surplus, préciser les structures qui existent (à l'instar de ce qui est prévu pour l'approvisionnement en électricité)[1945]. La possibilité de réglementer la profession du point de vue des prestataires sera analysée plus avant, dans la mesure où elles font l'objet d'une partie de la présente étude. D'autres questions les concernant se posent, notamment en lien avec le statut de ces organisations ou avec les garanties de la qualité de leurs prestations[1946]. 1232

1942 Cf. *supra* N 272 ss.

1943 FF 2017 2765, p. 2831.

1944 À titre de comparaison, la norme ISO/IEC 27032 : 2023 prévoit que les organisations appliquant la norme doivent établir une prestataire de gestion de cyberincidents bénéficiant du soutien d'une équipe de réponse aux incidents, cf. ISO/IEC 27032 : 2023, p. 16.

1945 AES, *Handbuch Grundschutz für « Operational Technology » in der Stromversorgung*, 2018, p. 24 ss.

1946 Cf. *infra* N 1300 ss.

L'art. 9 LSI impose dans ce contexte la reprise des exigences et des mesures dans les contrats liant les autorités et les organisations de l'art. 2 LSI à autrui. Cette exigence est nécessaire également auprès des autres infrastructures critiques. Elles font souvent appel à des organisations tierces pour des questions de sécurité et il est nécessaire que les infrastructures critiques puissent contrôler le respect des exigences minimales de sécurité par leurs prestataires[1947].

Schéma 20 : la modification proposée quant aux responsabilités

Réglementation actuelle

— Organisation, mise en oeuve et contrôle de la sécurité de l'information (art. 7 al.1 LSI)
— Définition opérationnelle des responsabilités pour la sécurité informatique dans les accords de projets et les conventions de prestations avec des fournisseuses internes de prestations (art. 30 al. 1 OSI)
— Préposée à la sécurité de l'information (art. 81 LSI) et responsable de la sécurité de l'information
— Reprise dans les contrats avec des tierces des exigences et des mesures (art. 9 LSI)

Modification proposée

— Tâches de la préposée d'office (art. 81 al. 2 LSI)

(iii) La sécurité de l'information et la sécurité informatique

1233 La LSI, l'OSI et la directive Si001 opèrent une distinction entre la sécurité de l'information et la sécurité des moyens informatiques, dans la mesure où tous les traitements d'informations ne sont pas effectués par le biais de moyens informatiques. Cela étant, les mesures qui sont utiles en termes de cybersécurité, de sécurité de l'information ou de sécurité des moyens informatiques se recoupent régulièrement et de nombreuses mesures permettent de servir à plusieurs de ces aspects. Partant, il n'est pas important de se perdre sur des considérations terminologiques concernant la division entre sécurité de l'information, cybersécurité et sécurité informatique ; nous les traitons simultanément et en déduisons des impacts sur la cybersécurité qui constitue le cœur de la présente étude[1948].

1234 Des obligations relatives à la gestion d'incidents figurent dans la LSI. Les autorités soumises à la LSI doivent tout d'abord établir des plans d'action

1947 FF 2017 2765, p. 2831.

1948 Par exemple, le recours aux méthodes d'authentification (typiquement multifactorielles) permet de protéger l'accès à un objet informatique et de protéger les informations auxquelles il est possible d'accéder une fois une personne authentifiée.

pour les « graves violations de la sécurité de l'information susceptibles de menacer l'accomplissement de tâches indispensables de la Confédération » et faire des exercices à cet effet (art. 10 al. 2 LSI). L'art. 12 OSI vient préciser que les unités administratives doivent fixer avec les fournisseuses de prestations la manière dont les incidents et vulnérabilités sont annoncées et maîtrisées et régler la compétence décisionnelle pour les mesures urgentes (art. 12 al. 1 OSI). Établir des plans de gestion d'incidents et de vulnérabilités est nécessaire. Il faut se préparer pour pouvoir comprendre au mieux les incidents, leurs causes, et pour y remédier et rétablir une situation sûre de la manière la plus efficiente. Cela étant, la limitation de la loi aux « graves incidents susceptibles de menacer l'accomplissement des tâches indispensables » est discutable. L'art. 10 al. 2 LSI doit être modifié pour les autorités et organisations de la Confédération, ainsi que pour les infrastructures critiques soumises aux exigences proposées par la présente étude. L'article doit prévoir une obligation d'établir des plans d'action pour les graves violations de la sécurité de l'information et non plus uniquement pour les violations susceptibles de menacer les tâches indispensables. L'art. 12 OSI doit être modifié par un ajout selon lequel le plan de gestion d'incidents doit tenir compte et faire état des ressources à disposition, des valeurs (notamment éthiques) à appliquer dans des cas urgents et ainsi de suite. Ce plan devrait logiquement faire partie du règlement de traitement des organisations soumises aux exigences minimales.

En parallèle et pour la sécurité des moyens informatiques, les personnes soumises à la LSI doivent déjà fixer les exigences minimales de sécurité applicables aux moyens informatiques. La protection de base est dans tous les cas obligatoire et elle se compose actuellement de la directive Si001 du NCSC[1949]. Les autorités et organisations doivent analyser s'il est nécessaire d'assurer la protection élevée ou très élevée, qui doit être assurée si les violations de la sécurité de l'information risquent de nuire considérablement ou, respectivement, gravement aux intérêts de sécurité intérieure ou extérieure de la Suisse, aux intérêts économiques de la Confédération et ainsi de suite (art. 1 al. 2 par renvoi de l'art. 17 LSI). En cas de révision de la loi pour que les exigences minimales de cybersécurité s'appliquent à un cercle plus important d'infrastructures critiques, il conviendra d'analyser s'il est nécessaire que toutes les exigences détaillées dans la directive Si001 du NCSC soient applicables à l'ensemble des infrastructures critiques ou si une autre directive (contraignante ou non mais mêlant à nouveau sécurité de l'information et sécurité informatique) 1235

1949 La directive reste en vigueur dans les trois ans suivant son adoption, à savoir jusqu'en 2025. Le service spécialisé de la Confédération pour la sécurité de l'information sera compétent dès 2025 pour émettre les directives concernant les exigences minimales pour les catégories de sécurité visées à l'art. 17 LSI (art. 29 al. 1 OSI).

devrait être applicable à toutes les infrastructures critiques soumises aux exigences proposées. La directive devrait émaner de l'OFCS et non pas du service spécialisé de la Confédération pour la sécurité de l'information qui détiendra cette compétence à partir de 2025 (art. 29 al. 1 OSI), dans la mesure où c'est l'OFCS qui conserve les compétences du NCSC pour la cybersécurité des infrastructures critiques. Il conviendrait dans tous les cas d'appliquer des mesures plus concrètes que les exigences légales aux infrastructures critiques pour les guider dans la mise en œuvre de la législation en prévoyant des mesures concrètes à l'instar d'authentifications ou de mots de passe[1950]. En outre, une directive (non contraignante) devrait traiter des alternatives et des bénéfices de disposer d'une prestataire de gestion de cyberincidents, pour que les organisations se familiarisent davantage avec cette possibilité (à l'interne ou à l'externe et peu importe la structure choisie) et pour laisse le choix aux organisations concernées quant à l'organisation de leurs compétences de gestion de cyberincidents.

1236 En fonction des exigences plus concrètes s'appliquant à l'infrastructure critique en fonction de son besoin de protection, elle devrait être soumise aux exigences des art. 16 LSI et 27 OSI qui imposent aux unités administratives d'élaborer une procédure de sécurité pour protéger la sécurité de l'information lors de l'utilisation de moyens informatiques, basée sur les besoins. La procédure de sécurité doit définir en particulier les critères pour évaluer le besoin de protection des informations avant la mise en service des moyens informatiques, les modalités de mise en œuvre des mesures de sécurité et leur contrôle, la compétence d'autoriser les moyens informatiques et la procédure à suivre en cas de modification des risques (art. 16 al. 2 LSI)[1951]. Les étapes principales relatives à la maîtrise d'incidents et les bons gestes pourraient être comprises à l'art. 16 al. 2 litt. b LSI en tant que mesures de sécurité, dont les modalités de mise en œuvre et leur contrôle doivent figurer dans la procédure de sécurité. L'art. 27 OSI impose aux unités administratives de mettre en œuvre les consignes minimales des différentes catégories de sécurité et de vérifier si des mesures de sécurité supplémentaires sont nécessaires (art. 27 al. 2 OSI).

1237 L'art. 19 LSI impose aux autorités et organisations soumises actuellement à la LSI de garantir la sécurité des moyens informatiques qu'elles exploitent. La disposition reste très générale[1952]. L'art. 30 OSI concrétisant l'art. 19 LSI est donc bénéfique. L'art. 30 al. 4 OSI précise en particulier que les fournisseuses

1950 NCSC, *Si001,* 2022, T5, T6 et T7, p. 10 s.

1951 FF 2017 2765, p. 2837 s.

1952 Les contrôles réguliers, les capteurs, les installations d'alarme ou de surveillance des réseaux ou encore les analyses régulières des fichiers journaux sont des mesures préventives selon le message, FF 2017 2765, p. 2831.

de prestations doivent procéder à une surveillance pour s'assurer que l'infrastructure informatique est utilisée de façon sûre et rechercher régulièrement les menaces et vulnérabilités. Cela étant, dans le contexte de la réglementation de la sécurité de l'information des infrastructures critiques, nous estimons qu'un alinéa supplémentaire devrait soumettre celles-ci à l'obligation de contrôler (soit elles-mêmes, soit lorsqu'elles délèguent cette tâche) que l'infrastructure informatique est surveillée, de sorte à garantir une utilisation sûre, et que les menaces et vulnérabilités sont régulièrement recherchées.

1238 L'OSI, ayant pour vocation de concrétiser la LSI, comporte davantage de mesures de prévention dans le cadre de l'art. 7 al. 1 LSI notamment. Parmi celles-ci figurent l'établissement d'un SGSI (art. 5 OSI), l'élaboration d'une liste de bases légales et d'obligations contractuelles (art. 6 OSI) et d'un inventaire des objets à protéger (art. 7 OSI). Ces mesures sont importantes et devraient s'appliquer aux infrastructures critiques dans leur ensemble dans la mesure où bon nombre sont incertaines quant aux réglementations leur étant applicables et que l'identification des objets à protéger constitue l'une des premières étapes pour appréhender les autres mesures de sécurité. L'inventaire doit être mis à jour et réévalué, notamment lors de changements, ce qui doit figurer dans l'ordonnance. Concernant plus précisément l'établissement d'un SGSI, il revêt une importance pratique considérable, se composant de procédures et de règles expliquant comment la sécurité de l'information est organisée dans un système et en documentant la répartition des tâches, des compétences et des responsabilités. Il permet ainsi de gérer et d'améliorer la sécurité de l'information au sein des organisations[1953]. Ces exigences devraient être applicables aux infrastructures critiques soumises aux exigences proposées.

1239 L'OSI consacre d'autres mesures organisationnelles, telles que la formation des collaboratrices (art. 11 OSI) ou la planification de contrôles et d'audits (art. 13 OSI). La formation et la sensibilisation des collaboratrices sont nécessaires pour une bonne cyberhygiène et doivent être faites également par les autres infrastructures critiques que celles de l'art. 2 LSI, qui peuvent au besoin s'appuyer sur la documentation que le service spécialisé de la Confédération pour la sécurité de l'information met à disposition (art. 11 al. 4 OSI)[1954]. La planification de contrôles limités informels ou d'audits formalisés doit informer sur la manière de contrôler le respect des prescriptions en fonction du

1953 Les SGSI sont d'ailleurs prévus par différentes normes internationales, dont la norme ISO/IEC 27001, cf. SG-DDPS, *Législation d'exécution relative à la loi sur la sécurité de l'information, Rapport explicatif*, 2022, p. 13.

1954 Cf. par exemple NCSC, *Campagne dans l'administration fédérale, La sécurité est en vos mains*.

risque et l'efficacité des mesures de sécurité (art. 13 al. 1 OSI) [1955]. Elle constitue une mesure nécessaire pour toutes les infrastructures critiques de la présente recommandation, dès lors que le manque de contrôle et d'audits est aujourd'hui réel.

1240 Finalement, des obligations de cybersécurité dès la conception et par défaut doivent être ancrées dans la loi, et non pas uniquement, comme c'est le cas aujourd'hui, comme principes directeurs de la Directive Si001 qui n'est applicable qu'à l'administration fédérale et pour les moyens informatiques[1956]. De nombreuses mesures doivent être prises de façon préventive à un incident. Il est nécessaire qu'elles soient envisagées dès le début d'un traitement d'information ou du recours à un moyen informatique, raison pour laquelle il est nécessaire de prévoir au sein de la LSI une obligation de cybersécurité dès la conception, faisant partie de la responsabilité des infrastructures critiques qui devront en vertu de l'art. 9LSI s'assurer du respect de ces exigences dans leurs contrats avec des tierces[1957]. Une obligation de cybersécurité par défaut doit simultanément être introduite afin de s'assurer que les infrastructures critiques assurent par défaut un traitement d'informations et une utilisation de moyens informatiques les plus sûres possibles.

1241 Le droit suisse ne règle pas forcément toujours la sécurité de la chaîne d'approvisionnement[1958]. À titre de comparaison, l'UE se fonde sur une autre approche qui consiste en la réalisation d'évaluations coordonnées des risques pour la sécurité liés à la chaîne d'approvisionnement critiques afin de déterminer les vulnérabilités, services et produits pertinents au cas par cas. C'est notamment le cas en matière de cybersécurité de la 5G dans l'UE (art. 22 Directive SRI2, c. 90 s. Directive SRI2)[1959]. Les évaluations menées dans l'UE doivent recenser les mesures, les plans d'atténuation et les meilleures pratiques contre les dépendances critiques, les éventuelles menaces, risques et vulnérabilités associées à une chaîne d'approvisionnement, tout en encourageant

1955 SG-DDPS, *Législation d'exécution relative à la loi sur la sécurité de l'information*, Rapport explicatif, 2022, p. 16.

1956 NCSC, *Si001*, 2022, p. 7 s. Autrement, l'économie du numérique se base sur une insécurité dès la conception *(unsecurity by design)*, cf. GHERNAOUTI, *Cybercriminalité*, 2023, p. 23 et 65 s.

1957 Pour un avis similaire concernant les applications utilisées par l'administration fédérale, cf. OA, *Enquête administrative « Fuite de données »*, 2024, N 579. Cf. à titre de comparaison les obligations de protection des données par défaut et dès la conception de l'art. 7 LPD, cf. CR LPD-FANTI/STAEGER, art. 7 N 21 ss.

1958 Mais nous avons vu que des mécanismes extralégaux existent, cf. *supra* N 55.

1959 En comparaison, la Suisse a constitué tout un dossier sur la 5G, mais de façon plus générale et non pas ciblé sur les questions de cybersécurité, cf. OFCOM, *Questions et réponses sur la 5G*.

les infrastructures critiques à les adopter en fonction de facteurs tels que leur utilisation des produits ou services concernés ou la pertinence de ces derniers sur des fonctions sensibles ou critiques (c. 90 s. Directive SRI2). Un tel mécanisme en Suisse devrait, comme dans l'UE et s'il venait à exister pour certaines technologies, impliquer une collaboration et une coordination entre différentes actrices telles que les autorités fédérales (comme l'OFCS), cantonales voire communales, les organisations (à l'instar du NTC) et le secteur concerné.

Schémas 21 et 22 : les ajouts et modifications proposées quant aux mesures pour la sécurité de l'information et pour la sécurité des moyens informatiques

Réglementation actuelle

- Etablissement de plans d'action pour les graves violations de la sécurité de l'information susceptibles de menacer les tâches indispensables de la Confédération (art. 10 al. 2 LSI)
- Elaboration d'une procédure de sécurité basée sur les besoins pour protéger la sécurité de l'information lors de l'utilisation de moyens informatiques (art.16 LSI, 27 OSI)
- Respect de la directive Si001 « Protection de base dans l'administration fédérale » (art. 17 LSI)
- Etablissement d'un SGSI (art. 5 OSI)
- Elaboration d'une liste de bases légales et d'obligations contractuelles (art. 6 OSI)

Modification proposée

- Etablissement de plans d'action pour les « graves violations » de la sécurité de l'information (art. 10 al. 2 LSI), plus d'informations
- Adoption d'une directive similaire pour l'ensemble des infrastructures critiques assujetties

Réglementation actuelle

- Elaboration d'un inventaire des objets à protéger (art. 7 OSI)
- Formation des collaboratrices (art. 11 OSI)
- Planification de contrôles et d'audits (art. 13 OSI)
- Classification d'informations (art. 11 à 15 LSI, 24 à 26 OSI)

Ajout et modification proposées

- Mise à jour et réévaluation de l'inventaire, notamment lors de changements
- Ajout des obligations de cybersécurité par défaut et dès la conception

(iv) Les autres mesures de la LSI

1242 Les art. 11 à 15 LSI et 24 à 26 OSI, prévoyant la classification d'informations, peuvent s'appliquer à l'ensemble des infrastructures critiques sans constituer une intrusion disproportionnée, dans la mesure où il est important que les organisations traitant des informations susceptibles de nuire aux intérêts définis à l'art. 1 al. 2 litt. a à d LSI classifient ce type d'informations. Il en va de même pour les mesures de protection physique (art. 22 s. LSI) qui se limitent à imposer de veiller à assurer une protection physique adéquate des informations et moyens informatiques dont elles sont responsables vis-à-vis de perturbations ou d'utilisations abusives.

1243 En revanche, les mesures relatives aux personnes (notamment en termes de conditions d'accès aux informations et moyens informatiques, art. 20 s. LSI), les contrôles de sécurité relatifs aux personnes (art. 27 à 48 LSI) ou les procédures de sécurité relatives aux entreprises (art. 49 à 72 LSI) sont trop intrusives et disproportionnées pour être applicables à l'ensemble des infrastructures critiques soumises aux exigences légales, raison pour laquelle il est préférable que la loi prévoie la possibilité de réglementer séparément ou renvoyer de façon analogique pour certains secteurs, certains postes ou certains mandats spécifiques.

Schéma 23 : la modification proposée quant aux autres mesures de la LSI

Réglementation actuelle

— Classification des informations (art. 11 à 15 LSI, 24 à 26 OSI)
— Mesures de protection physiques (art. 22 s. LSI)
— Mesures relatives aux personnes (art. 20 s. LSI)
— Contrôles de sécurité relatifs aux personnes (art. 24 à 48 LSI)
— Procédures de sécurité relatives aux entreprises (art. 49 à 72 LSI)

Modification proposée

— Les mesures relatives aux personnes (art. 20 s. LSI), les contrôles de sécurité relatifs aux personnes (art. 25 à 48 LSI) et les procédures de sécurité relatives aux entreprises (art. 49 à 72 LSI) ne doivent pas s'appliquer à l'ensemble des infrastructures critiques assujetties

c. La détection

Pour ce qu'il en va de la détection et de la réaction, l'art. 10 al. 1 LSI prévoit la procédure en cas de violation de la sécurité de l'information et impose de détecter des violations de la sécurité de l'information, d'en analyser les causes et de limiter au maximum leurs conséquences. En parallèle, l'art. 19 al. 1 LSI impose aux autorités et organisations de l'art. 2 LSI de garantir, de façon générale, la sécurité des moyens informatiques qu'elles exploitent. 1244

La garantie de la détection, entre la prévention et la réaction, sous-entend d'abord qu'une organisation dispose des mécanismes et des outils permettant de ne pas passer à côté d'un incident en surveillant les différents systèmes, réseaux et infrastructures pour détecter différents logiciels malveillants sur différents supports, en procédant à des scans de vulnérabilités et en mettant en place du monitorage. Les directives permettant de mettre en œuvre la législation peuvent aller à un niveau de précision plus approfondi que ce que prévoit la loi, en insistant sur l'importance de disposer de systèmes comme les systèmes de détection d'intrusion (*intrusion detection systems,* IDS), à l'image de ce qui figure dans la Directive Si001 applicable à l'administration fédérale[1960] ou dans la Norme minimale pour améliorer la résilience informatique de l'OFAE[1961]. Si de tels événements sont trop concrets pour figurer dans la loi, il n'est pas non plus nécessaire que l'ordonnance prévoie de telles illustrations. De telles informations peuvent figurer dans des actes d'exécution de droit souple. 1245

Certaines mesures contribuant à la prévention servent aussi à la détection d'un incident. L'exploitation d'instruments de surveillance fait partie des mesures de prévention et de détection, de même que le test des processus de détection. Le fait de s'assurer que les informations sur les incidents provenant de différents capteurs ou de différentes sources soient compilées et exploitées tombe dans la détection comme dans la réaction. Certaines dispositions contraignantes et non contraignantes adressant ces différentes informations (par exemple DE.AE-3 Norme minimale pour améliorer la résilience informatique pour l'exploitation des informations provenant de différents capteurs et sources), il n'est pas nécessaire, dans le cadre de la détection, d'aller plus loin dans la loi ou dans une ordonnance. 1246

1960 NCSC, *Si001,* 2022, Z5.1, p. 19.

1961 OFAE, *Norme minimale pour améliorer la résilience informatique,* 2023, D.CM, p. 28. Les IDPS permettent en pratique de se protéger de nombreuses exploitations malveillantes, MEYER/DAVIES, N 50.

Schéma 24 : la réglementation quant à la détection de cyberincidents

Réglementation actuelle

— Détection des violations de la sécurité de l'information (art. 10 al. 1 LSI)
— Garantie de la sécurité des moyens informatiques exploités (art. 19 al. 1 LSI)

Aucune modification nécessaire

d. La réaction et les mesures post-incidents

1247 L'art. 10 al. 1 LSI prévoit que les causes d'un incident de la sécurité de l'information doivent être clarifiées et ses conséquences limitées au maximum. L'art. 12 OSI précise principalement les relations entre les assujetties et les autorités compétentes (ce qui sera parcouru ci-dessous dans le cadre de la communication). La réaction comprend les analyses relatives à un incident, la limitation de sa diffusion, son éradication et le rétablissement d'une situation sûre. Ces différentes sous-étapes sont prévues à l'art. 10 al. 1 LSI. En revanche, l'ordonnance doit aller plus loin dans la concrétisation de cette catégorie de mesures.

1248 L'art. 12 OSI prévoit principalement des considérations relatives à la communication et à la coopération des autorités de surveillance et de l'organisation sujette aux obligations de la LSI. Il doit également préciser, comme à sa fonction, l'art. 10 al. 1 LSI. La première précision à ajouter a trait aux objectifs poursuivis par les analyses (art. 10 al. 1 LSI)[1962], afin de permettre aux organisations de prendre les mesures appropriées et d'appréhender correctement ces analyses. Un alinéa de l'art. 12 OSI peut à cette fin prévoir que « l'analyse doit notamment permettre de comprendre les causes et l'étendue d'un incident, identifier les bonnes réponses, avoir une vue d'ensemble, améliorer la sécurité de l'organisation et préparer les informations susceptibles d'être utilisées plus tard ». Une telle formulation permet aux organisations de mieux appréhender ces analyses. Pour être efficientes, les différentes analyses devant être entreprises n'ont pas nécessairement besoin de figurer dans l'ordonnance, mais l'opinion ici défendue estime en revanche que ces informations doivent figurer soit dans les ordonnances à vocation plus concrète, notamment l'ordonnance de l'OFCS, soit dans les actes de droit souple, afin d'orienter les organisations soumises aux exigences minimales.

1962 FF 2017 2765, p. 2831.

La seconde partie de la réaction porte sur la limitation au maximum des conséquences dommageables d'un incident (art. 10 al. 1 LSI). L'art. 12 OSI doit concrétiser cette obligation en précisant que pour ce faire, l'organisation doit veiller à limiter la diffusion d'un incident, à l'éradiquer et à rétablir une situation sûre. Cette considération doit, comme celle relative aux analyses, être précisée dans le droit souple et dans le rapport de l'ordonnance. 1249

Les mesures de réaction sont plus diversifiées que les mesures de prévention et elles sont plus spécifiques à chaque type d'incident que les mesures préventives. Partant, elles doivent davantage être concrétisées à un niveau inférieur. Il n'est pas exclu que l'OFCS adopte une ordonnance en abordant ces questions. Autrement, les mesures réactives sont plus susceptibles d'être abordées dans des actes de droit souple, permettant de préciser les mesures techniques et organisationnelles à mettre en place. 1250

L'ordonnance de l'OFCS (ou sa directive) devrait tout d'abord mentionner que les incidents doivent être priorisés (selon des critères préalablement établis lorsque cela est possible)[1963]. Ensuite, certains éléments d'orientation sur les analyses doivent être mentionnés, en précisant que l'analyse de l'incident et de ses causes doit typiquement porter sur l'environnement, les informations issues des connexions réseau, les processus logiciels, la mémoire, les fichiers de journalisation, les codes malicieux, les hôtes compromises et les artéfacts ou les traces laissées par une intruse. En complément, il est utile de préciser que les incidents doivent être contenus, à savoir que, régulièrement, l'hôte compromise doit être isolée du reste du réseau, par exemple en bloquant, déconnectant et modifiant le routage ou en effectuant des verrouillages d'urgence[1964]. L'éradication peut à ce même titre être appréhendée, en conseillant aux organisations, selon les cas de figure, l'élimination définitive des composants d'un incident, à l'instar des logiciels malveillants, de comptes d'utilisatrices infectés ou d'artéfacts sur un système ou, dans d'autres situations, le reformatage d'un disque dur ou sa destruction physique. Finalement, comme mesures concrètes pour le rétablissement d'une situation sûre ou de *recovery,* un acte de droit souple doit mentionner le nettoyage ou la désinfection d'un système, l'arrêt d'un système, la récupération de données effacées, la reconstruction à partir de zéro ou le renforcement de la sécurité, la modification de mots de passe ou encore le remplacement d'un fichier affecté par un fichier 1251

1963 Le P-OCyS prévoit désormais que des priorités peuvent être établies par l'OFCS en cas de demandes relatives à des cyberattaques dépassant ses capacités (art. 8 P-OCyS). Le fait que l'OFCS doive tenir compte des intérêts publics en jeu crée un facteur préalable nécessaire dans la prise de décision de l'office, OFCS, *Commentaire concernant l'OCyS*, 2024, p. 13.

1964 Voir à titre de comparaison NCSC, *Si001,* 2022, S4.2, p. 14.

propre ou la mise en place de correctifs. À noter que ces concrétisations pourraient également porter sur l'importance de la *forensic preparedness*, à savoir de la collecte et de la conservation d'informations durant la gestion d'un incident à des fins forensiques (en portant une attention aux modalités comme la méthode de collecte, le format des informations conservées ou la qualité de la sauvegarde pour pouvoir analyser et exploiter les moyens de preuve en découlant par la suite).

1252 La mention de ces informations dans un acte de droit souple doit être considérée en fonction de son apport réel, en le contrebalançant avec la complexité que peut amener la mention de toutes ces informations. L'objectif des exigences et des recommandations n'est pas de noyer les infrastructures critiques dans des informations.

1253 Les mesures post-incidents portent principalement sur les leçons tirées ou *lessons learned*. La LSI ne devrait pas spécialement être précisée concernant cette question, mais soit l'ordonnance soit le droit souple pourrait éventuellement préciser, pour faire le pont entre la réaction et la prévention, que des leçons doivent être tirées des incidents gérés pour améliorer la prévention de l'organisation et sa sécurité globale.

Schéma 25 : l'ajout et les modifications proposées quant aux mesures réactives et post-cyberincidents

Réglementation actuelle

- Classification des causes d'un incident de la sécurité de l'information (art. 10 al. 1 LSI)
- Limitation au maximum des conséquences d'un incident de la sécurité de l'information (art. 10 al. 1 LSI)
- Communications, coopération avec le service spécialisé de la Confédération pour la sécurité de l'information et avec l'OFCS (art. 12 OSI)
- Garantie de la sécurité des moyens informatiques

Ajout et modifications proposées

- L'art. 12 OSI, l'ordonnance de l'OFCS ou un acte de droit souple doit concrétiser l'obligation de l'analyse de l'incident
- L'art. 12 OSI, l'ordonnance de l'OFCS ou un acte de droit souple doit préciser les étapes principales de la limitation des consequences
- Précisions quant aux leçons à tirer pour améliorer la prévention et la sécurité globale

e. Tout au long du processus : les communications et la documentation

Des mécanismes de communication et de collaboration existent et peuvent 1254
être utilisés tout au long du processus de gestion de cyberincidents. Actuellement, l'art. 12 OSI prévoit les échanges d'informations avec le service spécialisé de la Confédération pour la sécurité de l'information et l'OFCS, voire la PFPDT, dans le cadre des incidents liés à la sécurité de l'information. Autrement, certains actes de droit souple fournissent des indications quant à ce qui peut être prévu en termes de communications à faire ou à prévoir (voir par exemple RS.CO-3, 4 et 5, RC.CO Norme minimale pour améliorer la résilience informatique). Cela étant, il faut prévoir plus largement que les différentes communications internes et externes doivent être établies par avance et effectuées lorsque cela est nécessaire. L'ordonnance doit le mentionner (en lien avec l'art. 7 LSI qui instaure la responsabilité pour la sécurité de l'information) pour permettre aux organisations de poser à l'avance les communications et leurs modalités (qui pourraient être précisées dans un instrument de droit souple). Les organisations pourraient s'aider de la liste de bases légales leur étant applicables pour s'orienter concernant les communications externes obligatoires applicables (art. 6 al. 1 OSI).

La documentation doit être consacrée à chaque étape de la gestion de 1255
cyberincidents, dans la mesure où elle concerne des mesures et des informations auxquelles une organisation accède tout au long du processus. En matière de prévention, il est nécessaire en pratique de documenter diverses informations ayant trait notamment aux éléments journalisés ou aux premières mesures de sécurité. Ensuite, les accès suspicieux détectés doivent typiquement être documentés, de même pour les mesures prises à la suite de la découverte des accès suspicieux pour analyser si ceux-ci consistent en de fausses alertes provenant d'un IDS ou s'il s'agit d'un incident. La réaction à un cyberincident doit également être documentée ; à ce titre, les informations en lien avec l'incident ou les moyens mis en œuvre doivent être collectés *(« Who, What, Where, Why and How »)*. Partant, une obligation de documentation devrait exister dans la législation. À titre de comparaison, l'art. 15 al. 4 OPDo prévoit en protection des données personnelles une obligation de documenter les violations (et les mesures y relatives). Une obligation similaire doit selon nous faire l'objet de la législation[1965].

1965 Ces informations pourraient figurer dans un SGSI. L'on pourrait par ailleurs se poser la question de savoir s'il est suffisant de prévoir cette obligation dans l'ordonnance ou si elle devrait figurer dans la loi.

Schéma 26 : les ajouts proposés quant à la communication et à la documentation

Réglementation actuelle

— Echanges d'informations dans la gestion d'une violation de la sécurité de l'information (art. 12 OSI)

Ajouts proposés

— Imposer une obligation de prévoir à l'avance les communications prévisibles lors d'un incident
— Introduire une obligation de documenter les mesures de sécurité et les éléments relatifs aux incidents de façon sécurisée, et prévoir sa durée de conservation

f. Le renvoi à l'état de la technique

1256 La loi pourrait, en complément des considérations susmentionnées, prévoir des renvois pour que les assujetties disposent de plus d'outils pour mettre en œuvre des mesures permettant de respecter les exigences minimales de cybersécurité découlant de l'approche fondée sur les risques. Les renvois sont envisageables également à des fins de simplification pour l'autorité législative quant à la réflexion à mener sur les aspects techniques. Un simple renvoi indirect, comme « selon l'état de la science et de la technique » est admissible[1966]. Un tel renvoi encourage le recours aux normes privées comme aide à l'interprétation des exigences minimales légales. Dans cette optique, le message doit préciser au moins quelques normes techniques reflétant, selon l'avis des autorités, l'état de la technique, ou d'autres précisions[1967].

1257 Pour accroître la souplesse du renvoi, il est possible de prévoir un renvoi dynamique indirect explicitement « recommandationnel »[1968], afin de préconiser aux assujetties de s'inspirer de l'état de la technique au lieu de les y assujettir[1969].

1966 Chf, *DTL*, 2013, N 122 ; OFJ, *Guide de législation*, 2019, N 752. Voir, pour un exemple, l'art. 10 al. 2 litt. c LPMA.

1967 OFJ, *Guide de législation*, 2019, N 752 ; SNV, *Le statut juridique des normes*, 2013, p. 4 ; FLÜCKIGER, p. 367 et 372. Par exemple, la suite de normes ISO 2700x, les cadres du NIST ou encore les normes BSI sont souvent citées internationalement ; pour plus d'informations sur ces normes, cf. *supra* N 366 ss.

1968 Le renvoi est recommandationnel lorsque la norme à laquelle il est renvoyé revêt la nature de simple recommandation à suivre, cf. FLÜCKIGER, p. 372.

1969 Cf. par exemple, en marchés publics, l'art. 30 al. 2 LMP, qui prévoit que « *dans la mesure où cela est possible et approprié, l'adjudicatrice fixe les spécifications techniques en se fondant sur des normes internationales ou, à défaut, sur des prescriptions techniques appliquées en Suisse, des normes nationales reconnues ou les recommandations de la branche* » ; FLÜCKIGER, p. 373.

Un renvoi dynamique semi-obligatoire serait plus précis que les deux alternatives de renvois indirects susmentionnées. Il présente autant de souplesse que le renvoi dynamique indirect explicitement recommandationnel. Le renvoi dynamique semi-obligatoire consiste en un renvoi à des normes internationales spécifiques desquelles les destinataires peuvent s'inspirer[1970]. 1258

Le renvoi indirect (explicitement recommandationnel ou non) offre le plus de flexibilité et est à privilégier. Il permet également aux entités sectorielles en Suisse d'adopter des normes qui seraient considérées comme l'état de la technique, comme ont commencé à le faire certains secteurs de l'approvisionnement du pays[1971]. 1259

g. L'utilisation d'une annexe ?

Finalement, l'on pourrait se demander s'il serait opportun de compléter la loi ou les ordonnances par une ou plusieurs annexes. En principe, elles peuvent servir d'aide-mémoire au sujet d'une procédure, ou servir à décrire des informations spécifiques à un domaine. Les annexes doivent être utilisées avec prudence afin d'une part de ne pas risquer de contredire la loi et d'autre part de s'assurer qu'elles sont bien nécessaires. Alors qu'une annexe de l'ordonnance relative aux infrastructures critiques assujetties à la proposition de loi semble cohérente, une annexe poursuivant comme unique but l'illustration du contenu de l'acte ne reviendrait pas à constituer la meilleure solution. Il serait plus approprié de diffuser l'information sous une autre forme, à l'instar de circulaires[1972]. 1260

4. Le contrôle de l'application de la législation

a. Les différents moyens de contrôler l'application de la législation

Différents mécanismes permettent de s'assurer de la conformité des assujetties avec les obligations prévues par une réglementation. Certains de ces mécanismes permettent aux assujetties de démontrer leur conformité avec les exigences de cybersécurité, d'autres habilitent des autorités à s'assurer de cette conformité. 1261

1970 FLÜCKIGER, p. 371 s. En revanche, nous n'abandonnons pas le sens de l'utilisation de renvois statiques ou dynamiques directs dans ce contexte, car l'utilisation de tels renvois serait problématique en relation avec l'acte auquel il est renvoyé, dans quelle version, avec quelles possibilités d'évolution et ainsi de suite ; pour plus d'informations au sujet de leur admissibilité, voir notamment ChF, *DTL*, 2013, N 138 ; OFJ, *Guide de législation*, 2019, N 758 ; SNV, *Le statut juridique des normes*, 2013, p. 3 s ; FLÜCKIGER, p. 366 ss.

1971 Ces normes comptent des normes payantes (comme les normes ISO), mais les renvois à des normes gratuites et, partant, plus accessibles (comme le cadre NIST), sont préférables.

1972 OFJ, *Guide de législation*, 2019, N 627 ss.

1262 Certains mécanismes permettent d'assurer en amont et durant l'exploitation des systèmes informatiques du respect des exigences minimales. La certification permet à ce titre d'attester d'un certain niveau de qualité et, en l'occurrence, de sécurité pour les systèmes exploités, tout en renforçant les capacités du marché. La certification doit coexister avec des moyens plus informels d'attester de la qualité pour respecter l'autonomie du marché[1973]. En effet, il faut d'une part permettre à toutes les organisations concernées de démontrer leur conformité aux exigences minimales de cybersécurité indépendamment de leurs ressources. D'autre part, il est judicieux d'attendre les décisions à venir des pays voisins en termes de certifications afin de ne pas se couper des marchés européens et internationaux.

1263 D'autres mécanismes doivent exister pour que les autorités compétentes puissent s'assurer activement du respect des exigences minimales. Ces autorités, qui doivent déjà être impliquées dans des mécanismes tels que la certification, doivent pouvoir mener des actes d'exécution. Il est à ce titre nécessaire que les autorités compétentes puissent concrétiser les attentes découlant des exigences minimales, mais aussi pour qu'elles puissent apporter leur soutien aux infrastructures critiques et qu'elles soient habilitées à effectuer ou à décider de contrôles ou encore prononcer des avertissements ou des sanctions.

b. La certification

1264 La certification est un outil qui favorise l'autoréglementation et le commerce. Cela étant, elle est en principe prévue par une loi[1974]. La certification doit être effectuée par un organisme indépendant reconnu par les autorités. La certification de sécurité consiste en une reconnaissance formelle, selon laquelle l'objet de la certification satisfait à des exigences légales et techniques, éprouvée à travers une évaluation par une tierce reconnue[1975].

1265 À titre de comparaison, plusieurs bases légales suisses prévoient des mécanismes de certification, tantôt facultatifs, tantôt contraignants. En matière de protection des données personnelles, les fournisseuses de systèmes de logiciels et de traitement de données peuvent, comme les personnes privées ou organes fédéraux traitant des données personnelles, soumettre leurs services, systèmes et processus à une certification (cf. art. 13 LPD concrétisé par l'Ordonnance sur les certifications en matière de protection des données,

1973 Les labels sont plus accessibles, mais bénéficient en principe d'une confiance moindre, cf. *infra* N 112.

1974 Cf. en comparaison avec la protection des données personnelles, CR LPD-FISCHER, art. 13 N 4 ; MEIER, N 1408. Pour des généralités au sujet des certifications, cf. *supra* N 110 ss.

1975 FF 2003 1915, p. 1948. Dans un ordre d'idées similaire, cf. SALAMON, p. 199.

OCPD). La certification est facultative et s'applique depuis la révision de la LPD aux services, en plus des produits[1976]. Elle porte sur les exigences de la LPD et de l'OPDo, parfois concrétisées par les directives complémentaires de la PFPDT, à l'instar des directives sur les exigences minimales qu'un système de gestion de la protection des données doit remplir). En termes de conséquences et outre un potentiel avantage concurrentiel, la certification entraîne dans ce contexte des conséquences légales. Elle fournit un indice du respect des exigences légales, en matière d'analyse d'impact ou de communication transfrontière des données[1977]. Afin d'assurer un caractère dynamique à la portée de la certification, ses conditions doivent être vérifiées chaque année par l'organisme de certification. Sa période de validité dure trois ans (art. 8 al. 2 OCPD)[1978]. En cas de manquements graves, l'organisme de certification peut suspendre ou révoquer la certification, par exemple si l'organisation au bénéfice de la certification utilise cette dernière de manière trompeuse ou abusive (art. 11 OCPD)[1979].

L'UE a également adopté une approche pour appréhender la question 1266
de la certification, cette fois plus précisément pour la cybersécurité. Certains schémas pour des produits TIC ou des services TIC peuvent être reconnus par les autorités, comme c'est le cas au sein de l'UE conformément au Règlement (UE) 2019/881. Par ailleurs, l'UE prescrit que l'utilisation de produits ou services TIC certifiés conformément aux schémas européens de l'art. 49 Règlement (UE) 2019/881 peut permettre de démontrer la conformité aux obligations de cybersécurité des infrastructures critiques (art. 24 Directive SRI2)[1980]. Un tel raisonnement devrait être mené en Suisse, car il permettrait d'une part d'assurer la confiance dans les produits et services fournis par une prestataire de gestion de cyberincidents et, d'autre part, de démontrer pour les infrastructures critiques le respect des exigences minimales de cybersécurité[1981].

Admettre un mécanisme légal de certification permettrait d'attester de 1267
manière plus officielle de la conformité à des exigences légales et techniques. Dans la mesure où la certification doit attester de la conformité à des exigences,

1976 OFJ, *Rapport explicatif OCPD*, 2022, p. 3.

1977 CR LPD-FISCHER, art. 8 N 27 ss.

1978 CR LPD-FISCHER, art. 13 N 58 ss. En revanche, un objet certifié peut faire l'objet d'un traitement de données personnelles non conforme à la loi, cf. HUSI-STÄMPFLI/MORAND, p. 150.

1979 CR LPD-FISCHER, art. 13 N 63 ; OFJ, *Rapport explicatif OCPD*, 2022, p. 11.

1980 L'EUCC, un premier schéma européen de certification de cybersécurité, a été créé pour reconnaître officiellement que les produits TIC peuvent être fiables durant l'entier de leur cycle de vie.

1981 Il reste important d'attendre de voir les schémas qui seront reconnus dans l'UE pour faciliter le marché entre la Suisse et l'UE.

il est nécessaire de se poser la question des exigences à respecter. Formellement, la loi doit prévoir les exigences et la certification, de façon comparable à ce qui existe en protection des données personnelles. Il faudrait spécifiquement que les certifications permettent de garantir le respect des exigences minimales de cybersécurité de la LSI en termes de cybersécurité par défaut et dès la conception, ou en matière de gestion de cyberincidents. La faculté devrait en outre être accordée à l'OFCS d'édicter dans des directives d'autres critères spécifiques pour les systèmes, produits ou services, avec la possibilité de s'inspirer de normes internationales reconnues (comme le fait la PFPDT avec ses directives sur la certification de l'organisation et de la procédure conformément à l'art. 7 al. 2 OCPD[1982]). À noter que la certification est accordée à un moment donné et il est difficile de s'assurer du respect permanent des exigences applicables, raison pour laquelle des mécanismes évolutifs et dynamiques doivent pouvoir exister[1983]. Les certifications ne doivent pas se limiter à des listes avec des cases à cocher, mais doivent au contraire être agiles et dynamiques pour permettre de s'adapter aux évolutions technologiques et de garantir en tout temps des processus appropriés et conformes au droit[1984]. Cela peut être appréhendé par un fonctionnement similaire à ce qui prévaut en protection des données personnelles avec un contrôle annuel du respect des exigences ainsi qu'une durée de trois ans maximum (art. 11 OCPD) ainsi qu'une éventuelle vérification prévue lors de changements importants de pratiques ou de risques[1985].

1268 Une certification facultative devrait être envisagée en Suisse, à l'instar de ce qui existe en protection des données personnelles. Une certification facultative permettrait au marché de continuer à se développer dans une perspective d'autoréglementation. Elle ne doit pas empêcher l'utilisation d'autres instruments plus souples comme l'évaluation ou la labellisation permettant aux organisations en pratique de garantir un certain niveau de prestations de sécurité informatiques. La LSI doit prévoir une telle possibilité, comme la LPD le fait à son art. 13, prévoyant une possibilité de recourir à une certification pour des prestations de services comme de fourniture de produits ou de systèmes.

1982 CR LPD-FISCHER, art. 13 N 55 ; voir PFPDT, *Directives sur la certification de l'organisation et de la procédure,* 2014.

1983 De façon analogue en protection des données personnelles, cf. CR LPD-FISCHER, art. 13 N 30.

1984 Les certifications doivent aussi se baser sur le modèle « PDCA » *(Plan, Do, Check, Act),* cf. de façon analogue en protection des données, CR LPD-FISCHER, art. 13 N 35.

1985 À noter qu'il faudra le cas échéant fixer les conséquences de la certification, à savoir si elle équivaut à une présomption de conformité aux exigences minimales, si elle constitue simplement un indice de respect des exigences et si d'autres avantages légaux ou pratiques peuvent découler d'une certification.

La compétence du CF (voire de l'OFCS) doit être prévue pour fixer les modalités de ce mécanisme. Une ordonnance similaire à l'OCPD devrait également être adoptée pour, justement, fixer les dispositions relatives aux certifications et à l'accréditation d'organismes.

Compte tenu de la pratique et du souhait des infrastructures critiques[1986], le mécanisme de certification doit être facultatif, du moins dans un premier temps[1987]. De nombreuses infrastructures critiques souhaitent que la certification ne soit pas réglementée de façon contraignante, souhait qui peut être exaucé par le caractère facultatif de la certification[1988]. Ensuite, l'OFCS devrait, en qualité d'autorité principale pour la cybersécurité, être associé à la procédure d'accréditation comme au contrôle ainsi qu'à la suspension et à la révocation des organismes procédant à la certification (comme l'est la PFPDT à l'art. 2 OCPD)[1989]. Les compétences du Service d'accréditation suisse (SaS) et de l'association suisse de normalisation (SNV) devraient également être mobilisées au cours du processus. L'on pourrait réfléchir à une certification étatique, mais les initiatives privées étant privilégiées, cela reviendrait à une intrusion importante[1990]. 1269

Comme susmentionné, la certification facultative peut coexister avec d'autres processus d'évaluation plus informels, qui ne présenteront probablement pas les mêmes avantages, mais qui pourront être plus accessibles aux organisations ne disposant pas des ressources leur permettant de certifier leurs processus, services, produits ou systèmes[1991]. 1270

1986 KNIEPS et al., p. 23.

1987 Une certification obligatoire constituerait à ce stade une intrusion disproportionnée dans le marché.

1988 KNIEPS et al., p. 23.

1989 CR LPD-FISCHER, art. 13 N 33 ; MEIER, N 1412. L'on pourrait réfléchir à des entités telles que le NTC, dont le mandat initial présentait un intérêt dans des contextes comme ceux des logiciels utilisés par des infrastructures critiques. La limitation de son mandat à l'analyse d'applications pourrait diminuer l'intérêt qu'une telle entité pouvait initialement présenter pour la cybersécurité auprès des infrastructures critiques raison pour laquelle il nous semblerait important soit de revenir à son mandat initial soit de se concentrer sur d'autres entités. Sur le NTC, cf. *supra* N 345.

1990 De même que ce qui a été convenu en protection des données personnelles, cf. CR LPD-FISCHER, art. 13 N 32.

1991 Par exemple, toute organisation peut créer son propre label, mais ce label n'offre pas la confiance qu'offre une certification. Il existe en cybersécurité différents labels suisses, comme par exemple le label CyberSeal, qui confirme qu'une prestataire IT met en œuvre les mesures techniques et organisationnelles nécessaires pour assurer la cybersécurité chez ses clientes ou, de façon plus générale, le label Cybersafe, tous deux reconnus comme des efforts coordonnés par l'OFCS, cf. Page d'accueil OFCS > Informations pour les autorités > Informations complémentaires / Liens.

c. Les mesures d'exécution par l'Office fédéral de la cybersécurité

1271 Le nouvel OFCS est l'autorité idéale pour contrôler l'application de la législation centrale. L'OFCS est le résultat de la transformation du NCSC, qui disposait déjà des compétences principales pour la cybersécurité en Suisse. Le NCSC participait tout d'abord à l'élaboration, à la formalisation et à la mise en œuvre de la politique publique de cybersécurité. Ensuite, le NCSC occupait une fonction incitative par le biais de ses conseils et de son assistance. Finalement, il pouvait prendre et réaliser un certain nombre d'actions qui pourraient difficilement être laissées à la charge d'autres actrices de cet écosystème, à l'instar de la publication de vulnérabilité selon l'art. 73*c* LSI2.

1272 La création du service spécialisé de la Confédération pour la sécurité de l'information amène de l'opacité dans la délimitation entre les compétences des deux nouvelles autorités. Le nouveau service spécialisé est compétent pour la sécurité de l'information et la sécurité des moyens informatiques auprès des autorités et organisations de la Confédération. Il devrait pouvoir compter sur les compétences techniques de l'OFCS notamment sur les questions de cybersécurité. L'OFCS demeure en outre responsable de réceptionner les signalements relatifs aux cybermenaces[1992]. Partant, l'OFCS devrait pouvoir occuper les fonctions de l'ancien NCSC en lien avec la cybersécurité des infrastructures critiques. L'OFCS devrait typiquement pouvoir apporter du soutien et fournir des conseils aux infrastructures critiques soumises aux exigences minimales de cybersécurité.

1273 D'autres mesures, plus strictes, devraient être envisagées. Le droit européen sert de source d'inspiration aux art. 32 ss Directive SRI2. Les art. 32 s. Directive SRI2 habilitent les autorités compétentes dans les États membres à procéder à diverses mesures de supervision à l'instar d'inspections sur place et contrôles (aléatoires ou non) à distance, d'audits de sécurités réguliers et ciblés (réalisés par une autorité compétente ou un organisme indépendant), des audits *ad hoc* en cas d'incidents importants ou de violations de la directive ou encore des demandes d'accès à des données nécessaires à l'accomplissement de leurs tâches (art. 32 par. 2, 33 par. 2 Directive SRI2). Elles sont aussi habilitées à prendre des mesures d'exécution prononçant des avertissements ou des ordres pour que les infrastructures soumises à sa surveillance mettent un terme à des violations de la directive ou qu'elles mettent en œuvre les recommandations formulées à la suite d'un audit (art. 32 par. 4, 33 par. 4 Directive SRI2). Il est nécessaire que le nouvel office suisse détienne des compétences

1992 SG-DDPS, *Législation d'exécution relative à la LSI, Explications,* 2023, p. 6.

similaires pour pouvoir d'une part accompagner les infrastructures critiques dans leur mise en œuvre des exigences minimales et d'autre part contrôler la bonne mise en œuvre.

Il est également possible de s'inspirer des compétences d'enquête de la PFPDT en matière de protection des données personnelles en Suisse (voir art. 49 ss LPD). Bien que le NCSC ait initialement constitué une autorité d'accompagnement plutôt qu'une autorité de surveillance, l'introduction de l'obligation de signaler les cyberattaques l'a placé à mi-chemin entre une autorité de soutien et une autorité de surveillance. Cette nouvelle posture permet de confier au nouvel office pour la cybersécurité une réelle mission de surveillance, tout en accompagnant les organisations sous son contrôle. 1274

d. Les sanctions

Outre ces mesures, les violations des exigences minimales de cybersécurité doivent être passibles de sanctions. Ces dernières vont exister déjà dans la LSI2 pour les violations de l'obligation de signaler une cyberattaque en vertu des art. 74*a* ss LSI2, plus précisément à l'art. 74*h* LSI2. Les art. 74*g* s. LSI2 prévoient un processus triptyque. La première étape est l'information par l'OFCS de l'organisation en cas d'indices que l'obligation de signaler n'est pas respectée (art. 74*g* al. 1 LSI2). La seconde étape est celle de la décision de l'OFCS avec un délai pour se conformer et la menace d'une amende en cas de non-conformité (art. 74*g* al. 2 LSI2). La troisième étape a lieu si l'organisation ne se conforme toujours pas à son obligation et consiste en la saisie par l'OFCS des autorités de poursuite pénale qui infligent une amende à l'organisation qui ne se conforme pas à la décision de l'OFCS (art. 74*h* LSI2)[1993]. Bien que la loi puisse prévoir une infraction spécifique et directe en cas de violation des exigences minimales de cybersécurité, la collaboration souhaitée entre l'OFCS et les infrastructures critiques et le principe de proportionnalité[1994] impliquent qu'il est préférable de prévoir plusieurs étapes comme ce qui existe en cas de violation de l'obligation de signaler les cyberattaques. Les sanctions doivent par ailleurs s'appliquer aux manquements intentionnels[1995]. 1275

Les dispositions pénales doivent permettre l'application du droit pénal administratif, dans la mesure où les infractions dans ce cadre sont fortement 1276

1993 FF 2023 84, p. 46 ss ; MEYER/MÉTILLE, *Loi fédérale sur la sécurité de l'information : version 2.0*, 2022, N 57.

1994 Au sujet du principe de proportionnalité dans ce contexte, OFJ, *Guide de législation*, 2019, N 890.

1995 En prévoyant par exemple une norme pénale similaire à l'art. 61 litt. c LPD qui sanctionne la personne qui ne respecte pas les exigences minimales en matière de sécurité des données édictées par le CF en vertu de l'art. 8 al. 3 LPD.

susceptibles de pouvoir être imputées à des personnes morales[1996]. Bien que les autorités législatives suisses soient fréquemment réticentes à introduire des amendes administratives aux organisations privées[1997], nous ne pouvons qu'encourager ces sanctions dans un domaine comme celui de la cybersécurité auprès des infrastructures critiques, comme ce qui existe à l'art. 60 LTC ou, en Europe, à l'art. 34 Directive SRI2 pour la cybersécurité ou à l'art. 82 s. RGPD en protection des données[1998].

E. Une conclusion sur la portée de cette solution

1. En résumé

1277 L'introduction d'exigences minimales légales transversales pose des questions relatives à la compétence législative fédérale, nécessaire pour permettre à la Confédération d'adopter une loi applicable aux infrastructures critiques. Ces dernières doivent ensuite pouvoir être sujettes à des réglementations différenciées selon les réglementations sectorielles et sous-sectorielles, contraignantes ou non contraignantes, leur étant spécifiquement applicables.

1278 Une loi doit nécessairement exister. La LSI sert de base légale adéquate, si ce n'est idéale pour adopter ces obligations, bien qu'une loi séparée puisse également être adoptée. La LSI est la loi centrale en sécurité de l'information et de sécurité informatique, ce qui en fait la loi principale pour la cybersécurité. Elle prévoit déjà des exigences minimales applicables à certaines infrastructures critiques et sa nouvelle obligation de signaler les cyberattaques s'appliquera à un cercle plus étendu d'infrastructures critiques.

1279 La LSI doit, en tant que loi au sens formel, contenir les dispositions importantes. Elle doit être concrétisée par une ordonnance. Outre l'OSI, nous estimons que le nouvel office pour la cybersécurité, autorité principale dans ce domaine, doit être en mesure d'adopter des ordonnances contraignantes ainsi que des instruments de droit souple pour guider les organisations assujetties dans la mise en œuvre de la loi et pour permettre une certaine agilité à cette réglementation à vocation évolutive.

1996 OFJ, *Guide de législation*, 2019, N 883. À noter qu'en parallèle, l'art. 102 CP demeure naturellement applicable, OFJ, *Guide de législation*, 2019, N 885.

1997 Voir pour un autre exemple le débat durant la révision de la LPD, cf. FF 2017 6565, p. 6597 et 6713 ss.

1998 À noter également que d'autres questions liées aux sanctions devraient être appréhendées, à l'instar de la responsabilité des autorités de l'administration fédérale. En protection des données personnelles notamment, les organes fédéraux ne peuvent pas se voir infliger une sanction en cas de non-respect d'une décision de la PFPDT, cf. MÉTILLE/MEYER, p. 32.

Il est délicat de prévoir le contenu complet de la réglementation proposée dans le cadre d'une étude telle que la présente. Il est tout de même possible de répondre aux questions centrales que pose une telle réglementation, à commencer par son champ d'application personnel. Les exigences minimales de la loi doivent s'appliquer aux infrastructures critiques les plus importantes en Suisse. Un niveau minimal harmonisé et uniforme en Suisse est aujourd'hui nécessaire. Les exigences minimales doivent se fonder sur ce que la LSI et l'OSI prévoient déjà et elles doivent être perfectionnées sur cette base pour mieux prendre en compte la gestion de cyberincidents dans ses différentes étapes. La LSI et son ordonnance constituent un fondement déjà complet qui permet, par quelques ajouts et modifications de fond, de bien appréhender les comportements que doivent adopter les infrastructures critiques pour assurer un niveau minimal suffisant de cybersécurité, surtout si les autorités compétentes conservent leur compétence de compléter la réglementation par d'autres actes d'exécution. 1280

2. Les conséquences positives

L'adoption d'une législation transversale permettrait tout d'abord d'assurer plus de clarté, de sécurité juridique et de prévisibilité du droit pour les assujetties[1999]. 1281

Ensuite, le fait de centraliser davantage la réglementation permettrait d'harmoniser à un niveau adéquat un droit actuellement particulièrement disparate et déséquilibré entre les différents secteurs et soussecteurs critiques ainsi qu'entre les infrastructures critiques. Cette solution permettrait d'assurer une unité matérielle qu'une réglementation sectorielle pourrait difficilement atteindre[2000]. La loi fixerait un niveau minimal transversal de cybersécurité, ce qui illustre aussi une volonté de la Confédération de se saisir de la problématique de la cybersécurité des infrastructures critiques sur le plan réglementaire. Une telle solution, si elle comprend une législation centralisée et des compléments de réglementation sectoriels, permettrait aussi de respecter le fédéralisme et les compétences cantonales ainsi que l'autonomie sectorielle. Elle ne causerait pas d'atteinte à l'autonomie et à l'autoréglementation dans la mesure où les entités compétentes présentement ne verraient pas leurs compétences volées par la Confédération. 1282

Aussi, cette solution permettrait de clarifier le rôle du nouvel office, de ne pas alourdir les processus auprès du pouvoir législatif avec une nouvelle loi. 1283

1999 Sur l'importance de lois plus uniformes et moins exigeantes pour les assujetties, cf. notamment SOLOVE/HARTZOG, p. 197 s.

2000 OFJ, *Guide de législation*, 2019, N 598.

Elle éviterait également la surcharge des autorités de surveillance sectorielles, ce qui impliquerait une centralisation des compétences, une facilitation de la collecte d'information et une simplification des processus.

1284 Finalement, cette solution entraînerait des conséquences plus étendues en permettant d'appréhender d'autres questions que l'autorité législative se pose actuellement. Si la proposition législative susmentionnée d'introduire des exigences minimales légales de cybersécurité est adoptée, un ensemble de technologies serait réglé légalement. Il en irait de la sorte pour la sécurité des informations et des moyens informatiques lors du recours par les infrastructures critiques à des processus algorithmiques, pour la sécurité de l'exploitation qu'elles font d'objets industriels connectés, ou encore pour la responsabilité de ces infrastructures dans leur utilisation de solutions infonuagiques[2001].

3. Les défis dans une perspective critique

1285 Le passage d'une réglementation actuellement décentralisée à une réglementation totalement centralisée semble utopique et questionnable car cela revient à un changement des pratiques réglementaires en Suisse dans ce domaine. C'est pourquoi un système mixte est de loin préférable à une unique loi centrale. En effet, s'il n'existait qu'une réglementation centrale et unique au niveau fédéral sans possibilités pour les cantons de légiférer davantage, le principe de subsidiarité risquerait d'être violé (art. 5*a* et 43a Cst.). Il est impensable de nos jours d'adopter une quelconque législation dans un domaine hautement libéralisé sans prendre en compte les différentes personnes impactées par la réglementation, dont les autorités sectoriellement compétentes, les associations professionnelles et les organisations assujetties[2002]. Le respect de l'autonomie sectorielle et du principe de subsidiarité représente donc un enjeu de taille à garantir.

1286 Dans le cadre de la solution telle qu'elle est proposée, la densité normative constitue un défi. La vitesse des processus législatifs en comparaison avec les avancées technologiques et pratiques constitue systématiquement un défi de taille lorsqu'il s'agit de réglementer sur des questions relatives au cyberespace. La loi doit fixer les exigences minimales applicables aux infrastructures critiques au moins dans leur principe, sans aller dans des détails superflus qui ne seraient plus adaptés à la pratique d'ici peu[2003]. La possibilité

2001 Sur ces technologies et sur la responsabilité des fournisseuses de services informatiques dans ce contexte, cf. *supra* N 147 ss ; sur la portée des propositions de la présente étude à ce sujet, cf. *infra* N 1367 ss.

2002 Dans un ordre d'idées comparable, SALAMON, p. 253.

2003 Dans un sens similaire, SOLOVE/HARTZOG, p. 51 ss.

pour le CF, l'OFCS et les entités sectorielles compétentes d'adopter des actes d'exécution doit permettre de limiter les effets indésirables découlant de cette problématique.

De la même manière que les autres législations émergentes imposant des 1287
obligations et des mécanismes de contrôle de l'application des prescriptions, la solution proposée va de pair avec une mobilisation de ressources tant auprès des assujetties qu'auprès des autorités compétentes pour l'application de la réglementation.

Finalement, les échanges entre l'OFCS et les infrastructures critiques 1288
deviennent plus rigides, passant d'un échange volontaire à une obligation de signaler certaines cyberattaques en vertu des art. 74*a* ss LSI2. Avec cette formalisation des échanges, il y a un risque que moins d'informations soient partagées, déjà à l'interne des organisations, afin de ne pas alerter l'OFCS en cas de mauvaises pratiques de sécurité, notamment pour des questions de réputation. Si des exigences minimales sont introduites, ce risque sera vraisemblablement plus élevé car une sanction pourrait tomber en cas de violation des exigences minimales. Cette situation pourrait conduire à une vue d'ensemble moins complète pour le nouvel office pour la cybersécurité. Cela étant, l'OFCS devant en contrepartie soutenir les infrastructures critiques, la cybersécurité des infrastructures critiques devrait finalement s'en trouver améliorée.

III. Une conclusion au chapitre 9

L'amélioration de la cybersécurité des infrastructures critiques doit passer 1289
par la réglementation et l'adoption d'exigences minimales de cybersécurité applicables à ces autorités et organisations. Deux pistes réglementaires sont envisageables à cette fin. La première consiste en l'approche suivie dans la CSN. Elle consiste en l'examen en tout temps des lacunes et des besoins réglementaires et le comblement des lacunes constatées le cas échéant. La seconde réside dans l'introduction d'exigences minimales légales de cybersécurité applicables de façon transversale aux infrastructures critiques.

La première alternative réglementaire est celle suivie par le CF dans la 1290
CSN de 2023, qui suppose l'examen en tout temps des besoins en termes de réglementations pour les infrastructures critiques et pour différentes technologies (I.A). Lorsque des lacunes légales sont à déplorer, il faut les combler. Cette alternative se fonde sur les récents développements législatifs et réglementaires (I.B). À ce titre, l'adoption et la révision de la LSI forment des étapes importantes. Le secteur de l'approvisionnement en énergie fait l'objet de diverses modifications de lois et d'ordonnances pour mieux inciter les organisations

actives dans le secteur à assurer leur cybersécurité. D'autres secteurs disposent d'instruments plus ou moins contraignants (I.C). Dans la mesure où des exigences minimales de cybersécurité n'existent pas pour toutes les infrastructures critiques, il est tout d'abord nécessaire de savoir à quelles organisations les exigences fragmentées devraient s'appliquer et s'assurer qu'aucune organisation ne passe entre les mailles du filet. Il faut ensuite que les exigences soient suffisantes, claires, aptes à évoluer et, dans la mesure où c'est nécessaire, harmonisées. Des ressources doivent finalement exister pour que les autorités d'application des lois puissent contrôler la conformité des infrastructures critiques aux exigences (I.D).

1291 Cette alternative permet d'éviter une ingérence réglementaire importante par l'adoption d'une loi centralisée au niveau de la Confédération. Le principe de subsidiarité et l'autonomie sectorielle sont ainsi aisément garantis. Les spécificités sectorielles sont prises en compte et la manière de procéder est cohérente avec les développements réglementaires menés jusqu'à présent. En revanche, certaines infrastructures critiques risquent d'être soumises à des exigences de cybersécurité insuffisantes et un clivage non négligeable entre le niveau attendu par certains cantons pour les infrastructures critiques soumises à leur compétence risque d'exister. Nous serions là face à un risque qui n'est pas acceptable. Cette manière de procéder est par ailleurs particulièrement longue et risque de conduire à un manque de clarté plus important pour les organisations qui ne sauront pas à quelles exigences elles sont soumises en raison de la fragmentation de celles-ci. Finalement, il est à prévoir que plusieurs autorités sectoriellement compétentes pour contrôler l'application de la loi manquent des ressources pour s'assurer de la conformité des assujetties à des exigences de cybersécurité (I.E).

1292 La seconde alternative consiste en l'introduction d'exigences minimales légales de cybersécurité applicables aux infrastructures critiques. L'adoption d'une loi transversale est une solution digne d'être examinée. En effet, le niveau d'exigences de cybersécurité varie en fonction des sous-secteurs critiques et évolue à des rythmes variés, les processus réglementaires prennent du temps et l'unité matérielle de la loi justifie que l'on se penche sur la possibilité d'introduire des exigences légales transversales (II.A). La Confédération peut se fonder sur ses compétences constitutionnelles pour légiférer en la matière bien que plusieurs fondements soient envisageables et en dépit des controverses. Elle peut à ce titre se fonder sur les bases constitutionnelles servant déjà à la LSI et l'art. 57 Cst. devrait y être ajouté (II.B). L'intégration de ces exigences minimales dans la LSI est la solution idéale bien qu'il soit également envisageable d'adopter une nouvelle loi applicable uniquement aux infrastructures critiques. La loi doit en tout cas être accompagnée d'actes d'exécution. Le CF

dispose de la compétence d'adopter une ordonnance, mais l'OFCS doit selon nous également disposer d'une telle compétence. L'OFCS et les autorités sectorielles doivent en outre avoir la possibilité d'adopter des actes de droit souple pour concrétiser la loi (II.C). La LSI doit prévoir les dispositions importantes, en particulier les définitions, le champ d'application des exigences (qui soulève la question de la définition de la notion d'infrastructure critique) ainsi que les obligations principales. En revanche, il revient aux actes d'exécution de prévoir les mesures concrètes. En effet, les actes d'exécution revêtent une densité normative plus forte qu'une loi et peuvent plus rapidement être adaptés aux évolutions technologiques par exemple. La loi doit prévoir des mécanismes de contrôle de l'application de la loi, à l'instar d'un mécanisme de certification facultative. L'OFCS est l'autorité d'application de la loi idéale susceptible de prendre des mesures d'exécution. Des sanctions doivent finalement pouvoir être prononcées afin que les infrastructures critiques soumises aux exigences soient dissuadées de ne pas s'y conformer (II.D).

Cette alternative permet plus de clarté et de prévisibilité juridique pour 1293
les organisations. En effet, elles peuvent savoir si elles sont des infrastructures critiques, si elles sont soumises aux exigences et les lois centralisées sont en général plus connues par les organisations. En outre, l'introduction d'exigences minimales légales transversales de cybersécurité permettrait une meilleure harmonisation du niveau attendu entre les différentes organisations et les différents secteurs et sous-secteurs critiques. Cette alternative conduit à la clarification du rôle de l'OFCS et doit permettre la mobilisation de ses ressources. En revanche, certains défis existent et doivent être surmontés par l'introduction de ces exigences. Premièrement, le principe de subsidiarité de l'intervention réglementaire de la Confédération doit être respecté et l'autonomie sectorielle doit être garantie dans la mesure du possible. C'est pourquoi la législation centralisée doit laisser la possibilité aux cantons d'aller plus loin et aux secteurs de concrétiser les exigences transversales en fonction des besoins et des spécificités. Deuxièmement, la sécurité juridique peut faire l'objet de tensions entre l'exigence de prévisibilité de la loi et de son adaptabilité. Pour apaiser ces tensions, il est nécessaire qu'une loi prévoie des exigences minimales, mais que celles-ci soient concrétisées dans des actes d'exécution plus aptes à s'adapter rapidement aux évolutions technologiques notamment. Troisièmement, les ressources de nombreuses intervenantes vont être nécessaires, ce qui implique un budget et la mobilisation des moyens nécessaires. Quatrièmement, l'OFCS devra s'assurer de maintenir une certaine confiance de la part des infrastructures critiques en dépit des changements organisationnels pour la cybersécurité au sein de la Confédération et en dépit du renforcement de son rôle d'autorité de surveillance (II.E).

1294 L'introduction d'exigences minimales légales de cybersécurité pour les infrastructures critiques est préférable à la réglementation ponctuelle comme imaginée par la CSN. Les exigences minimales doivent être centralisées. La centralisation des compétences de cybersécurité a commencé et il est maintenant temps d'assumer cette prise de position qui doit conduire à une amélioration de la cybersécurité des infrastructures critiques. Celles-ci sont les premières responsables de leur cybersécurité, mais elles ne sont pas les uniques responsables. Elles font souvent appel à l'interne ou à l'externe à des expertes en gestion de cyberincidents, en cybersécurité et en informatique en général. Ces prestataires doivent également assumer leur part de responsabilité. En outre, l'introduction d'exigences minimales légales de cybersécurité applicables aux infrastructures critiques implique la mobilisation de l'OFCS de façon importante, raison pour laquelle son mandat et celui de son équipe d'intervention, GovCERT, doivent être analysés.

Chapitre 10 : les solutions ciblant les prestataires de gestion de cyberincidents

Préambule au chapitre 10

1295 La pratique des prestataires de gestion de cyberincidents n'est pas spécifiquement réglementée à l'heure actuelle. Leur activité est néanmoins nécessaire à d'autres organisations, dont les infrastructures critiques. La loi appréhende certains aspects de leur activité en raison de leur statut d'infrastructure critique, ainsi qu'en fonction de leur clientèle ou des prestations qu'elles fournissent. Certaines bénéficiaires de prestations sont soumises à des exigences de cybersécurité qui lient leurs prestataires de sécurité informatique. Le droit des contrats ou des marchés publics permettent aux clientes de prestataires de gestion de cyberincidents de régler certains aspects de l'activité notamment en termes de diligence. En cas d'actes illicites, les expertes informatiques peuvent engager leur responsabilité. Elles sont susceptibles d'être soumises à d'autres obligations, notamment si elles fabriquent des produits, matériels ou logiciels informatiques, ou si elles traitent certains types d'informations spécifiques, à l'instar de données personnelles ou d'informations couvertes par des secrets[2004].

1296 Force est de constater que la loi appréhende de façon plus réactive que proactive la cybersécurité de ces prestataires. La présente étude a démontré la nécessité de réglementer la cybersécurité des infrastructures informa-

2004 Cf. *supra* N 619 ss.

tiques et de l'activité des prestataires de gestion de cyberincidents selon une approche *ex ante*. Les prestataires de gestion de cyberincidents sont des infrastructures critiques et doivent être soumises aux exigences minimales légales de cybersécurité proposées dans le chapitre 9[2005]. Le présent chapitre part de ce postulat. Elles doivent être soumises à des exigences supplémentaires en raison de leur statut d'infrastructure critique, de leur importance pratique et de leur double casquette. Comme nous le verrons, les exigences auxquelles doivent être soumises ces fournisseuses de services informatiques doivent servir d'incitations non pas seulement pour la cybersécurité des moyens informatiques exploités par la prestataire de gestion de cyberincidents et des informations qu'elle traite, mais également pour les prestations qu'elle fournit.

1297 Les prestataires de gestion de cyberincidents ont une double casquette : la première en tant qu'infrastructure critique, la seconde en tant que fournisseuse de prestations notamment à d'autres infrastructures critiques (I.A). Les prestataires de gestion de cyberincidents font partie des organisations offrant des services informatiques qui bénéficieraient, en tant qu'infrastructures critiques, à être soumis aux exigences minimales de cybersécurité du chapitre 9 ainsi qu'à des exigences supplémentaires. L'ensemble des organisations actives dans le sous-secteur critique des services informatiques est en effet confronté à des questions similaires en termes de cybersécurité dans leurs prestations. Les exigences légales de cybersécurité supplémentaires proposées dans ce chapitre doivent en outre s'appliquer aux fournisseuses de services informatiques et, plus précisément, aux prestataires de gestion de cyberincidents indépendamment de leur structure ou des prestations qu'elles fournissent. Pour que ces exigences de cybersécurité puissent être adoptées par la Confédération, il est nécessaire que cette dernière puisse se prévaloir d'une compétence constitutionnelle (I.B). Il conviendra d'examiner dans quelle base légale ces exigences doivent figurer (I.C) ainsi que leur contenu (I.D). Des mécanismes de contrôle doivent exister pour que l'autorité compétente puisse s'assurer de la conformité des organisations assujetties aux exigences (I.E).

1298 La situation est différente pour l'OFCS et la CERT qu'elle exploite, GovCERT. L'OFCS étant un organe fédéral, son activité doit être réglementée de façon séparée (II.A). Gouverné par le principe de la légalité, l'OFCS doit baser son activité sur la loi. La loi est en pleine révision, l'OFCS est un nouvel office qui remplace l'ancien NCSC et qui continue d'héberger GovCERT. Les bases légales pour son activité doivent tenir compte de ces éléments. (II.A). Les propositions législatives du présent chapitre cherchent à appréhender et à améliorer des compétences du nouvel OFCS compte tenu de la pratique de GovCERT,

2005 Cf. *supra* N 1145 ss.

en s'inspirant du droit européen (II.C). L'autorité principale pour la cybersécurité en Suisse doit s'appuyer sur des bases légales plus claires pour ses compétences de soutien et de réglementation, mais il est surtout essentiel qu'elle puisse mieux investir son nouveau rôle d'autorité de surveillance (II.D).

I. La réglementation des prestataires de gestion de cyberincidents

A. La raison à l'origine d'une réglementation de ces prestations

1. La double casquette des prestataires de gestion de cyberincidents

1299 Les prestataires de gestion de cyberincidents revêtent deux casquettes : une casquette d'infrastructure critique et une autre en tant que fournisseuse de diverses prestations utilisées par l'ensemble des infrastructures critiques et par toute l'économie. En d'autres termes, elles font partie des infrastructures critiques reconnues en Suisse et peuvent être la cible d'attaques ou subir des incidents. Ces organisations spécialisées peuvent aussi faire l'objet d'attaques ciblant une autre organisation finale. Elles ont finalement un statut particulier en ce qu'elles soutiennent les efforts d'autres infrastructures pour prévenir, détecter les cyberincidents et y réagir[2006].

1300 Compte tenu de ce qui précède, non seulement leurs systèmes informatiques et leurs processus doivent faire l'objet d'une protection, mais aussi les produits et les services qu'elles fournissent à des tierces. Bien que les deux se recoupent parfois, la sécurité informatique assurée en son sein ne revient pas forcément à assurer celle des produits et de services offerts à ses clientes (critiques ou non). Une limitation à l'adoption d'exigences minimales pour les infrastructures critiques est donc insuffisante. Les fournisseuses de services informatiques, en particulier de services numériques de sécurité (comprenant les prestataires de gestion de cyberincidents), doivent répondre à des exigences supplémentaires pour assurer que leurs prestations sont sécurisées, en particulier lorsqu'elles sont destinées à d'autres infrastructures critiques.

2. Des fournisseuses de services informatiques

1301 De prime abord, la question de la réglementation des prestataires de gestion de cyberincidents se pose comme telle. Toutefois, ces prestataires font partie d'un sous-secteur critique qui est le sous-secteur des services informatiques.

2006 Pour une réflexion similaire en droit européen, cf. c. 86 Directive SRI2.

Partant, il faut se demander si les particularités relatives à l'activité des prestataires de gestion de cyberincidents leur sont spécifiques ou si la cybersécurité des prestations fournies par l'ensemble des fournisseuses services informatiques pourrait bénéficier d'une réglementation plus complète en matière de cybersécurité.

Le sous-secteur des services informatiques comprend selon la Stratégie PIC les « services informatiques à l'attention de l'économie (en particulier traitement et stockage de données) »[2007]. Ce sous-secteur englobe les processus relatifs à la sécurité informatique, à la maintenance, ou encore au fonctionnement des systèmes informatiques, des logiciels et du matériel informatiques (*softwares* et *hardwares*)[2008]. 1302

Les exigences minimales en matière de cybersécurité proposées au chapitre 9 doivent être applicables à l'ensemble des infrastructures critiques, dont font partie les fournisseuses de services informatiques. L'introduction de telles exigences vise la cybersécurité, la sécurité de l'information et les systèmes informatiques des services informatiques, mais pas particulièrement les produits et services informatiques fournis à leur clientèle (en dehors de leurs traitements d'informations par le biais de moyens informatiques). Les organisations opérant dans ce sous-secteur critique ne se limitent pas uniquement aux prestataires de gestion de cyberincidents. Elles jouent un rôle en tant qu'infrastructure critique et un autre en tant que fournisseuse de diverses prestations informatiques. 1303

Bien que les solutions examinées se concentrent sur les prestataires de gestion de cyberincidents, les mêmes exigences pourraient être applicables à toutes les prestataires de services informatiques, sans se limiter aux services numériques de sécurité. Partant, afin de couvrir un maximum de situations, la présente étude va inclure dans la mesure du possible l'ensemble des fournisseuses de services informatiques dans la proposition législative. 1304

3. Les différentes structures

Un nombre toujours croissant d'organisations se dotent d'expertes en cybersécurité et en gestion de cyberincidents ou y font appel. De nombreuses structures existent. Une prestataire de gestion de cyberincidents peut être externe ou interne, mais une organisation peut également faire appel simultanément ou en fonction des prestations à des entités internes et externes. Il convient d'appréhender les compétences et les prestations offertes par les 1305

2007 FF 2018 491, p. 522 ; FF 2023 1659, p. 25.

2008 OFPP, *Factsheet zum kritischen Teilsektor IT-Dienstleistungen*, 2012 p. 1. Pour plus d'informations, cf. *supra* N 470 ss.

prestataires de gestion de cyberincidents et non pas se limiter aux CSIRT ou aux SOC par exemple[2009].

1306 Les prestataires de gestion de cyberincidents peuvent prendre différentes formes et être internes comme externes aux organisations qu'elles servent. Les prestataires externes de gestion de cyberincidents fournissent des prestations à des organisations tierces en matière de cybersécurité. Ces fournisseuses externes seront concernées, comme les autres prestataires de gestion de cyberincidents, par les propositions d'obligations ci-après.

1307 En revanche, les prestataires internes ne fournissent pas des prestations à des organisations tierces, mais agissent pour l'organisation à laquelle elles sont intégrées. Elles n'ont pas de systèmes informatiques indépendants de ceux de la bénéficiaire de leurs prestations. Elles traitent les informations relatives aux cyberincidents à l'interne de l'infrastructure critique ou de l'organisation qu'elles servent, raison pour laquelle nous estimons que les exigences minimales de cybersécurité applicables aux infrastructures critiques devraient suffire pour ces prestataires.

1308 Il est important de comprendre que l'introduction d'exigences supplémentaires pour les entreprises fournissant des services numériques de sécurité permet d'appréhender la cybersécurité dans l'activité des fournisseuses de services informatiques et non pas uniquement les compétences de gestion de cyberincidents. En plus de permettre d'appréhender de façon plus globale la cybersécurité des infrastructures critiques, la réglementation de la cybersécurité dans les prestations fournies par des prestataires de gestion de cyberincidents et autres fournisseuses de services informatiques permet également d'assurer la cybersécurité dans les prestations fournies à d'autres personnes physiques ou morales.

4. La prise en compte des différents services et des différentes prestations

1309 Parmi les fournisseuses de services informatiques et en particulier de services numériques de sécurité et de prestations de gestion de cyberincidents, certaines organisations offrent des prestations de services à leur clientèle, d'autres mettent à disposition ou partagent des produits. La réglementation doit couvrir la cybersécurité des produits comme des prestations de services fournies par ces prestataires.

1310 Les exigences applicables aux organisations offrant des prestations informatiques ne doivent pas se limiter à la fourniture de logiciels et de matériel

2009 Au sujet des différentes structures, cf. *supra* N 272 ss.

informatique. Elles doivent aussi couvrir des prestations de services comme les conseils, le soutien juridique, technique, et les autres obligations de moyens.

En outre, les prestations en particulier des fournisseuses de services numériques de sécurité ne se limitent pas à la réaction à des cyberincidents. Leurs compétences peuvent porter sur des mesures préventives et détectives également, ce qui implique un large éventail de compétences. 1311

B. La compétence constitutionnelle de la Confédération à légiférer

L'art. 95 al. 1 Cst. permet à la Confédération de légiférer sur l'exercice des activités lucratives privées. La disposition attribue de larges compétences à la Confédération qui peut réglementer l'exercice d'une activité lucrative privée, les conditions matérielles et personnelles de cet exercice ainsi que les règles de mise sur le marché de produits sur le principe de la reconnaissance mutuelle entre l'UE, l'Espace économique européen (EEE) et la Suisse[2010]. 1312

Il serait envisageable de fonder en plus cette législation sur l'art. 97 Cst. qui attribue à la Confédération la compétence de prendre des mesures destinées à protéger les consommatrices (art. 97 al. 1 Cst.). La possibilité d'inclure des personnes morales dans la notion de consommatrice est controversée[2011], mais nous estimons qu'elles devraient être comprises dans la notion lorsque la loi a pour but de protéger des intérêts qu'une personne morale est susceptible d'avoir en tant que consommatrice, à l'instar des intérêts économiques. L'art. 97 Cst. permet à la Confédération de prendre des mesures de protection visant à assurer le bon fonctionnement d'une économie de marché tout en augmentant la transparence du marché, en protégeant les intérêts économiques des consommatrices ou en favorisant le pouvoir de négociation de ces dernières[2012]. 1313

Que la Confédération se base sur l'art. 95 Cst. ou sur la combinaison des art. 95 et 97 Cst., elle doit mettre en balance l'intérêt à légiférer avec les autres intérêts consacrés par la Constitution, à l'instar de la liberté économique (art. 27 Cst.)[2013]. Les exigences de cybersécurité supplémentaires pour les fournisseuses de services informatiques restreignent la liberté économique au sens de l'art. 27 Cst. et doivent par conséquent respecter les conditions de 1314

2010 CR Cst.-CANAPA, art. 95 N 18. À noter que si l'on se limitait à la réglementation des prestataires de gestion de cyberincidents auprès d'infrastructures critiques, l'on pourrait ajouter l'art. 57 Cst. à l'art. 95 al. 1 Cst. au titre de fondement constitutionnel.

2011 BSK BV-BIAGGINI, art. 97 N 5 ; CR Cst.-PICHONNAZ, art. 97 N 10.

2012 CR Cst.-PICHONNAZ, art. 97 N 19.

2013 CR Cst.-PICHONNAZ, art. 97 N 18 ; CR Cst.-CANAPA, art. 95 N 21.

l'art. 36 Cst.[2014]. Les exigences supplémentaires doivent figurer dans une base légale formelle[2015]. Un intérêt public doit être poursuivi, ce qui est le cas avec la sécurité publique. Particulièrement, la proportionnalité doit être respectée, ce qui implique que l'État ne peut pas réglementer l'activité des prestataires informatiques de façon trop extensive et faire intrusion dans la sphère économique de façon disproportionnée[2016].

C. Le choix des normes

1. La loi

1315 La question du choix de la base légale se posait déjà lors de l'examen de la possibilité d'introduire des exigences minimales de cybersécurité pour les infrastructures critiques[2017]. Dans le cas concret, les questions sont de savoir si la LSI est adéquate, s'il conviendrait de s'appuyer également ou exclusivement sur d'autres lois existantes (comme la Loi fédérale sur la sécurité des produits, LSPro) ou si une nouvelle loi devrait être adoptée au niveau de la Confédération.

1316 La LSI va prévoir une première obligation strictement liée à la cybersécurité. L'obligation de signaler les cyberattaques sera applicable à un nombre important d'infrastructures critiques dont les fournisseuses de services informatiques. Placer des obligations supplémentaires pour ces dernières dans la même loi suivrait une certaine logique. En outre, si la proposition législative du chapitre 9, visant à introduire des exigences minimales légales pour la cybersécurité des infrastructures critiques, venait à être suivie, la LSI consacrerait une série d'exigences minimales de cybersécurité aux infrastructures critiques. Il suffirait donc d'ajouter l'art. 95 Cst. (et possiblement l'art. 97 Cst.) dans les dispositions constitutionnelles servant de fondements à la LSI pour encadrer l'activité des prestataires de gestion de cyberincidents et des autres prestataires informatiques dans une perspective de cybersécurité.

1317 La Confédération se penche sur l'adoption d'une nouvelle réglementation pour les grandes plateformes de communication[2018]. Ce n'est pas dans ce contexte que la question des exigences de cybersécurité pour les prestataires

2014 Sur la distinction entre restrictions et dérogations dans ce contexte, cf. MARTENET, N 25 ss.

2015 Sur la notion de dispositions importantes et sur l'exigence qu'elles figurent dans une loi au sens formel, cf. *supra* N 1173 ss.

2016 CR Cst.-PICHONNAZ, art. 27 N 93 ss.

2017 Cf. *supra* N 1177 ss.

2018 CF, *Grandes plateformes de communication: Le Conseil fédéral aspire à une réglementation*, 5 mai 2023 (consulté le 20.3.2024).

informatiques doit être posée. Les grandes plateformes de communication sont en partie actives dans le sous-secteur critique des services informatiques, mais elles ne représentent en tout cas qu'une partie de ces organisations. Par ailleurs, la réglementation semble s'inspirer des règles du Règlement européen sur les services numériques (*Digital Services Act,* DSA), qui ne prévoit pas d'obligations en termes de cybersécurité, mais qui couvre davantage de questions ayant trait à la sécurité des utilisatrices et à d'autres types d'obligations.

Pour les fournisseuses de produits informatiques, la LSPro ne servirait 1318
pas de fondement idéal pour l'adoption d'une ordonnance plus spécifique. La LSPro poursuit des objectifs de protection de l'intégrité physique et de la santé des utilisatrices, mais pas de cybersécurité ou de protection des informations[2019]. Partant, la LSPro est insuffisante pour abriter les exigences supplémentaires de cybersécurité. Il en va de même pour la LPD, qui se limite aux données personnelles alors que la cybersécurité concerne d'autres informations traitées par des systèmes informatiques. Bien qu'il soit possible d'élargir les objectifs, le champ d'application et le contenu de ces lois, la LSI est à privilégier, dans la mesure où elle règle la cybersécurité et va abriter des dispositions revêtant un intérêt particulier pour les fournisseuses de services informatiques.

Si une nouvelle loi venait à être adoptée pour les exigences minimales 1319
applicables aux infrastructures critiques, les obligations supplémentaires applicables aux prestataires informatiques pourraient suivre le sort de celles-là.

Finalement et au vu de l'adéquation de la LSI et de ses ordonnances pour 1320
réglementer cette situation, nous estimons que l'adoption d'une nouvelle loi est à l'heure actuelle disproportionnée. L'on ne peut toutefois exclure qu'une nouvelle loi doive un jour être adoptée pour l'activité des services informatiques et de façon analogue à la LTC pour les fournisseuses de services de télécommunication, pour imposer des obligations de cybersécurité ainsi que d'autres obligations aux prestataires informatiques.

2. Les actes d'exécution

Dans la mesure où la loi fédérale doit contenir les normes importantes en 1321
termes d'obligations, il va de soi que des ordonnances doivent pouvoir être adoptées et que la législation doit pouvoir être précisée par différents actes d'exécution. Les fournisseuses de services informatiques ne sont aujourd'hui pas réglementées et ne sont pas soumises à la surveillance d'une autorité spécifique. Nous estimons qu'il est important qu'une autorité sectorielle les surveille.

2019 Cf. *supra* N 484 ss.

1322 Bien que la mise sur le marché de produits informatiques ou la fourniture de services informatiques ne soulèvent pas uniquement des questions de sécurité, l'OFCS est l'autorité adéquate, voire idéale, pour surveiller la cybersécurité des organisations offrant des prestations informatiques. Elle détient en effet d'importantes compétences techniques et est l'autorité principale pour la cybersécurité. Les actes d'exécution devraient émaner du CF et de l'OFCS pour ces organisations[2020].

D. Le contenu de la réglementation

1. Les conditions matérielles et personnelles de l'exercice

1323 Il est possible de réglementer l'accès à ces professions en le subordonnant à certaines qualifications[2021]. À titre d'exemples, il existe au niveau fédéral une réglementation pour les conseillères en brevet (voir la Loi sur les conseils en brevets, LCBr), ou des réglementations cantonales hétérogènes pour les pompières[2022].

1324 La profession de « professionnelle de la gestion de cyberincidents », de spécialiste de la sécurité informatique, de service de sécurité ou encore plus largement de fournisseuse de services informatiques n'est à ce jour pas réglementée, ce qui implique que les cantons sont encore compétents pour édicter des règles concernant l'accès à ces professions si besoin. Plusieurs métiers sont réglementés en Suisse, à un niveau cantonal, intercantonal ou fédéral. En vertu de l'art. 95 Cst., les cantons disposent de la compétence de réglementer les professions, du moins jusqu'à ce que la Confédération fasse usage de la sienne. Sur le plan national, il ne nous semble pas nécessaire de légiférer aujourd'hui sur l'accès à ce type de professions, dans la mesure où une telle réglementation serait particulièrement intrusive, du fait que ce domaine est encore récent dans la pratique.

1325 Néanmoins, quelques mesures pourraient être anticipées au niveau de la loi pour assurer que les personnes actives auprès d'une fournisseuse de services informatiques prennent en compte les enjeux de cybersécurité. À titre d'exemple, le Concordat du 18 octobre 1996 conclu entre cantons romands sur les entreprises de sécurité impose l'obtention d'une autorisation préalable pour l'exploitation d'une entreprise de sécurité ou d'une succursale dans les cantons concordataires, pour l'exercice d'une activité tombant dans le champ du Concordat ou pour l'utilisation d'un chien de garde (art. 7 al. 1 Concordat sur les entreprises de sécurité, CES).

2020 Sur la question des actes d'exécution par ces deux autorités, cf. *supra* N 1187 ss et 1195.

2021 SEFRI, *Professions et activités réglementées en Suisse,* 2023, p. 3.

2022 SEFRI, *Professions et activités réglementées en Suisse,* 2023, p. 19.

De telles dispositions sont à l'heure actuelle disproportionnées, du moins pour l'ensemble des prestataires de gestion de cyberincidents ou pour l'ensemble des fournisseuses de services informatiques. En revanche, il est possible de prévoir, sur le plan intercantonal ou sur le plan fédéral, des dispositions analogues aux art. 15*a* ou 16 CES. L'art. 15*a* impose aux entreprises de sécurité de dispenser une formation initiale et une formation continue aux employées, qui sont toutes deux certifiées par des tests écrits sous la responsabilité des cheffes d'entreprise. Le contenu, les modalités et le contrôle des formations sont prévus par une directive édictée par la Commission concordataire (art. 15*a* al. 3 CES). À destination des prestataires informatiques, il serait envisageable de prévoir également la formation initiale ou continue en matière de cybersécurité pour les personnes exerçant de telles fonctions[2023]. Une attention particulière devrait le cas échéant porter sur les modalités d'introduction, de faisabilité et de mise en œuvre d'une telle disposition, notamment quant à la forme de la base légale et les compétences d'adoption de l'acte, quant au type de formation, à la disponibilité pratique des formations ou encore aux compétences au sein des organisations. Bien qu'intéressantes, ces réflexions paraissent complexes à intégrer dans le cadre réglementaire et dans la pratique actuelle. Il n'est pas certain que de telles obligations soient réellement utiles, du moins à l'heure actuelle où la volonté porte réellement sur la responsabilité des organisations fournissant ces prestations. Elles pourraient en outre bloquer le marché. 1326

2. La réglementation de l'exercice de l'activité

a. L'obligation de cybersécurité dans les prestations

(i) L'obligation générale de cybersécurité

La LSI et son ordonnance se sont déjà attardées sur cette question (voir plus précisément art. 30 OSI) pour les prestataires internes de la Confédération, qui sont à la fois des prestataires et des unités administratives[2024]. L'art. 19 al. 1 LSI, sur lequel se base l'art. 30 OSI, impose aux autorités et organisations soumises à la loi de garantir la sécurité des moyens informatiques qu'elles exploitent pour elles-mêmes ou sur mandat d'une autre autorité ou organisation. L'art. 30 OSI impose aux fournisseuses internes de prestations à son al. 3 OSI de veiller à disposer, sur le plan du personnel et des finances, des capacités 1327

2023 L'art. 16 CES dispose aussi du rapport de ces entreprises avec la police, prévoyant que les personnes soumises au concordat prêtent assistance à la police spontanément ou sur requête (art. 16 al. 2 du Concordat). L'introduction d'une obligation aux équipes de gestion de cyberincidents de collaboration accrue avec des autorités telles que l'OFCS en cas de large cyberincident doit être analysée, cf. *infra* N 1342 ss.

2024 SG-DDPS, *Législation d'exécution relative à la LSI, Explications*, 2023, p. 21.

ainsi que des compétences nécessaires à la détection, à l'analyse et à la maîtrise des incidents et des vulnérabilités que les concernent ou qui concernent les bénéficiaires de leurs prestations. L'art. 30 al. 4 OSI leur impose de surveiller l'utilisation de leur infrastructure informatique ainsi que de l'examiner régulièrement pour rechercher des menaces et des vulnérabilités techniques. L'art. 30 al. 4 *in fine* OSI octroie la faculté aux fournisseuses de déléguer cet examen à des tierces.

1328 Ces obligations découlent de l'art. 19 LSI qui impose une obligation de sécurité aux autorités et organisations de la Confédération. C'est sur cette base que l'art. 30 OSI a été adopté. Les obligations prévues à l'art. 30 al. 3 et 4 OSI valent uniquement pour les fournisseuses internes de prestations. Selon le rapport explicatif de l'ordonnance, les fournisseuses internes ont notamment l'obligation générale de fournir des prestations informatiques de façon conforme aux techniques les plus récentes ainsi qu'une obligation générale de transmettre les informations nécessaires relatives à la sécurité à leurs bénéficiaires. La responsabilité quant à la définition des responsabilités revient en revanche à la bénéficiaire des prestations informatiques[2025]. Les prestataires internes sont naturellement soumises à la responsabilité de l'autorité ou de l'organisation de laquelle elles font partie. Dans la mesure où des fournisseuses internes peuvent offrir leurs prestations à plusieurs autorités publiques, elles doivent néanmoins être responsabilisées lorsqu'elles traitent des informations ou exploitent des moyens informatiques pour les bénéficiaires de prestations[2026].

1329 Pour un point de comparaison impliquant des prestataires et des clientes, l'art. 8 LPD impose aux responsables du traitement et aux sous-traitantes d'assurer par des mesures appropriées une sécurité adéquate des données personnelles par rapport au risque du traitement (art. 8 al. 1 LPD). L'art. 9 al. 2 LPD impose à la responsable du traitement de s'assurer que sa sous-traitante est en mesure de garantir la sécurité. L'on peut voir que l'art. 9 al. 2 LPD prévoit donc une responsabilité pour la responsable du traitement d'une façon similaire à la bénéficiaire de prestation à l'art. 19 LSI. La sous-traitante demeure néanmoins également responsable de la sécurité des données qu'elle traite[2027]. Elle est à ce titre soumise individuellement au principe de sécurité des données ainsi qu'aux exigences du CF en vertu des art. 8 LPD et 1 ss OPDo[2028].

2025 SG-DDPS, *Législation d'exécution relative à la LSI, Explications*, 2023, p. 21.

2026 OA, *Enquête administrative « Fuite de données »*, 2024, N 576. Cette situation particulière devrait être appréhendée dans les bases légales habilitant ces autorités à effectuer de telles prestations.

2027 CR LPD-MÉTILLE, art. 9 N 79.

2028 Pour plus d'informations sur les exigences liées à la sécurité des données personnelles, cf. *supra* N 873 ss.

La situation qui nous occupe présentement est principalement celle des prestataires privées de gestion de cyberincidents fournissant leurs prestations à une clientèle externe. Elles ne sont actuellement pas soumises à des obligations légales de cybersécurité concernant leur infrastructure informatique ou les traitements informatiques d'informations auxquelles elles procèdent. Elles ne sont pas non plus soumises à des exigences de cybersécurité pour les prestations qu'elles fournissent, en termes de prestations de services ou de produits fournis, à l'instar de systèmes de détection et de prévention d'intrusion (*intrusion detection and prevention systems,* IDPS). Si la proposition législative du chapitre 9 venait à être adoptée[2029], ces prestataires seraient soumises à des exigences minimales légales de cybersécurité concernant leur infrastructure informatique et leurs traitements informatisés d'informations, d'une façon similaire à ce qui est prévu tant aux art. 19 LSI et 30 OSI qu'aux art. 8 LPD et 1 ss OPDo. En revanche, certaines des activités à l'attention de leur clientèle risquent de ne pas être couvertes par ces exigences minimales. Cela concerne précisément les traitements d'informations informatisés sur l'infrastructure informatique d'une cliente, les prestations de conseil ou d'audit ou encore la transmission et l'exploitation par la cliente d'un logiciel fabriqué par une organisation fournissant des services numériques de sécurité ou par une fournisseuse de services informatiques. Bien que la LSI et la LApEl imposent à certaines infrastructures critiques de soumettre leurs prestataires informatiques aux exigences de la loi[2030], il n'en va pas de la sorte pour toutes les infrastructures critiques. 1330

La LSI n'impose déjà pas expressément une obligation aux fournisseuses internes de prestations informatiques dont des prestations de sécurité informatique, mais l'OSI leur impose des obligations. Il existe certes quelques obligations à l'instar de l'art. 7 al. 2 de l'Ordonnance sur le traitement de données personnelles et de données de personnes morales lors de l'utilisation de l'infrastructure électronique de la Confédération (OTUIC) qui impose aux personnes morales chargées de travaux techniques comme la maintenance de l'infrastructure électronique de la Confédération de conserver les informations de façon sécurisée et de protéger leur confidentialité d'accès illicites. Cette disposition est générale, et elle limite sa protection aux données personnelles et de personnes morales, ainsi que son champ d'application aux personnes morales effectuant ces travaux sur l'infrastructure électronique de la Confédération. En parallèle, l'art. 11 al. 1 OTNI conditionne, toujours du côté des autorités de l'administration fédérale, l'accès des fournisseuses externes aux 1331

2029 Cf. *supra* N 1145 ss.

2030 Cf. *supra* N 671 s.

données non accessibles au public notamment à la mise en place de mesures contractuelles, organisationnelles et techniques appropriées pour éviter que les données soient accessibles à autrui (art. 11 al. 1 litt. c OTNI). Bien que la disposition protège plus d'informations que l'OTUIC, elle impose indirectement des mesures permettant uniquement de protéger la confidentialité des informations[2031].

1332 En protection des données personnelles, la LPD prévoit un principe de sécurité concrétisé au niveau de l'ordonnance. En cybersécurité, il est important que les fournisseuses de services informatiques soient soumises à une obligation leur imposant de garantir la cybersécurité dans les prestations qu'elles offrent et pas uniquement dans le cadre des exigences minimales de cybersécurité applicables aux infrastructures critiques. En effet, la loi doit apporter un soutien dans l'attribution claire des responsabilités[2032]. Une obligation générale au niveau de la loi d'assurer la cybersécurité dans les prestations offertes présenterait un caractère suffisamment général pour pouvoir être concrétisée dans les ordonnances. Une telle obligation disposerait d'une densité normative similaire à l'art. 8 LPD. Il est essentiel que des exigences concrètes dans les actes d'exécution tirent leur fondement d'une loi au sens formel[2033].

(ii) Quelques exemples de concrétisation de l'obligation

1333 La disposition doit prévoir que le CF concrétise les obligations et mesures de cybersécurité, compétence pouvant être déléguée à l'OFCS. Plusieurs dispositions habilitent le CF à concrétiser des exigences minimales de sécurité. Il en va de la sorte pour l'art. 8 al. 3 LPD, dont le principe de sécurité est concrétisé aux art. 1 ss OPDo. Il en va de même pour le nouvel art. 8*a* al. 2 LApEl, qui prévoit que le CF peut étendre l'obligation aux gestionnaires de réseau, productrices et agents de stockage de prendre les mesures de protection adéquates des installations contre les cybermenaces à d'autres prestataires, ainsi que prévoir des exceptions[2034]. Une formulation similaire permettrait d'une part au CF d'exempter certaines organisations actives dans les services informatiques de l'obligation de sécurité ou de certaines obligations concrètes en découlant si les obligations ne leur sont pas pertinentes. L'ordonnance du CF ou

2031 Alors que la sécurité de l'information compte d'autres composantes, à savoir l'intégrité, la disponibilité ou encore la traçabilité.

2032 SOLOVE/HARTZOG, p. 75 et 194 s.

2033 Sur la nécessité d'introduire les « dispositions importantes » dans une loi et sur l'impossibilité de se limiter à des ordonnances ou à des actes de droit souple, cf. *supra* N 1173 ss et 1197 ss.

2034 FF 2023 84, p. 56 s.

de l'OFCS pourrait d'autre part concrétiser l'obligation de cybersécurité, par exemple par une obligation pour les fournisseuses de services informatiques de séparer leurs systèmes informatiques de ceux de ses clientes.

En termes de contenu, l'art. 30 al. 3 et 4 OSI ainsi que son rapport explicatif mentionnent des obligations particulièrement pertinentes. Comme susmentionné, l'art. 30 al. 3 OSI impose aux fournisseuses internes de prestations informatiques de garantir qu'elles disposent des capacités et compétences tant personnelles que financières nécessaires pour déceler à temps, analyser techniquement et maîtriser les incidents de sécurité ou les failles de sécurité qui les concernent ou qui concernent leurs bénéficiaires de prestations. Les fournisseuses internes de prestations informatiques doivent également effectuer des surveillances permettant de s'assurer que l'infrastructure informatique soit utilisée de manière sûre ainsi que rechercher régulièrement les menaces et vulnérabilités (art. 30 al. 4 OSI). Des concrétisations à l'instar de ce qui précède doivent figurer dans les dispositions de l'ordonnance applicables aux fournisseuses de services informatiques. 1334

Le contenu de l'ordonnance doit aussi permettre la distinction entre différentes entreprises de services informatiques pour mieux appréhender les différences dans leurs pratiques et dans les défis auxquels ils sont susceptibles d'être confrontés. À titre d'exemple comparatif, l'Ordonnance sur la sécurité des ascenseurs (OAsc) prévoit des dispositions générales à l'instar de son art. 2 al. 1 litt. a qui dispose que les ascenseurs doivent notamment être installés et entretenus correctement et utilisés conformément à leur destination ou dans des conditions raisonnablement prévisibles pour être mis sur le marché et en service. L'Oasc distingue ensuite les obligations selon le rôle de l'organisation, à savoir si elle agit comme installatrice, fabricante, mandataire, importatrice ou distributrice (art. 4 al. 1 Oasc[2035]). Un mécanisme similaire dans la LSI et dans les ordonnances permettrait d'introduire des obligations spécifiques en fonction du rôle des prestataires et permettrait d'appréhender des considérations spécifiques selon les services informatiques offerts et le rôle des organisations concernées. 1335

Il est important de s'inspirer des réglementations et propositions de réglementations étrangères pour la concrétisation de l'obligation d'assurer la cybersécurité dans les prestations. Par exemple, l'annexe I de la proposition de Loi sur la cyberrésilience (*Cyber Resilience Act,* CRA) pose les exigences essentielles de cybersécurité et les exigences pour la gestion de vulnérabilités 1336

2035 L'art. 4 al. 1 OAsc renvoie aux différentes dispositions topiques dans la Directive 2014/33/UE du Parlement européen et du Conseil du 26 février 2014 relative à l'harmonisation des législations des États membres concernant les ascenseurs et les composants de sécurité pour ascenseurs.

applicables aux fabricantes et aux importatrices de produits informatiques en vue d'assurer la cybersécurité des produits. Les exigences y figurant incluent la conception, le développement et la production propres à limiter les surfaces d'attaques (en incluant les interfaces), la protection de la disponibilité des fonctions essentielles d'un produit informatique ou la mise en place de stratégies sur la divulgation coordonnée de vulnérabilités (Annexe I CRA). De telles exigences pourraient typiquement, en droit suisse, figurer dans une ordonnance du CF ou de l'OFCS.

(iii) Le respect du principe de proportionnalité

1337 Le principe de proportionnalité doit être respecté par la loi, en ce sens que la législation fédérale doit se limiter à la barrière clairement identifiée et ne pas réglementer davantage de questions[2036]. Dans le cas d'espèce, la problématique à réglementer est la nécessité d'assurer un niveau de sécurité dans les prestations offertes par des fournisseuses de services informatiques. Pour ce faire, la loi et les ordonnances doivent, en tout cas actuellement, se limiter à des obligations générales qui sont aujourd'hui inexistantes, avec des concrétisations dans les actes d'exécution de la loi. Il n'est pas exclu que les évolutions à venir conduisent à des adaptations législatives.

1338 En revanche, pour respecter le principe de la proportionnalité, la loi ne doit pas réglementer les questions devant être laissées à la pratique. Par exemple, elle ne doit pas, du moins à l'heure actuelle, régler les questions de façon plus limitative que ce qui existe en droit des obligations, par exemple lorsqu'il en va des questions d'accords de confidentialité[2037].

b. L'obligation de transparence

1339 En parallèle, la transparence permet pour différentes organisations de démontrer qu'elles présentent certaines qualités. Les obligations de transparence, soit auprès d'une autorité susceptible de rendre compte au public, soit directement à la population, permettent de parvenir à de tels objectifs. À titre d'exemple, l'art. 12*a* LTC, concrétisé par l'art. 10*e* OST, impose un tel devoir aux fournisseuses de services de télécommunication. Concrètement, les fournisseuses de télécommunication peuvent être obligées de publier des informations sur la qualité des services qu'elles offrent, pour comprendre par exemple si la mauvaise qualité d'une vidéo est due à des mesures prises par la fournisseuse

2036 CR Cst.-CANAPA, art. 95 N 21.

2037 Sur les accords de confidentialité et autres outils pratiques, cf. *supra* N 1008 ss, en particulier 1011 ss.

d'accès à Internet ou à d'autres raisons[2038]. Les fournisseuses de services de télécommunication doivent spécifiquement fournir des informations relatives aux différentes pratiques et aux traitements différenciés[2039].

Il faut s'inspirer de ce type de dispositions pour imposer aux fournisseuses de services informatiques un devoir de transparence relatif à la sécurité des informations et de leurs systèmes informatiques. Cette obligation peut passer soit par une information du public au sujet du niveau de qualité des services (ou, en d'autres termes, du respect de normes) et de la sécurité des prestations (qui peut notamment passer par une certification)[2040], soit par une information à l'OFCS qui pourrait par la suite publier des rapports permettant aux organisations de choisir avec quelle fournisseuse de services informatiques contracter. L'objectif est d'éviter que les entreprises utilisent des sites Internet tape-à-l'œil *(« shiny websites »)* avec une qualité discutable dans les prestations[2041]. L'obligation de transparence doit figurer dans la LSI et être concrétisée dans l'OSI, éventuellement l'ordonnance technique de l'OFCS. 1340

c. L'examen d'autres obligations

(i) Une obligation de collaboration accrue ?

Il est maintenant établi que les fournisseuses de services informatiques, mais surtout les fournisseuses de services numériques de sécurité, dont les prestataires de gestion de cyberincidents, jouent un rôle particulier en matière de cybersécurité. Ces organisations permettent de prévenir, de détecter et de réagir aux cyberincidents, aux vulnérabilités et aux autres cybermenaces. Partant, elles sont particulièrement susceptibles d'avoir accès à des informations qui pourraient aider l'OFCS à réaliser ses missions, dont la vue d'ensemble des cybermenaces et, si nécessaire, de soutien aux groupes cibles (dont principalement les infrastructures critiques)[2042]. Elles peuvent également détenir des informations utiles aux autorités de poursuite pénale ou au SRC. 1341

Certaines bases légales prévoient des obligations de collaboration accrue. Tel est le cas pour la sécurité, avec l'art. 16 CES qui prévoit le rapport de ces 1342

2038 FF 2003 7245, p. 7266.

2039 FF 2017 6185, p. 6241 s.

2040 Sur la certification, cf. *supra* N 1265 ss.

2041 Il est possible que la communication d'informations soit amoindrie par l'introduction de telles exigences, raison pour laquelle il est crucial qu'elles soient accompagnées par des mesures de sensibilisation et de vulgarisation. La population et l'industrie doivent comprendre que la prestation parfaite n'existe pas pour que les entreprises fournissant des services informatiques puissent être les plus transparentes possibles.

2042 Cf. notamment FF 2023 84, p. 33 ; MEYER/MÉTILLE, *Loi fédérale sur la sécurité de l'information : version 2.0,* 2022, N 35 ss.

entreprises avec la police. Les personnes soumises au concordat prêtent assistance à la police spontanément ou sur requête (art. 16 al. 2 CES).

1343 Une telle obligation semble à l'heure actuelle trop intrusive dans la pratique des prestataires de gestion de cyberincidents. Il existe déjà un mécanisme de coopération volontaire entre l'OFCS et les fabricantes de logiciels ou de matériels informatiques. Toute personne est susceptible d'annoncer des cybermenaces au NCSC en vertu de l'art. 73*b* LSI2. Lorsque l'OFCS prend connaissance de vulnérabilités, il en informe la fabricante en lui fixant un délai pour l'éliminer. Si la fabricante y consent (ou qu'elle n'a pas éliminé la vulnérabilité dans le délai fixé), l'OFCS peut publier des informations relatives aux vulnérabilités en indiquant le matériel informatique ou le logiciel concerné (art. 73*c* al. 2 LSI2). La question d'une coopération plus accrue se pose, surtout dans le contexte de l'activité des pirates éthiques qui évoluent dans une zone souvent grise[2043].

1344 Les art. 73*b* s. LSI2 doivent servir d'incitations pour que les fabricantes de matériel informatique et de logiciels corrigent et éliminent les vulnérabilités. La pratique après l'entrée en vigueur de la LSI2 nous permettra de comprendre si l'incitation est suffisante ou si une obligation légale d'éliminer les vulnérabilités doit être adoptée. Le cas échéant, il faudra réfléchir aux modalités de l'obligation, notamment en relation avec le délai pour corriger la vulnérabilité ou avec le niveau de risques qu'elle doit atteindre pour devoir être éliminée.

1345 En parallèle, il est important de poursuivre la ligne de pensée selon laquelle les fournisseuses de services informatiques revêtent un statut particulier pour le domaine de la cybersécurité. L'on pourrait imaginer l'adoption d'une disposition similaire à l'art. 76 al. 2 LSI2 pour permettre à l'OFCS de communiquer des données personnelles aux entreprises offrant des services informatiques lorsque c'est nécessaire à la protection contre les cybermenaces, et vice versa. C'est d'ailleurs ce qui prévaut sous le régime de la première version de la LSI, avec une possibilité de communication entre les services tels que l'OFCS et les « fournisseurs et exploitants de services informatiques et de communication » (art. 76 al. 3 LSI)[2044]. Cela étant, une telle disposition n'est pas nécessaire dans la mesure où l'art. 76 LSI2 permet déjà la collaboration entre l'OFCS et les infrastructures ainsi que la communication de données personnelles lorsque c'est nécessaire pour la protection contre les cybermenaces.

2043 Sur les pirates éthiques, cf. *infra* N 475 ss et 1350 ss.

2044 La notion de service informatique n'étant pas précisée, il n'est pas certain que l'autorité législative entendît réellement intégrer les fournisseuses de services informatiques comme compris dans la présente étude dans la notion ; qui plus est, la disposition ne prévoit de motif justifiant une communication et serait donc trop large dans sa première version. En revanche, l'ajout de la notion de « fournisseur de services informatiques » à l'art. 76 al. 2 LSI2 serait bienvenu.

Les entreprises de services informatiques faisant partie des infrastructures critiques, cette base légale est suffisante pour permettre la coopération par la communication de données personnelles lorsque c'est nécessaire[2045]. Il est en tout cas important que les communications entre les autorités d'application de la loi et les entreprises offrant des services numériques de sécurité soient protégées[2046].

(ii) L'obligation de souscrire à une assurance responsabilité civile ?

1346 D'autres obligations pourraient être examinées dans ce cadre. Il pourrait par exemple en aller de la sorte avec l'introduction d'une possible obligation pour les prestataires informatiques de souscrire à une assurance de responsabilité civile professionnelle. En effet, il est important que les clientes d'une prestataire informatique puissent s'assurer que la prestataire peut assumer la couverture des dommages potentiels. La clause contractuelle type de la Conférence des achats de la Confédération (CA) prévoit justement qu'une disposition du contrat liant une autorité fédérale et une prestataire informatique peut concerner l'obligation à la prestataire de souscrire à une assurance responsabilité civile pour les cyberattaques[2047].

1347 À titre de comparaison, la Loi sur la libre circulation des avocats (LLCA) impose aux avocates d'être « au bénéfice d'une assurance responsabilité civile professionnelle offrant une couverture adaptée à la nature et à l'étendue des risques liés à son activité » (art. 12 litt. f LLCA). La somme permettant de couvrir les événements dommageables pour une année doit être d'au minimum un million de francs. L'assurance peut être remplacée par des sûretés (art. 12 litt. f *in fine* LLCA).

1348 Les prestataires informatiques devraient, selon l'opinion ici défendue et au-delà de la situation dans laquelle elles offrent leurs prestations à la Confédération, être au bénéfice d'une assurance responsabilité civile professionnelle. Les dommages potentiels doivent en effet pouvoir être pris en charge. Cela étant, l'introduction pour les avocates de l'obligation d'être au bénéfice d'une telle assurance a consisté en la codification d'une règle déontologique[2048]. Pour cette raison, il conviendrait d'abord d'étudier le marché des prestataires informatiques avant de s'assurer que l'introduction d'une telle obligation légale est opportune et réaliste.

2045 FF 2023 84, p. 49.

2046 Cette question est à nouveau particulièrement pertinente pour l'activité des pirates éthiques, cf. *infra* N 1350 ss.

2047 CA, *Clause contractuelle type de la CA pour les cyberattaques*, 2024, p. 2, 4 et 8.

2048 FF 2005 6207, p. 6219.

(iii) L'exemple particulier des pirates éthiques

1349 Réglementer le piratage éthique pourrait permettre d'améliorer la sécurité juridique quant aux activités des pirates éthiques[2049]. Le droit permet d'appréhender une partie des comportements des pirates éthiques dans un cadre contractuel, à condition de prévoir des clauses adéquates dans le contrat qui les lie à leur clientèle, du moins sur l'infrastructure de leurs clientes. Il ne s'agit pas ici d'examiner des obligations, mais le cadre légal autour de l'activité et le statut des pirates éthiques.

1350 L'on pourrait éventuellement réfléchir à une exclusion de la responsabilité en cas d'acte de piraterie éthique, ou à l'établissement d'une pratique reconnue selon laquelle l'OFCS ne dénonce pas aux autorités de poursuite pénale les signalements de vulnérabilités transmis par des pirates éthiques[2050]. Les modalités, les conditions et les garde-fous de cette exclusion de responsabilité devraient être appréhendés le cas échéant. Si les exigences de cybersécurité pour les fournisseuses de services informatiques venaient à être introduites, l'exclusion de responsabilité pourrait figurer dans la section de la LSI relative à ces organisations. Il serait également possible de faire figurer cette exclusion pour mobiles honorables dans les dispositions concernées, à l'instar des art. 143, 143*bis* et 144*bis* CP.

1351 Il est important que la police puisse être au courant d'actes répréhensibles que les pirates découvriraient dans leur activité. Pour ce faire, la collaboration entre les autorités de poursuite pénale et l'OFCS doit pouvoir continuer aux conditions et sur la base de l'art. 73*d* al. 2 LSI2. Il faut néanmoins garantir en pratique que les signalements peuvent se faire anonymement, ce qui implique que la personne qui signale ne devrait pas se voir reprocher son comportement à l'origine du signalement dans le cadre d'une procédure pénale. L'art. 73*c* al. 3 AP-LSI2 prévoyait expressément que les informations transmises par le biais d'un signalement au NCSC ne pouvaient pas être utilisées contre la personne à l'origine du signalement dans le cadre d'une procédure pénale. Cette disposition a disparu durant la révision de la loi, mais il demeure possible de procéder à un signalement anonyme (art. 73*b* al. 1 LSI2). Il est nécessaire, dans ce contexte comme de façon plus générale, que les personnes signalant à l'OFCS des vulnérabilités et autres menaces ne soient pas dissuadées d'apporter une sorte d'aide à l'autorité. Qui plus est, la personne à la tête de l'OFCS est déliée de l'obligation de dénoncer en vertu de l'art. 22*a* al. 1 de la Loi sur le personnel

2049 Ce qui est par ailleurs souhaité par le CF, voir CF, *CSN*, 2023, p. 20.

2050 Ce qui soulèverait naturellement d'autres questions, comme celle de savoir comment s'assurer qu'une personne signalant une vulnérabilité est une pirate éthique.

de la Confédération (LPers). L'on peut donc espérer que les personnes dirigeant l'OFCS renonceront à dénoncer aux autorités de poursuite pénale si le signalement d'une pirate éthique laisser présumer, par exemple, un accès indu à un système informatique. Au vu de la formulation du message, il semblerait que cette transmission d'information ne concerne que les infractions les plus graves (comme la découverte suite au signalement de matériel pornographique). C'est pourquoi nous estimons que l'OFCS ne transmettra probablement pas des informations au sujet d'une pirate éthique qui émet un signalement aux autorités de poursuite pénale, mais qu'il conservera cette faculté pour des cas exceptionnels[2051].

1352 Pour augmenter la sécurité juridique au profit des pirates éthiques, un rôle dans la loi (la LSI servant de fondement adéquat) de signaleuse de confiance pourrait être imaginé, avec la possibilité de s'inspirer en partie de ce qui a été créé dans le contexte des services numériques dans l'UE (art. 22 DSA). Dans le contexte des pirates éthiques en Suisse, ce statut de signaleuse devrait pouvoir être attribué à des personnes physiques comme morales, qui démontrent notamment qu'elles détiennent une expertise dans la recherche de vulnérabilités, cyberincidents et autres cybermenaces, qu'elles sont indépendantes et qu'elles travaillent de façon diligente et objective[2052]. Les procédures les concernant, leurs fonctions ainsi que les conséquences liées à leur statut devraient les cas échéant être évaluées et clarifiées. Les signaleuses de confiance au sens du DSA ont pour missions principales de transmettre auprès des services numériques concernés des notifications en cas de contenu illicite et de publier des rapports à ce sujet. En revanche, la signaleuse de confiance au sens de la LSI aurait davantage un statut particulier de confiance auprès de l'OFCS et pourrait par exemple bénéficier d'une exclusion générale de responsabilité pour des infractions telles que l'accès indu à un système informatique ou la soustraction de données lorsqu'elle effectue des signalements au sens de l'art. 73*b* al. 1 LSI2.

1353 En parallèle de ces questions et relativement aux questions de sécurité dans les prestations, l'introduction d'exigences aux prestataires de services informatiques serait ici aussi pertinente. Le cas échéant et si la qualité de fournisseuse de services informatiques est reconnue aux pirates éthiques lorsqu'elles agissent sur la base d'un contrat ou en suivant les directives d'une entreprise[2053], ces exigences permettraient d'assurer que leurs prestations

2051 FF 2023 84, p. 29.

2052 Pour un point de comparaison dans le DSA, voir art. 22 par. 2 DSA ; c. 61 DSA.

2053 Les entreprises peuvent fixer le type de piratage éthique qu'elles acceptent, ses modalités et ses conditions. Ces informations sont publiées dans des directives sur le

sont faites en garantissant la cybersécurité comprenant la sécurité informatique et la sécurité des informations traitées par des systèmes informatiques.

E. Les mécanismes de contrôle

1. Les instruments pour l'ensemble des infrastructures critiques

1354 Certains instruments permettent de contrôler la conformité aux obligations devant découler de la LSI pour toutes les infrastructures critiques. Le nouvel OFCS doit pouvoir prendre un ensemble de mesures de supervision et d'exécution. Un mécanisme de certification facultative bénéficierait ici aussi d'un intérêt. Des sanctions adaptées devraient être prévues par la LSI.

1355 Les fournisseuses de services informatiques devraient tout d'abord être soumises comme les autres infrastructures critiques à des audits externes, des avertissements et d'autres mesure d'exécution dans les conditions prévues par la loi[2054]. La certification sur le modèle expliqué précédemment est ensuite particulièrement pertinente pour ces entreprises, parmi lesquelles figurent les développeuses de logiciels et les fabricantes de matériels informatiques[2055]. Les sanctions décrites auparavant devraient finalement aussi s'appliquer aux prestataires de services informatiques en cas de violation des exigences supplémentaires[2056].

2. Les obligations d'annonce ou l'autorisation

1356 L'on pourrait se demander si, outre les mesures susmentionnées, d'autres mécanismes spécifiques pour les fournisseuses de services informatiques devaient être mis en place, comme une obligation d'autorisation ou d'annonce pour exercer une activité tombant dans ce sous-secteur.

1357 L'annonce est moins intrusive que l'autorisation et est donc préférable en termes de proportionnalité. Elle permet à l'autorité à qui les entreprises s'annoncent de savoir qui offre des prestations de cybersécurité et de contrôler le cas échéant plus facilement le respect des exigences de cybersécurité. L'obligation d'annonce devrait être assortie d'une sanction en cas de non-respect, afin de permettre une prise de conscience de la nécessité de se conformer à cette annonce. L'annonce revêt l'avantage d'être moins intrusive que l'autorisation, tout en permettant à l'État d'avoir une vue d'ensemble et d'intervenir

signalement et la diffusion de vulnérabilités. Alors que rares sont les organisations procédant ainsi, le CF encourage cette démarche, cf. CF, *La promotion du piratage éthique en Suisse*, 2023, p. 7 et 14.

2054 Cf. *supra* N 1272 ss.

2055 Cf. *supra* N 1265 ss.

2056 Cf. *supra* N 1276 s.

si la situation l'exige[2057]. Si une obligation d'annonce est introduite, l'OFCS est l'autorité idéale pour recevoir les annonces. L'Institut national de test pour la cybersécurité (NTC) aurait pu constituer une autorité intéressante pour les annonces des fabricantes de matériel informatique, de même que l'Office fédéral de l'informatique et de la télécommunication (OFIT)[2058]. Le statut et les missions du NTC ne sont pas claires et semblent être limitées par rapport à son mandat initial, raison pour laquelle il paraît difficilement concevable en l'état de compter sur cette entité pour recevoir les annonces[2059]. L'OFIT disposant principalement de compétences pour l'administration fédérale, l'OFCS est l'autorité appropriée. En cas d'introduction d'une telle obligation, les autorités devraient analyser la meilleure alternative.

1358 Si un régime d'annonce ne permet pas d'atteindre le but visé, l'on peut analyser l'autorisation, qui entraîne un travail administratif plus conséquent. L'autorisation doit être prévue dans une loi au sens formelle, qui doit circonscrire les comportements admissibles avec une autorisation et qui peut (en tant que personne physique ou personne morale) bénéficier d'une autorisation, tout en précisant les modalités de l'autorisation[2060]. Il faudrait, parmi les modalités à analyser, savoir si l'autorisation est limitée dans le temps, si, quand et comment elle est sujette à renouvellement, et l'autorité qui doit l'octroyer. Si le pouvoir législatif venait à admettre qu'une annonce n'est pas suffisante, il serait préférable de passer par une autorisation émanant d'une autorité et non pas d'un organisme indépendant comme le NTC.

1359 Ces mécanismes permettraient aux autorités, ici principalement l'OFCS, d'avoir une vue d'ensemble du marché et d'assurer une qualité suffisante des prestations. En revanche, ces processus demandent une charge importante de travail pour les organisations concernées. En outre, le marché des services informatiques est très étendu en pratique, ce qui implique une difficulté de mise en œuvre de la loi. En outre, l'autorisation plus précisément requiert d'autant plus de ressources pour l'OFCS comme pour les prestataires de gestion de cyberincidents ou plus largement pour les fournisseuses de services informatiques. Finalement, qu'il s'agisse de l'obligation d'annonce ou du régime d'autorisation, il n'est pas certain que la proportionnalité d'une telle mesure soit assurée. D'une part, nous doutons que l'annonce soit apte à atteindre le

2057 OFJ, *Guide de législation*, 2019, N 843 et 847 s.

2058 Dans quel cas les relations entre l'OFCS et l'autre entité compétente devraient être clarifiées.

2059 Sur les compétences du NTC, cf. *supra* N 345. Pour un commentaire sur son rôle, cf. MEYER Pauline, *TikTok : une analyse technique helvétique des risques de sécurité*, 12 septembre 2023 (consulté le 20.3.2024).

2060 OFJ, *Guide de législation*, 2019, N 841 ss.

but d'un tel mécanisme de contrôle, dans la mesure où l'on cherche à assurer le respect d'exigences dans la fourniture de prestations de gestion cyberincidents et que l'annonce n'implique pas *de facto* ni *de jure* un contrôle. D'autre part, l'autorisation risque d'être trop intrusive dans la pratique des organisations concernées, mise dans la balance avec l'objectif poursuivi de contrôle de la qualité des prestations, dans un marché aujourd'hui très libre.

F. Une conclusion

1. Laisser le temps au temps

1360 Les bases légales doivent dès à présent intégrer des exigences supplémentaires pour encadrer dans une perspective de cybersécurité la pratique des prestataires de gestion de cyberincidents et, par la même occasion, des fournisseuses de services informatiques.

1361 Il est important de ne pas tomber dans la surréglementation. L'adoption de quelques obligations générales de cybersécurité au sein de la LSI pour les prestataires informatiques, susceptibles d'être concrétisées dans les ordonnances, est cohérente avec les évolutions actuelles comme avec les évolutions proposées dans la présente étude. En revanche, la réglementation de l'accès à la profession ou l'introduction d'un mécanisme d'autorisation reviennent à des exigences trop intrusives dans des pratiques encore très hétérogènes et laissées au marché. Il est préférable d'attendre les évolutions à venir, sur les plans pratique et politique, avant de réglementer de manière plus intrusive et de risquer une atteinte disproportionnée à la liberté économique. Certaines affaires en cours pourraient mettre en lumière de façon plus précise les lacunes légales[2061].

1362 Les responsabilités doivent dans tous les cas être bien réparties entre les prestataires informatiques et leurs clientes. Les responsabilités des clientes sur leurs infrastructures informatiques ne doivent pas être excessivement limitées par des obligations applicables à leurs prestataires de services informatiques. Les exigences auxquelles sont soumise les infrastructures critiques peuvent toujours être reprises dans les contrats les liant à des prestataires informatiques.

2061 Voir l'enquête sur la cyberattaque ayant visé l'entreprise Xplain, fournisseuse de services de sécurité informatique pour certaines autorités de la Confédération, cf. OFCS, *Rapport concernant les analyses de données effectuées après la cyberattaque contre l'entreprise Xplain*, 2024, p. 3 ; CF, *Cyberattaque contre l'entreprise Xplain: le Conseil fédéral approuve le mandat d'enquête*, 23 août 2023 (consulté le 20.3.2024).

2. En résumé, une réglementation minimaliste

Les prestataires de gestion de cyberincidents ne sont à l'heure actuelle soumises qu'à certaines exigences générales qui encadrent leur pratique. Cependant, leur pratique soulève des risques particuliers en termes de cybersécurité et leur rôle est particulièrement important. Elles revêtent comme les autres fournisseuses de services informatiques deux casquettes : celle d'infrastructure critique et celle de prestataire notamment aux autres infrastructures critiques. Une réglementation permettant d'assurer la cybersécurité dans leurs prestations peut déjà découler d'obligations légales et contractuelles, mais la loi doit être plus proactive et il est important que des procédures de contrôle de la conformité puissent être menées indépendamment de l'action d'une cocontractante ne disposant pas forcément de compétences suffisantes. C'est pour cette raison que les exigences supplémentaires susmentionnées doivent être introduites dans la LSI[2062]. La réglementation de certains aspects de la profession offre un autre angle d'approche qui permet de responsabiliser les prestataires de gestion de cyberincidents et les autres fournisseuses de services informatiques. 1363

L'introduction d'exigences supplémentaires permet également de couvrir la variété des prestations offertes en termes de produits de sécurité informatique et de services de sécurité informatique pour l'ensemble des prestataires informatiques. Une telle réflexion permet spécifiquement d'appréhender l'ensemble de la chaîne d'approvisionnement de produits informatiques qui peuvent être utilisés soit par les services de sécurité informatique soit, de façon plus large, par l'ensemble des infrastructures critiques (et le reste des organisations). Une telle démarche est aujourd'hui importante. Conjointement aux exigences minimales de cybersécurité pour les infrastructures critiques, ces exigences supplémentaires devraient aider à la clarification des responsabilités ainsi que contribuer à éviter un report des responsabilités des bénéficiaires sur les prestataires et inversement. 1364

Cette solution peut être mise en œuvre, par une section dans la LSI traitant des exigences minimales de cybersécurité pour les fournisseuses de services informatiques. La faculté accordée au CF et à l'OFCS de développer les obligations découlant de l'obligation de cybersécurité dans les prestations offertes permet au droit de s'adapter aux évolutions technologiques, comme c'est le cas pour les exigences minimales applicables aussi aux autres infrastructures critiques. En outre, comme pour ces dernières, les mécanismes analysés devraient permettre un contrôle adéquat de l'application de la loi par les prestataires informatiques. 1365

2062 Cf. *supra* N 1316 ss.

3. Une portée plus large

a. Les technologies impactées

1366 Les réflexions menées ci-dessus appréhendent les questions juridiques ayant trait à la réglementation de la cybersécurité des infrastructures critiques à la lumière de la gestion de cyberincidents. Il n'est pas exclu que ces propositions réglementaires permettent d'appréhender également d'autres questions importantes aujourd'hui. Les discussions et évolutions actuelles dans de nombreux pays illustrent la nécessité de s'interroger sur diverses problématiques, technologies ou concepts qui soulèvent des questionnements plus ou moins spécifiques. La réglementation de technologies porte aujourd'hui principalement sur trois technologies : l'intelligence artificielle (IA), l'informatique en nuage et l'Internet des objets (IdO). L'exemple le plus frappant est celui de l'IA ou des systèmes algorithmiques, qui est au centre des débats politiques sur les plans nationaux et supranationaux. Sur le plan international, plusieurs autorités ont déjà admis la nécessité de réglementer ou d'encadrer l'intelligence artificielle[2063]. La Suisse réfléchit également aux possibilités de réglementation face à de nouvelles évolutions[2064]. La CSN préconise par ailleurs de tenir compte des technologies telles que ou l'informatique en nuage ou l'IdO et de leurs évolutions dans les réflexions autour de la réglementation et de la normalisation pour la cyberrésilience en Suisse[2065].

b. L'intelligence artificielle

1367 Si l'on impose en outre des obligations renforcées de cybersécurité aux fournisseuses de services informatiques, les fabricantes de systèmes d'IA tomberaient sous le coup de cette obligation même si elles n'exploitent pas les systèmes elles-mêmes et l'entier du cycle de vie de systèmes algorithmiques devrait être sécurisé. Cela étant, il est impossible de limiter la réglementation de l'IA à cette question. En effet, l'utilisation de systèmes d'IA soulève de nombreuses autres problématiques devant être appréhendées par la loi, notamment en lien avec les devoirs de transparence sur leur fonctionnement, les risques de

2063 Voir par exemple au sein de l'UE la législation sur l'intelligence artificielle *(Artificial Intelligence Act, AI-Act),* au sujet de laquelle le Parlement européen et le Conseil ont récemment abouti à un accord, cf. COMMISSION EUROPÉENNE, *Statement by President von der Leyen on the political agreement on the EU AI Act* (consulté le 20.3.2024) ; 18 États, dont les USA et le Royaume-Uni, ont publié des lignes directrices pour le développement de systèmes d'intelligence artificielle sûrs, cf. CISA, *DHS CISA and UK NCSC Release Joint Guidelines for Secure AI System Development*, 26 novembre 2023 (consulté le 20.3.2024).

2064 En Suisse, cf. CF, *Intelligence artificielle : le Conseil fédéral examine les approches réglementaires*, 22 novembre 2023 (consulté le 20.3.2024).

2065 CF, *CSN*, 2023, p. 7 et 21.

biais et de discriminations ou encore les questions relatives à l'exactitude de leurs décisions[2066]. La Confédération a par conséquent estimé nécessaire de réglementer l'IA. Des approches réglementaires devraient être proposées au plus tard fin 2024[2067]. L'analyse des approches réglementaires devrait se baser sur le droit suisse tout en assurant une compatibilité avec le Règlement européen sur l'intelligence artificielle (AI-Act)[2068] et avec la Convention du Conseil de l'Europe sur l'intelligence artificielle (CAI). Cette réglementation devra appréhender les aspects autres que liés à la sécurité, mais également la sécurité pour les organisations non critiques qui exploitent des systèmes d'IA. Bien que les modifications de la LSI proposées dans la présente étude puissent permettre d'appréhender certains éléments liés aux risques aujourd'hui posés par l'utilisation de système IA, d'autres questions doivent être approfondies afin de réglementer ces technologies de façon satisfaisante[2069]. Si une nouvelle loi venait à être adoptée, l'interaction entre cette dernière et la LSI devrait être réglée.

c. L'internet des objets

Si des exigences minimales étaient à introduire dans la LSI pour les infrastructures critiques, mais surtout pour les fournisseuses de services informatiques, les fabricantes d'IdO et les infrastructures critiques exploitant des objets connectés seraient soumises à des exigences de cybersécurité pour ces objets. Ces exigences permettraient d'assurer la cybersécurité d'objets connectés durant l'entier de leur cycle de vie. Une telle réglementation permettrait d'apporter une complémentarité dans l'applicabilité des art. 96 ss OST et des autres normes applicables. 1368

d. L'informatique en nuage

Il existe aujourd'hui des exigences sectorielles de cybersécurité, des exigences transversales de données personnelles et relatives aux informations soumises à des secrets. Certaines exigences contraignantes devraient bientôt voir le 1369

2066 Comme relevé par le CF dans ses lignes directrices, CF, « Intelligence artificielle » – lignes directrices pour la Confédération, 2020, p. 5 ; OFCOM, *Suivi des lignes directrices « Intelligence artificielle » pour la Confédération*, 2022, p. 3 ss.

2067 CF, *Intelligence artificielle : le Conseil fédéral examine les approches réglementaires*, 22 novembre 2023 (consulté le 20.3.2024).

2068 Le Règlement européen sur l'intelligence artificielle prévoit des obligations de cybersécurité, d'information et ainsi de suite (cf. art. 8 ss AI-Act).

2069 En parallèle des initiatives privées qui commencent à voir le jour, à l'instar de l'« AI Alliance » qui compte plusieurs dizaines de membres s'engageant pour un développement des technologies d'IA responsables (consulté le 20.3.2024).

jour s'agissant concrètement de l'utilisation de solutions en nuage[2070]. Par les propositions législatives de la présente étude relatives aux exigences minimales de cybersécurité pour les infrastructures critiques, les infrastructures critiques utilisant des solutions en nuage devraient s'assurer dans leurs collaborations avec des organisations tierces que les exigences et mesures prévues par la LSI sont reprises dans les accords et les contrats, dont la mise en œuvre doit être contrôlée (art. 9 LSI par analogie). Partant, l'infrastructure critique qui utiliserait une solution d'informatique en nuage devrait s'assurer que l'entreprise lui fournissant la solution en garantit également la cybersécurité.

1370 En outre, les fournisseuses de solutions en nuage tombent dans le soussecteur critique des services informatiques. L'adoption de la seconde proposition législative de la présente étude impliquerait des exigences supplémentaires de cybersécurité pour ces organisations. C'est pour inclure ce type de fournisseuses de prestations que la proposition de réglementation doit porter sur l'ensemble du soussecteur critique des services informatiques sans se limiter aux fournisseuses de services de sécurité informatique et de prestations de gestion de cyberincidents. Par ailleurs, en raison des fournisseuses importantes de solutions d'informatique en nuage ayant un siège à l'étranger, il nous semble nécessaire que ces exigences minimales ne soient pas limitées aux organisations ayant un siège en Suisse[2071].

1371 En parallèle, il va de soi que les lois sur la protection des données applicables aux organisations recourant à des solutions d'informatique en nuage continuent de s'appliquer, de la même façon que les dispositions sur les secrets lorsqu'il existe un ou plusieurs secrets ou des législations spécifiques à un cercle d'utilisatrices de solutions en nuage[2072].

1372 Il n'est pas exclu qu'une réglementation ayant d'autres vocations que la cybersécurité soit nécessaire, raison pour laquelle l'OFCOM examine actuellement quelles exigences s'imposent dans l'informatique en nuage[2073]. Il est important de réfléchir aux différentes incitations pour les risques divers et variés qui entourent l'informatique en nuage, à l'instar des risques politiques ou réputationnels liés à la conclusion de contrats pour des services en nuage

2070 Une directive contraignante pour l'administration fédérale devrait être adoptée dans le contexte de la migration vers Microsoft 365 afin notamment d'indiquer où les diverses informations doivent être stockées dans le nuage de Microsoft, cf. CF, *Deux premières unités administratives passent à Microsoft 365*, 22 février 2024 (consulté le 20.3.2024).

2071 Contrairement à ce que prévoit actuellement la LSI pour l'obligation de signaler les cyberattaques visant de telles fournisseuses de services informatiques. À ce sujet, cf. *supra* chapitre 9, II.D.2.

2072 Voir ChF, *Cadre juridique pour l'utilisation de services d'informatique en nuage public au sein de l'administration fédérale*, 2022, p. 12 ss.

2073 CF, *CSN*, 2023, p. 21.

entre l'administration fédérale et certaines prestataires[2074]. D'autres autorités revêtent également des rôles importants dans ce contexte, à l'instar de l'Office fédéral de l'informatique et de la télécommunication (OFIT), qui exploite et soutient pour le moment en particulier l'administration fédérale dans l'utilisation de solutions informatiques[2075].

e. La chaîne d'approvisionnement

En parallèle des lois usuelles de protection des données et de sécurité des produits, certaines réglementations sectorielles imposent des obligations de vérification ou de contrôle, comme dans le sous-secteur critique de l'approvisionnement en électricité ou des autorités. Les autorités soumises à la LSI ou les organisations soumises à la LApEl sont par exemple soumises aux contrôles de sécurité relatifs aux personnes (art. 20*a* LApEl et 27 ss LSI). Un autre moyen de vérification prévu par la loi est le contrôle de la mise en œuvre lors de la collaboration avec des tierces (art. 9 LSI)[2076]. 1373

Les propositions législatives de la présente étude visant l'introduction d'exigences de cybersécurité pour les infrastructures critiques et pour les fournisseuses de services informatiques en particulier devraient permettre à chaque intervenante d'assurer la sécurité des produits et des prestations informatiques à chaque étape d'un produit, d'un système ou d'une prestation et ce pour chaque intervenante dans l'approvisionnement et le cycle de vie. En revanche, pour les produits et systèmes exploités par d'autres organisations ou personnes que des infrastructures critiques, seules les prestataires de produits et de services informatiques seraient soumises à des obligations de sécurité. Il s'agirait là déjà d'un progrès non négligeable par rapport à la situation actuelle. 1374

II. La réglementation de l'activité de l'OFCS

A. La nécessité d'une réglementation exclusive

Contrairement aux autres prestataires de gestion de cyberincidents, l'OFCS est investi d'une mission d'intérêt public. En tant qu'autorité, l'OFCS est soumis au principe de la légalité et son activité doit donc reposer sur la loi. La 1375

2074 ChF, *Cadre juridique pour l'utilisation de services d'informatique en nuage public au sein de l'administration fédérale,* 2022, p. 10.

2075 Cf. *supra* N 262.

2076 CF, *Rapport « Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense »,* 2021, p. 16 s. ; FF 2017 2765, p. 2831 et 2846 ss.

législation applicable à l'autorité et son équipe d'intervention doit pour ces raisons différer de la réglementation applicable aux autres prestataires de gestion de cyberincidents.

1376 GovCERT constitue l'un des services de l'OFCS, dont les compétences sont réglementées explicitement et dont l'activité soulève d'autres questions en relation avec la cybersécurité des infrastructures critiques. Par conséquent, les questions de réglementation de l'activité de GovCERT doivent être traitées conjointement aux questions concernant l'OFCS.

B. Le principe de la légalité

1. Un rappel de la situation actuelle

1377 La LSI2 définit les missions principales du NCSC, autorité principale en matière de cybersécurité en Suisse (art. 73*a* ss LSI2), qui s'est transformée le 1er janvier 2024 en OFCS. L'OFCS est le NCSC (art. 15a al. 1 Org-DDPS). Parallèlement, le service spécialisé de la Confédération pour la sécurité de l'information a été mis sur pied (art. 83 LSI), qui s'est vu attribuer certaines compétences qui incombaient avant janvier 2024 au NCSC. L'aOPCy, abrogée à l'entrée en vigueur de la LSI, prévoyait plus précisément le rôle de GovCERT à son art. 12 al. 1 litt. c. L'art. 15*a* al. 2 litt. f Org-DDPS prévoit que l'OFCS gère l'équipe d'intervention de GovCERT pour aider les infrastructures critiques à se protéger contre les cybermenaces[2077].

1378 Comme déjà relevé[2078], la formulation dans une ordonnance législative selon laquelle l'OFCS est le NCSC n'est pas satisfaisante, bien que l'on comprenne l'intention de l'autorité législative de simplifier la révision de la LSI. Cela étant, cette disposition manque de clarté juridique et doit être temporaire. Pour des raisons de clarté juridique, le cadre légal doit (le plus rapidement possible) harmoniser les notions et que seul l'OFCS soit mentionné, dès lors que le NCSC n'existe plus et a justement été transformé en office.

1379 Les compétences de cybersécurité du nouvel office figurent aux art. 73*a* ss LSI2 (concrétisées dans le P-OCyS), à l'art. 43 OSI et à l'art. 15*a* Org-DDPS. Les compétences de l'OFCS décrites dans l'OSI ne concernent que la première version de la LSI et visent les compétences de l'OFCS en lien avec la sécurité de l'information des autorités et organisations de la Confédération. Ses compétences de cybersécurité auprès des infrastructures critiques devraient

2077 Pour plus d'informations sur les enchevêtrements de compétences entre l'OFCS et le service spécialisé de la Confédération pour la sécurité de l'information et sur le rôle de GovCERT dans cette nouvelle organisation, cf. *supra* N 781 ss.

2078 Cf. *supra* N 704.

être précisées expressément dans la seconde version de l'ordonnance, par suite de l'adoption de la LSI2. L'OSI confère un rôle technique important à l'OFCS en lien avec la cybersécurité. L'art. 15 al. 2 Org-DDPS ainsi que le rapport explicatif de l'OSI précisent que l'OFCS est la destinataire des signalements de cyberattaques en vertu des art. 74*a* ss LSI2 et qu'il soutient les infrastructures critiques dans le cadre de leur protection contre les cybermenaces[2079]. Par conséquent, nous pouvons en déduire que l'OFCS va conserver les compétences détenues précédemment par le NCSC en vertu des art. 73*a* ss LSI2 pour la cybersécurité des infrastructures critiques (comme également prévu à l'art. 15*a* al. 2 litt. f OrgDDPS). La présente étude partira de ce postulat pour la formulation d'une piste réglementaire.

2. L'OFCS, son équipe technique et le principe de la légalité

Le principe de la légalité, selon lequel le droit est la base et la limite de l'activité de l'État, est la pierre angulaire régissant l'action étatique[2080]. Son premier sous-principe est celui de la primauté de la loi, selon lequel l'État est tenu par la loi dans le cadre de ses activités ; celui-ci n'agit pas valablement en violant une norme légale et il reste tenu d'agir en conformité avec les buts, moyens, conditions et circonstances autorisées par la loi. Le second sous-principe est celui de la réserve de la loi, selon lequel l'État ne peut pas agir si la loi ne prévoit aucune action[2081]. Le principe de la légalité (art. 5 Cst.), dans la variante de la réserve de la loi, implique que toute activité étatique doit reposer sur une règle de droit[2082]. Les dispositions importantes relatives aux tâches et aux prestations de la Confédération doivent figurer dans une loi au sens formel (art. 164 al. 1 litt. e Cst.). 1380

La seule mention légale de GovCERT se trouve à l'heure actuelle à l'art. 15*a* al. 2 litt. f Org-DDPS. La disposition prévoit que GovCERT est l'équipe d'intervention gérée par l'OFCS pour soutenir les infrastructures critiques dans le cadre de leur protection contre les cybermenaces. Son mandat devrait être précisé dans la future ordonnance sur la cybersécurité (art. 7 P-OCyS9). 1381

L'art. 12 aOPCy prévoyait que GovCERT était « dirigée » par le NCSC. La mention à l'art. 15*a* al. 2 litt. f Org-DDPS selon laquelle GovCERT est « gérée » par l'OFCS n'a pas de réel impact selon l'opinion défendue par la présente étude ; prévoir que GovCERT est gérée par l'OFCS est suffisant. Il est raisonnable que 1382

2079 SG-DDPS, *Législation d'exécution relative à la LSI, Explications*, 2023, p. 6.

2080 CR Cst.-DUBEY, art. 5 N 6.

2081 OFJ, *Guide de législation*, 2019, N 717 ; CR Cst.-DUBEY, art. 5 N 6 s. et 38 ss ; MEYER/MÉTILLE, *Computer security incident response teams : are they really regulated ? The Swiss example*, 2022, p. 11 ; SURY, *Digital in Law*, 2021, p. 16 et 277.

2082 CR Cst.-DUBEY, art. 5 N 38.

la loi prévoie les compétences de l'OFCS et pas de son service d'intervention. La description des tâches de l'OFCS est suffisante sans que la mission de ses services soit expressément prévue par la loi. Au demeurant, la conservation de la mention de GovCERT dans les bases légales, ainsi que le prévoit l'art. 15*a* Org-DDPS, est opportune. Nous pouvons tout de même nous demander si l'art. 15*a* Org-DDPS dispose d'une densité normative acceptable ou s'il est préférable de décrire plus précisément dans l'Org-DDPS ou dans l'OSI les tâches de GovCERT comme c'était le cas à l'art. 12 aOPCy.

1383 L'art. 12 al. 1 litt. c aOPCy prévoyait un rôle plus étendu pour GovCERT. La disposition instituait GovCERT comme service spécialisé national pour la gestion technique des cyberincidents, pour l'analyse des questions techniques, pour l'évaluation technique des menaces et pour l'appui technique au guichet unique suisse. Il est préférable que l'art. 15*a* Org-DDPS ou que l'OSI prévoie plus explicitement le mandat et les compétences de GovCERT en tant que service technique de l'OFCS, mais il n'est pas nécessaire que les bases légales aillent plus loin dans la description du mandat de l'équipe d'intervention. Si le mandat de GovCERT venait néanmoins à être précisé, il serait suffisant qu'une ordonnance le prévoie. En effet, dans la mesure où les compétences de l'autorité à laquelle GovCERT est rattachée sont décrites dans la loi et qu'elle lui apporte principalement un soutien technique, il ne s'agit pas d'une disposition importante au sens de l'art. 164 al. 1 Cst. L'art. 15*a* al. 2 litt. f Org-DDPS remplit cette fonction.

1384 Ensuite, l'OFCS et son service technique détiennent des compétences hors de la gestion de cyberincidents particulièrement importantes dans le contexte de la cybersécurité des infrastructures critiques. Il est donc nécessaire d'analyser comment la loi doit permettre à leur position d'évoluer. Nous allons voir comment le NCSC en tant que nouvel office, avec l'appui technique de GovCERT, peut évoluer pour détenir des compétences plus étendues et plus claires afin d'assurer la cybersécurité, en particulier auprès des infrastructures critiques. Les compétences doivent porter sur le contrôle de l'application de la loi. Elles passent aussi par l'implication de l'OFCS dans les mécanismes de certification, par les contrôles qu'il devrait pouvoir réaliser à son initiative ou encore par le prononcé d'avertissements et de recommandations[2083].

C. Le droit européen comme point de comparaison

1. Les autorités de la Directive SRI2 et leurs compétences principales

1385 Le droit européen constitue régulièrement une source d'inspiration et un point de comparaison pour le droit suisse. La Directive SRI2, modifiant la

2083 Cf. *supra* N 1272 ss.

Directive (UE) 2016/1148 ou Directive SRI, est plus mûre que la LSI en Suisse. Il est intéressant de s'inspirer des avancées européennes, des enseignements liés à la révision de la directive et des premiers retours pratiques pour se questionner sur le rôle des autorités compétentes en Suisse et sur la façon de contrôler au mieux l'application des réglementations[2084].

La Directive SRI2 impose aux États membres de désigner ou d'établir une ou plusieurs autorités compétentes chargées de la cybersécurité et de contrôler le respect de la directive (art. 8 par. 1 Directive SRI2)[2085], un point de contact unique (art. 8 par. 3 Directive SRI2)[2086], une ou plusieurs autorités de gestion des incidents de cybersécurité majeurs et de crises[2087] coordonnant ces dernières (art. 9 par. 1 Directive SRI2) ainsi qu'une ou plusieurs CSIRT (art. 10 Directive SRI2). Ces dernières assument des tâches de surveillance et d'analyse des cybermenaces, vulnérabilités et incidents au niveau national, de soutien aux entités « essentielles » et « importantes » face aux incidents, de coordination pour la divulgation de vulnérabilités ou encore de contribution au déploiement d'outils de partage d'informations sécurisés (art. 11 par. 3 Directive SRI2)[2088]. 1386

Les autorités chargées de la cybersécurité et du contrôle du respect de la directive peuvent mener auprès des entités importantes et essentielles au sens de l'art. 3 Directive SRI2[2089] des inspections sur place et des contrôles à distance ex post, des audits de sécurité ciblés effectués par des organismes indépendants ou des autorités compétentes, des scans de sécurité (réalisés sur des critères d'évaluation des risques répondant à certains critères) conformément aux art. 32 par. 2 et 33 par. 2 de la directive. Elles peuvent également formuler des demandes d'informations nécessaires à l'évaluation *ex post* des mesures de gestion des risques pour la cybersécurité, des demandes d'accès à des données, documents et informations nécessaires à ses tâches de supervision ou des demandes de preuves de la mise en œuvre de politiques de cybersécurité (art. 32 par. 2 et 33 par. 2 Directive SRI2). Ces autorités ont le pouvoir d'émettre des avertissements lors de violations de la directive, d'adopter des 1387

2084 Voir notamment c. 2 ss Directive SRI2.

2085 C. 38 et 122 ss Directive SRI2.

2086 C. 39 s. Directive SRI2.

2087 Un incident de cybersécurité majeur est « un incident qui provoque des perturbations dépassant les capacités d'action du seul État membre concerné ou qui frappent plusieurs États membres », qui peut dégénérer en se transformant en crise à part entière, qui empêcherait le bon fonctionnement du marché intérieur ou qui présenterait de graves risques de sûreté et de sécurité publique pour plusieurs États membres, c. 69 Directive SRI2.

2088 C. 41 ss Directive SRI2.

2089 Les notions d'entités essentielles et importantes sont similaires à la notion en Suisse d'infrastructures critiques.

instructions contraignantes ou d'enjoindre les entités à pallier les insuffisances ou aux violations constatées. Elles peuvent aussi ordonner aux entités de mettre un terme à un comportement violant la directive, de ne pas le réitérer, de garantir leur conformité avec la directive de manière spécifique et dans un délai déterminé, de procéder à des informations, de mettre en œuvre des recommandations ou de rendre publics des aspects des violations de la directive (art. 32 par. 4, 33 par. 4 Directives SRI). Ces autorités doivent finalement pouvoir imposer ou demander aux organes compétents d'infliger des amendes administratives (art. 32 par. 4 et 33 par. 4 Directives SRI, lesquels renvoient à l'art. 34 Directive SRI2). Les autorités chargées de la cybersécurité disposent de compétences supplémentaires s'agissant des entités essentielles, avec la possibilité de soumettre celles-ci à des audits *ad hoc* lorsqu'ils sont justifiés (art. 32 par. 2 litt. c Directive SRI2), de désigner temporairement une responsable du contrôle pour superviser le respect de la directive (art. 32 par. 4 litt. g Directive SRI2) ou de faire suspendre une certification (art. 32 par. 6 Directive SRI2).

1388 Les points de contact uniques remplissent naturellement une fonction de liaison et permettent d'assurer la coopération transfrontière des autorités de l'État membre et des autres États membres de l'UE, avec les autorités européennes compétentes ainsi que la coopération intersectorielle avec les autres autorités de l'État membre (art. 8 par. 4 Directive SRI2). À noter que la directive n'impose pas l'autorité devant recevoir les notifications d'incidents et de cybermenaces ; elle précise en revanche que les points de contact uniques doivent être informés de ces menaces (art. 13 par. 3 Directive SRI2).

1389 L'autorité ou les autorités de gestion des crises cyber coordonne la gestion des incidents de cybersécurité majeurs et les crises cyber (art. 9 par. 1 et 2 Directive SRI2)[2090].

1390 Les CSIRT surveillent et analysent les cybermenaces, les vulnérabilités et les incidents au niveau national. Sur demande, elles apportent une assistance aux entités essentielles et importantes pour surveiller en temps réel ou quasi réel leurs réseaux et systèmes d'information (art. 11 par. 3 litt. a Directive SRI2). Elles activent en outre au plus vite les mécanismes d'alerte précoce, de diffusion de messages d'alerte, les annonces et la diffusion d'informations sur les cybermenaces, les vulnérabilités ou les incidents pour les entités essentielles et importantes concernées, pour les autorités compétentes ou pour les parties prenantes concernées (art. 11 par. 3 litt. b Directive SRI2). Elles réagissent aux incidents et apportent une assistance aux entités essentielles et importantes concernées, rassemblent et analysent des données de police scientifique en

2090 Compétence à mettre en lien avec le réseau européen pour la préparation et la gestion des crises cyber (EU-CyCLONe), art. 9 par. 5 et art. 16 Directive SRI2 ; c. 68 ss Directive SRI2.

assurant une analyse dynamique des risques et incidents ainsi qu'une appréciation de la situation de cybersécurité (art. 11 par. 3 litt. c et d Directive SRI2). Les CSIRT réalisent à la demande d'entités essentielles ou importantes des scans proactifs du réseau et des systèmes d'information, participent au réseau des CSIRT en apportant une assistance mutuelle et contribuent au déploiement d'outils de partage d'informations sécurisés (art. 11 par. 3 litt. f, h Directive SRI2). Elles peuvent également être désignées comme coordinatrices dans le processus de divulgation coordonnée de vulnérabilités (art. 11 par. 3 litt. g et art. 12 Directive SRI2). Elles détiennent également un rôle de point de contact en échangeant des informations avec les communautés sectorielles et intersectorielles d'entités essentielles et importantes, en coopérant avec le réseau des CSIRT, avec les centres de réponse aux incidents de sécurité informatique nationaux des pays tiers ou au sein de réseaux de coopération internationale en vertu des art. 10 par. 4 et 6 à 8 et art. 11 par. 1 Directive SRI2.

2. La difficulté de comparer les deux systèmes

La situation helvétique pour la cybersécurité est en pleine évolution et l'OFCS a remplacé le NCSC comme autorité principale pour la cybersécurité. L'art. 15*a* Org-DDPS prévoit à son alinéa 1 que l'OFCS équivaut au NCSC. L'office fédéral voit ses compétences principales en la matière définies à l'art. 73*a* ss LSI2 et à l'art. 15*a* Org-DDPS. L'art. 43 OSI précise des compétences du nouvel OFCS en lien avec la sécurité de l'information au sein de la Confédération. 1391

L'on comprend de ces considérations que la situation actuelle peut être délicate à comparer au système européen. Premièrement, la Suisse n'est pas un État membre de l'UE et ne fonctionne pas d'une manière similaire à celle de l'UE. Deuxièmement, l'organisation helvétique n'est pas aussi construite que l'organisation européenne pour le domaine de la cybersécurité ; la LSI et son ordonnance ne fixent pas un cadre aussi précis et complet que celui mis en place par la Directive SRI2. Troisièmement, l'organisation de la cybersécurité au sein de la Confédération est en pleine évolution. 1392

En revanche, ce n'est pas un problème que la CSIRT suisse soit intégrée à une autre autorité. GovCERT se limite à être un service de l'OFCS, qui semble détenir de façon plus expresse la majorité des compétences attribuées par la Directive SRI2 à des autorités distinctes. Le droit européen n'exclut pas que les différentes autorités soient réunies au sein d'une même entité dans un État membre (voir par exemple art. 8 par. 3 Directive SRI2). Le fait qu'il existe une autorité centrale avec différents services en Suisse implique que l'OFCS est susceptible de remplir des tâches similaires à celles des CSIRT, des autorités chargées de la cybersécurité, des points de contact uniques, de la Commission ou de l'ENISA. 1393

1394 L'OFCS occupe par ses compétences des art. 73*a* ss LSI2 une position similaire à celles des autorités chargées dans l'UE de la cybersécurité. Ses compétences de contrôle du respect de l'obligation de signaler les cyberattaques ont été conservées lors de sa transformation en office fédéral[2091]. Ce faisant, ses compétences peuvent servir de fondement pour que la réorganisation de la cybersécurité au sein de la Confédération se fasse de façon optimale. Des ajustements sont requis pour que ses compétences essentielles se fondent sur des bases légales adéquates. Il n'est pas exclu que le P-OCyS, concrétisant la LSI2, comporte des modifications ou des précisions dans les compétences de l'OFCS, du service spécialisé de la Confédération pour la sécurité de l'information et de GovCERT. Cela étant, il est possible d'analyser quelles compétences devraient être ajustées pour être plus adaptées à la gestion de cyberincidents et au soutien des infrastructures critiques dans leur cybersécurité, ainsi que pour permettre une réorganisation optimale de la cybersécurité au sein de la Confédération. Cet examen doit se faire à la lumière de la Directive SRI2 afin de déterminer si les directions suisses et européennes sont similaires et, en même temps, de s'intéresser à un droit plus évolué s'agissant des différents rôles de l'OFCS.

D. Les changements nécessaires

1. Les compétences de soutien

a. Les compétences générales, préventives et détectives

1395 De façon générale, l'OFCS est compétent sur la base de l'art. 73*a* al. 1 LSI2 et de l'art. 15*a* al. 2 litt. b Org-DDPS pour réaliser des analyses techniques afin d'évaluer et contrer les cyberincidents et les cybermenaces. Ses analyses techniques lui permettent aussi d'identifier et éliminer les vulnérabilités dans le cadre de la protection de la Suisse contre les cybermenaces (art. 73*a* al. 1 *in fine* LSI2 et art. 15*a* al. 2 litt. b *in fine* Org-DDPS). Cette compétence impacte naturellement les infrastructures critiques dans la mesure où les informations et le soutien que l'OFCS et GovCERT leur fournissent dépendent en partie de ces analyses techniques et de leurs résultats[2092].

1396 Afin de rester dans le périmètre de la présente étude, la suite des compétences analysées se réfère exclusivement aux compétences de l'autorité compétente pour la cybersécurité des infrastructures critiques, à savoir l'OFCS et non d'autres autorités. Nous estimons en outre que l'OFCS peut apporter, notamment par le biais de GovCERT, son soutien aux infrastructures critiques

2091 SG-DDPS, *Législation d'exécution relative à la LSI, Explications*, 2023, p. 6.

2092 C'est aussi à la suite de ces analyses que le NCSC alerte les personnes concernées en cas de cybermenaces en vertu de l'art. 73*a* al. 2 litt. b LSI2, de façon similaire aux CSIRT dans l'UE (art. 11 par. 3 litt. b Directive SRI2).

à différentes étapes de la gestion de cyberincidents, de vulnérabilités et d'autres cybermenaces. Ce soutien peut se faire par l'élaboration de lignes directrices non contraignantes et le partage d'informations et d'outils, comme par des recommandations plus concrètes ou par un soutien pratique.

Pour répondre aux besoins accrus des infrastructures critiques, l'art. 74 al. 2 litt. b et c LSI2 habilite l'OFCS, avec l'aide de GovCERT, à diffuser des informations, des recommandations, des instruments et des instructions à ces organisations sur les mesures préventives, détectives et réactives à prendre contre les cyberincidents[2093]. L'OFCS met également à disposition un système de communication pour un échange sécurisé d'informations (art. 74 al. 1 litt. a LSI2). Ce genre de tâches reviennent en principe aux CSIRT dans l'UE (art. 11 par. 3 litt. f et h Directive SRI2). Il n'est pas exclu que ces compétences soient précisées dans l'ordonnance révisée, mais cette base légale permet déjà à l'OFCS ainsi qu'à son équipe technique de soutenir les infrastructures critiques dans l'implémentation de mesures permettant d'assurer leur cybersécurité et de bénéficier des outils techniques de l'OFCS. 1397

En droit européen, les CSIRT sont compétentes pour assister les infrastructures critiques, sur demande, en les assistant dans la surveillance en temps réel ou quasi réel de leurs réseaux et systèmes d'information. Elles sont également compétentes pour réaliser des scans proactifs du réseau et des systèmes d'information (art. 11 par. 3 Directive SRI2). En Suisse, l'art. 43 al. 1 litt. c OSI octroie la faculté à l'OFCS de rechercher des menaces et vulnérabilités techniques sur Internet ou, moyennant concertation avec les responsables de la sécurité de l'information et les fournisseuses de prestations, dans l'infrastructure informatique de l'administration fédérale, compétence qu'il peut déléguer[2094]. En revanche, la loi n'est pas claire quant aux compétences de l'OFCS (ou de l'ancien NCSC) pour mener de telles mesures en prévention d'un cyberincident auprès de l'ensemble des infrastructures critiques. 1398

b. Les compétences réactives

Comme en droit européen (art. 23 par. 1 Directive SRI2), la réception et le traitement de signalements par l'OFCS entraînent plusieurs conséquences en matière de compétences. 1399

2093 FF 2023 84, p. 30 s. ; MEYER/MÉTILLE, *Loi fédérale sur la sécurité de l'information : version 2.0,* 2022, N 38. L'art. 43 al. 1 litt. a OSI habilite par ailleurs l'OFCS à conseiller plus spécifiquement l'administration fédérale, l'armée et les organes de sécurité de la Confédération au sujet des questions liées à la sécurité technique de l'information. GovCERT participe aux recommandations de mesures faites aux autorités de la Confédération en lien avec des menaces opérationnelles dans le domaine technique si la sécurité de l'information de la Confédération est menacée (art. 83 al. 1 litt. b LSI), cf. FF 2017 2765, p. 2877.

2094 SG-DDPS, *Législation d'exécution relative à la LSI, Explications,* 2023, p. 25.

1400 Si une infrastructure critique soumise à l'obligation de signaler les cyberattaques (art. 74*a* ss LSI2) effectue un tel signalement, l'OFCS la conseille et la soutient dans la gestion de l'attaque[2095]. Les infrastructures critiques de l'art. 74*b* LSI2 ont droit à ce soutien en vertu de l'art. 74*a* al. 3 LSI2 dans les cas de l'art. 74*d* LSI2[2096].

1401 L'OFCS peut également conseiller et soutenir l'ensemble des infrastructures critiques dans la gestion des cyberincidents et dans l'élimination des vulnérabilités lorsque le fonctionnement de l'infrastructure critique concernée est en péril (art. 74 al. 3 LSI2)[2097]. L'art. 74 al. 3 LSI2 prévoit également que l'OFCS peut conseiller et soutenir les infrastructures critiques privées dans la gestion de cyberincidents et l'élimination de vulnérabilités à condition, en plus que l'infrastructure soit en péril, qu'il ne soit pas possible d'obtenir un soutien équivalent sur le marché en temps voulu. Cette mesure est limitée à un soutien d'urgence subsidiaire encadré par des conditions strictes, ce qui permet d'éviter une distorsion de la concurrence[2098]. Cette mesure se fonde sur une base légale, poursuit un intérêt public, est proportionnelle et respecte la neutralité concurrentielle. Partant, elle ne viole pas la liberté économique (art. 94 Cst.)[2099].

1402 Actuellement, les infrastructures critiques n'ont droit au soutien de l'OFCS que dans la réaction aux cyberattaques devant être signalées. Compte tenu de l'importance pratique des infrastructures critiques dans la protection de la Suisse contre les cybermenaces, l'OFCS et GovCERT doivent être obligées de soutenir les infrastructures critiques plus largement et non uniquement lors de signalements de cyberattaques en vertu des art. 74*a* ss LSI2. Une obligation faite à l'OFCS de soutenir les infrastructures critiques face à l'ensemble des cybermenaces auxquelles elles sont confrontées est inconvenable au vu des ressources actuelles de l'OFCS. En revanche, une formulation imposant à l'OFCS d'aider les infrastructures qui le demandent ou en cas de cyberincident ou de vulnérabilité atteignant un certain seuil de gravité est préférable à la situation actuelle[2100]. L'obligation de signaler les cyberattaques devait par ailleurs initialement être une obligation de signaler les

2095 FF 2023 84, p. 33.

2096 FF 2023 84, p. 31 et 43.

2097 FF 2023 84, p. 30.

2098 Cette subsidiarité s'applique dans le cadre de l'art. 74 LSI2 comme lorsque l'OFCS apporte un soutien technique dans le cadre de l'obligation de signaler les cyberattaques, cf. FF 2023 84, p. 31.

2099 ATF 138 I 378, c. 6 ; CR Cst.-MARTENET, art. 94 N 29. À ce sujet, cf. *supra* N 128 ss.

2100 Ce qui supposera bien entendu un travail de collaboration, comme cela a été le cas pour l'analyse des informations compromises à la suite de l'attaque d'Xplain, cf. OFCS, *Rapport concernant les analyses de données effectuées après la cyberattaque contre l'entreprise Xplain,* 2024, p. 7.

cyberincidents[2101]. En outre, l'introduction d'une obligation de signaler les vulnérabilités en plus des cyberattaques a été proposée par le Conseil national durant les débats parlementaires[2102]. Pour respecter la liberté économique et la subsidiarité de l'intervention étatique, il conviendrait de s'assurer que l'aide fournie par l'OFCS est subsidiaire à celle du marché (comme le prévoit pour la gestion de cyberincidents et de vulnérabilités l'art. 74 al. 3 LSI2). L'attribution de plus de compétences d'exécution de la loi devrait permettre d'éclaircir la répartition entre les compétences de l'OFCS et des actrices privées.

1403 Hors du contexte des échanges entre infrastructures critiques et l'OFCS, des cybermenaces et cyberincidents peuvent être signalés à cette autorité par toute personne. Lorsque l'OFCS reçoit de tels signalements au sujet de vulnérabilités (faisant partie des signalements volontaires de l'art. 73*b* LSI2), il peut notamment émettre une recommandation, sur demande, quant aux mesures à prendre, à condition qu'aucune analyse ou clarification supplémentaire ne soit nécessaire (art. 73*b* al. 2 LSI2)[2103]. Il occupe un rôle similaire à celui des CSIRT européennes dans le cadre de la procédure de divulgation coordonnée des vulnérabilités *(coordinated vulnerability disclosure)*[2104]. Cette procédure consiste en l'information de la fabricante du logiciel ou du matériel informatique pour l'inciter à éliminer la vulnérabilité[2105]. C'est une compétence importante des CSIRT[2106].

1404 L'assistance que l'OFCS peut apporter est plus limitée que dans l'UE, mais des considérations pratiques relatives notamment à ses ressources peuvent expliquer cette décision. En outre, le droit européen prévoit que l'ENISA met à disposition une base de données relatives aux vulnérabilités (art. 12 par. 2 Directive SRI2), ce qui n'est pas prévu en droit suisse. Cette base de données permet notamment aux différentes entités et fournisseuses de réseaux et de systèmes d'information de divulguer et enregistrer à titre volontaire les vulnérabilités publiées (art. 12 par. 2 Directive SRI2). L'OFCS peut toutefois publier des informations relatives aux logiciels vulnérables, à condition que la fabricante y consente ou qu'elle n'ait pas éliminé la vulnérabilité dans le délai imparti par l'OFCS en vertu de l'art. 73*b* al. 3 LSI2 (art. 73*c* LSI2)[2107]. La

2101 CF, *Rapport « Obligation de déclarer les incidents graves affectant la sécurité des infrastructures critiques »,* 2019, p. 3 ss.

2102 BO 2023 N 555.

2103 FF 2023 84, p. 26 s.

2104 Au sujet du processus de divulgation coordonnée des vulnérabilités, cf. notamment CF, *La promotion du piratage éthique en Suisse,* 2023, p. 8.

2105 FF 2023 84, p. 27. Cette compétence devrait être précisée dans l'OCyS (art. 9 P-OCyS).

2106 Cf. à titre de comparaison art. 11 par. 3 litt. g et art. 12 Directive SRI2.

2107 FF 2023 84, p. 28.

loi ne prévoit pas clairement que l'OFCS met à disposition une base de données pour que les différentes organisations (critiques ou non) puissent avoir accès à ces informations. En revanche, l'OFCS est compétent pour publier des informations sur la cybersécurité (art. 73*a* al. 2 litt. b LSI2). Alors que l'on pourrait se demander s'il devrait tenir une telle base de données, GovCERT semblait en pratique déjà publier fréquemment des informations techniques sur les vulnérabilités existantes[2108]. Il n'est par ailleurs pas exclu que l'OFCS et GovCERT mettent à disposition des infrastructures critiques davantage d'informations sur des vulnérabilités sur la base de l'art. 74 al. 2 litt. b LSI2.

1405 Les compétences de l'OFCS et, partant, de GovCERT, se rapprochent en termes de soutien de ce qui est prévu par la Directive SRI2 sur sol européen. Alors que l'art. 74 al. 3 LSI2 octroie seulement la possibilité à l'OFCS de soutenir et conseiller toutes les infrastructures critiques dans la gestion des cyberincidents et des vulnérabilités, la formulation de l'art. 74*a* al. 4 LSI2 pose plus fermement le principe selon lequel le signalement de cyberattaques par les infrastructures critiques les plus importantes en Suisse donne lieu à des recommandations de l'OFCS. En d'autres termes, seules les infrastructures assujetties à l'obligation des art. 74*a* ss LSI2 ont droit au soutien technique apporté par l'OFCS et GovCERT dans ce cadre[2109]. Partant, la présente étude estime que l'introduction d'exigences minimales devrait permettre à l'ensemble des infrastructures critiques de bénéficier, *de facto* et *de jure,* des recommandations de l'OFCS et de son soutien, en tenant compte de la liberté économique et de la subsidiarité de l'intervention étatique. Pour ce faire, il conviendrait de s'assurer que l'aide fournie par l'OFCS est subsidiaire à celle du marché (comme le prévoit pour la gestion de cyberincidents et de vulnérabilités l'art. 74 al. 3 LSI2). L'attribution de plus de compétences d'exécution de la loi devrait permettre d'éclaircir la répartition entre les compétences de l'OFCS et des actrices privées.

c. Le rôle de l'office dans les échanges d'informations

1406 Lorsque des sujets requièrent la mise sur pied d'ISAC impliquant l'État, la loi doit prévoir certains aspects[2110]. En général, les ISAC existent pour des secteurs. Il est important qu'ils impliquent l'autorité compétente pour la cybersécurité. Il s'agit en l'occurrence du nouvel OFCS, qui détient certaines informations utiles pour les secteurs et qui a pour mission d'avoir une vue d'ensemble de la cybersécurité et des cybermenaces en Suisse. Pour simplifier les évolutions

2108 Voir les archives du blog de GovCERT (consulté le 20.3.2024).

2109 FF 2023 84, p. 31.

2110 Par exemple, l'UE compte certains ISAC pour des secteurs spécifiques, cf. ENISA, *ISAC,* 2018, p. 20 s.

à venir dans ce contexte, nous pourrions par exemple envisager que la LSI habilite l'OFCS à être impliqué dans des ISAC sectoriels et intersectoriels. La loi doit donner la possibilité à l'ordonnance d'apporter des précisions si nécessaire. Le principe de la légalité requiert en effet que les échanges d'informations impliquant des autorités soient prévus dans une base légale.

1407 En dehors des cas de figure où des autorités sont concernées, les interlocutrices échangeant des informations dans le cadre de plateformes dédiées peuvent le faire librement. D'autres partenariats doivent par ailleurs être mis en place pour certaines questions ou certains phénomènes spécifiques. Des *« informal working groups »* peuvent être à cette fin privilégiés en parallèle de structures légales comme les ISAC[2111]. À titre d'exemple, la lutte contre les rançongiciels est aujourd'hui un point important en matière de protection contre les cybermenaces. Ce phénomène délictuel touche l'administration, les infrastructures critiques ou encore les petites ou moyennes entreprises (PME). Les PME ne faisant en général pas partie d'ISAC en Suisse, elles peuvent être démunies face à une attaque par rançongiciel et être tentées de payer une rançon. Une plateforme d'échange d'informations sécurisée alliant des autorités compétentes et différentes entreprises permettrait d'échanger des informations au sujet des modes opératoires, des mesures possibles pour empêcher le succès de telles attaques ou en atténuer les conséquences dommageables[2112]. Si des autorités, à l'instar de l'OFCS, viennent à prendre part à ce projet, le principe de la légalité impose que leur participation soit prévue par la loi, problème pouvant être résolu en prévoyant, comme susmentionné, que des autorités comme l'OFCS peuvent rejoindre des structures d'échanges d'informations[2113].

1408 Il n'est naturellement pas exclu que l'État soutienne et encourage de telles plateformes d'autres façons qu'en y participant directement, ce qui est susceptible d'entraîner des répercussions sur un potentiel cadre légal, mais qui sort de considérations purement juridiques. Par ailleurs, il serait également intéressant d'analyser les ISAC et les réseaux de collaboration que l'OFCS pourrait rejoindre ou avec lesquels elle pourrait contracter afin de collaborer au mieux à différents échelons et entre différentes actrices[2114]. De la même manière que

2111 Ce type de plateforme est effectivement plus apte à répondre à la pratique pour des phénomènes qui sont susceptibles de disparaître.

2112 MEYER/PANGRAZZI/SARRASIN, p. 1156 et références citées.

2113 La récolte d'informations par l'État dans le domaine de la sécurité doit être clairement circonscrite, cf. CourEDH, arrêt *Antunes Rocha c. Portugal* du 31.5.2005, 64330/01, § 67 ss ; CR Cst.-BLEICKER, art. 57 N 46.

2114 Comme certains réseaux dont GovCERT fait déjà partie, cf. *supra* N 341 ss. Concernant les réseaux avec lesquels la Suisse pourrait conclure, voir par exemple ce qui est instauré par la Directive SRI2 avec un groupe de coopération, un réseau de CSIRT et EU-CyCLONe (art. 17 Directive SRI2 ; c. 73 Directive SRI2).

sur le plan national, des réglementations doivent exister lorsque des autorités sont concernées, contrairement aux ISAC se limitant à certaines organisations de l'industrie.

Schéma 27 : les propositions relatives aux compétences de soutien

Compétences actuelles

- Recherche de cybermenaces et analyses techniques
- Diffusion d'informations, de recommandations, d'outils et d'instructions
- Potentiel soutien et conseils dans la maîtrise d'incidents et l'élimination de vulnérabilités pour les infrastructures critiques
- Soutien à l'infrastructure critique signalant une cyberattaque en vertu des art. 74a ss LSI2
- Recommandations relativement aux cybermenaces pour la personne signalant une cybermenace si pas d'analyse supplémentaire nécessaire
- Divulgation coordonnée des vulnérabilités

Compétences proposées

- Plus de clarté concernant la faculté d'effectuer des scans proactifs et de rechercher des menaces sur les systèmes d'information des infrastructures critiques
- Obligation plus étendue de soutenir les infrastructures critiques dans la gestion de cyberincidents et dans l'élimination de vulnérabilités

2. La limite entre soutien et surveillance : les compétences « réglementaires »

1409 L'OFCS peut notamment fournir des informations sous différents formats afin de permettre aux différents groupes cibles la mise en place de mesures appropriées pour faire face aux cybermenaces. Certaines informations sont non contraignantes, comme les instructions qui seront transmises aux infrastructures critiques sur la base de l'art. 74 LSI2[2115]. D'autres instruments sont contraignants, comme la Directive Si001 pour la catégorie de sécurité « protection de base » pour les autorités de la Confédération (art. 17 LSI).

1410 Les directives en matière de sécurité informatique du NCSC resteront applicables durant les trois ans qui suivent l'entrée en vigueur de l'OSI (art. 51 al. 1 OSI). Le service spécialisé de la Confédération pour la sécurité de l'information sera compétent dès le 1er juillet 2025 pour adopter de telles directives pour les autorités et organisations de la Confédération (art. 27 al. 7 et 29 al. 1 OSI). En raison de la création de cette nouvelle autorité et du temps qu'il lui

2115 De la même façon de ce qui est prévu en droit européen, par exemple à l'art. 25 Directive SRI2.

faut pour être totalement opérationnelle, l'OFCS est compétent pour adopter notamment les directives qui s'imposent jusqu'en 2025 (art. 51 al. 6 OSI), mais pour un maximum de deux ans après l'entrée en vigueur de l'ordonnance (art. 51 al. 7 OSI). La situation est particulièrement complexe pour les autorités et organisations de la Confédération, mais, s'agissant des autres infrastructures critiques, nous estimons que l'OFCS devrait, en tant qu'autorité principale pour la cybersécurité bénéficiant des compétences du NCSC, rester compétent pour adopter des directives contraignantes applicables à ce cercle d'organisations assujetties, en particulier dans l'hypothèse où des exigences minimales de cybersécurité viendraient à être introduites pour les infrastructures critiques. Cette position se justifie d'autant plus que le NCSC détient d'ores et déjà certaines compétences d'une autorité de soutien et d'autres incombant aux autorités de surveillance.

Schéma 28 : les propositions relatives aux compétences réglementaires

Compétences actuelles

— Adoption de directives contraignantes pour les autorités et organisations de la Confédération
— Elaboration d'instructions et de recommandations pour les infrastructures critiques

Compétences proposées

— Adoption de directives contraignantes pour les infrastructures critiques

3. Les compétences de surveillance

L'OFCS dispose déjà de quelques compétences de surveillance en tant qu'autorité chargée de l'application de la loi, bien que le souhait des autorités politiques soit au contraire d'affirmer qu'il n'assume pas ce rôle[2116]. Alors que la collaboration horizontale entre les différentes destinataires de la LSI et le NCSC était privilégiée dans la première version du texte légal, l'introduction de l'obligation de signaler les cyberattaques a ouvert la porte à une transformation du NCSC en autorité de surveillance. Le NCSC étant maintenant l'office fédéral pour la cybersécurité, une partie des compétences de l'office contribuera probablement au soutien des différentes autorités et organisations en Suisse et une autre aura vraisemblablement davantage vocation à contrôler le respect de la réglementation. GovCERT soutiendra vraisemblablement l'office dans ses différentes fonctions en raison de ses compétences techniques. 1411

2116 FF 2023 84, p. 33.

1412 Les compétences de l'OFCS dans le cadre de l'obligation de signaler les cyberattaques se manifestent comme suit. En cas d'indices d'une violation de l'obligation de signaler, l'OFCS informe l'infrastructure critique assujettie de l'obligation et fixe à cette dernière un délai approprié pour s'acquitter de celle-ci (art. 74*g* al. 1 LSI2). Si l'organisation ne s'acquitte pas de son obligation, l'OFCS rend une décision au sujet de l'obligation en fixant un nouveau délai et en assortissant sa décision de la menace d'une amende (art. 74*g* al. 2 LSI2). La personne qui ne se conforme pas intentionnellement à la décision est punie par les autorités de poursuite pénale compétentes d'une amende de 100 000 francs au maximum (art. 74*h* al. 1 et 4 LSI2)[2117].

1413 En parallèle de l'obligation de signaler les cyberattaques, l'OFCS détient d'autres compétences proches des compétences de surveillance quant au cercle de destinataires plus précis des fabricantes de logiciels. Lors du signalement d'une vulnérabilité, l'OFCS en informe immédiatement la fabricante du logiciel ou du matériel informatique concerné en lui fixant un délai approprié pour l'éliminer (art. 73*b* al. 3 LSI2). Il peut publier des informations sur cette vulnérabilité tout en indiquant le logiciel ou le matériel informatique concerné si la fabricante y consent ou si elle n'a pas éliminé la vulnérabilité dans le délai fixé en amont (art. 73*c* al. 2 LSI2)[2118].

1414 Alors que les compétences actuelles de l'OFCS en termes de surveillance se limitent à ce qui est susmentionné, le droit européen sert de source d'inspiration lorsqu'il en va de contrôler la mise en œuvre d'exigences minimales de cybersécurité auprès des infrastructures critiques. Les art. 32 et 33 Directives SRI2 disposent que les autorités compétentes doivent pouvoir, lorsqu'elles accomplissent leurs tâches de supervision auprès des entités essentielles et importantes, procéder à des inspections et des contrôles, permettre la réalisation d'audits réguliers et ciblés par des organismes indépendants ou par des autorités compétentes, requérir des informations ou des preuves ou encore accéder à des informations, imposer des comportements, prononcer des avertissements ou imposer ou demander aux autorités compétentes d'imposer des amendes administratives (art. 32 par. 2 et 4, art. 33 par. 2 et 4 Directive SRI2). Elles doivent en outre pouvoir, pour les entités essentielles, imposer des audits *ad hoc* notamment lorsqu'ils sont justifiés par un incident important ou une violation de la directive ou, en cas d'insuffisance d'autres mesures, faire

2117 FF 2023 84, p. 46 ss ; MEYER/MÉTILLE, *Loi fédérale sur la sécurité de l'information : version 2.0*, 2022, N 57. L'art. 74*h* al. 2 et 3 LSI2 règle les questions relatives à la punissabilité des entreprises. Sur l'obligation de signaler les cyberattaques, cf. *supra* N 525 ss ; sur la responsabilité des fournisseuses de services informatiques comme infrastructures critiques en cas de violations de leur obligation des art. 74*a* ss LSI2, cf. *supra* N 693 s.

2118 FF 2023 84, p. 28.

suspendre une certification ou une autorisation ou interdire l'exercice d'une responsabilité dirigeante au sein de l'entité concernée (art. 33 par. 2 litt. c, par. 5 Directive SRI2).

Les autorités compétentes dans l'UE détiennent des compétences bien plus étendues que l'OFCS en Suisse. Il est important que, dans l'éventualité où des exigences minimales de cybersécurité pour les infrastructures critiques venaient à être introduites, l'application de la réglementation puisse être contrôlée. Partant, le nouvel office devrait disposer de plus de compétences, d'une façon similaire à ce qui est prévu en droit européen[2119]. Il faut s'inspirer de ces compétences pour permettre au nouvel OFCS de prendre un rôle relevant davantage d'une autorité de surveillance à proprement parler. Il est déjà compétent pour surveiller le respect par certaines infrastructures critiques de l'obligation de signaler les cyberattaques et il détient déjà certaines compétences de supervision et d'exécution. Si l'on décide d'introduire des exigences minimales légales de cybersécurité pour les infrastructures critiques, il faut que l'OFCS dispose de plus de fonctions, qui doivent être prévues dans une loi afin de respecter le principe de la légalité (art. 5 al. 1 Cst.). 1415

À noter que la loi doit à l'heure actuelle attribuer plus de compétences de surveillance l'OFCS pour la surveillance des infrastructures critiques dans un premier temps. Dans un second temps, il n'est pas exclu de considérer que certaines de ces tâches puissent également être réalisées auprès d'autres entités. 1416

Schéma 29 : les propositions relatives aux compétences de surveillance

Compétences actuelles

- Information, décision et sanction en cas de non-respect de l'obligation de signaler une cyberattaque pour les assujetties
- Information des fabricantes en cas de vulnérabilités et publication d'informations à leur sujet

Compétences proposées

- Actes de supervision et d'exécution
- Enquêtes en cas d'indices de violations des exigences minimales de cybersécurité pour les infrastructures critiques
- Possibilité de sanctionner ou de saisir les autorités de poursuite pénale en cas de violation intentionnelle des exigences minimales de cybersécurité pour les infrastructures critiques assujetties

2119 Cf. *supra* N 1272 ss.

4. Les autres compétences prévues par le droit européen

1417 Alors que la gestion de crise ne fait pas, à ce jour en Suisse, l'objet de la compétence d'une autorité spécifique pour la cybersécurité, mais d'un ensemble d'autorités, la CSN de 2023 prévoit que le NCSC sera impliqué dans un réseau lorsqu'une crise a une composante cyber[2120]. Il n'est pas exclu que l'OFCS soit compétent pour coordonner la gestion de crises cyber (de la même façon que l'autorité de gestion de crises cyber, art. 9 Directive SRI2).

1418 Contrairement à la compétence d'autorité de gestion de crise cyber, le rôle attribué par la Directive SRI2 au point de contact national est attribué en Suisse à l'OFCS. Il est l'autorité chargée d'échanger avec les services analogues à l'étranger ainsi qu'avec les groupes sectoriels (art. 76 à 77 LSI2), d'une façon similaire à ce qui est prévu pour les CSIRT et les points de contact uniques européens (art. 8 par. 3, 4 Directive SRI2)[2121]. L'OFCS gère en parallèle un guichet unique qui sert à recevoir les signalements de cybermenaces, vulnérabilités, cyberincidents et cyberattaques en vertu des art. 73*a* al. 2 litt. b, 73*b* al. 1 LSI2 et 15*a* al. 2 litt. c Org-DDPS. Cette compétence peut en droit européen incomber à l'une des autorités de la Directive SRI2 (art. 13 par. 3 Directive SRI2)[2122].

E. En conclusion : des perspectives d'avenir

1419 L'analyse des compétences de l'OFCS est basée sur l'hypothèse selon laquelle des exigences minimales de cybersécurité seraient introduites en droit suisse pour les infrastructures critiques. L'OFCS reste l'autorité principale pour la cybersécurité en Suisse et la nouvelle autorité conserve la position du NCSC pour la protection des infrastructures critiques contre les cybermenaces. L'OFCS dispose déjà de compétences importantes pour le soutien des infrastructures critiques. Dans le soutien que l'OFCS peut apporter à celles-ci, la loi devrait être plus claire quant aux mesures qu'il peut prendre. En outre, il est nécessaire que l'OFCS soutienne de façon plus importante les infrastructures critiques et non seulement de façon limitée à l'obligation de signaler les cyberattaques. Au-delà du soutien et dans le cadre de compétences réglementaires, l'OFCS doit pouvoir adopter des normes applicables aux infrastructures critiques dans l'intérêt de leur protection contre les cybermenaces. Finalement, l'OFCS commence à occuper une position d'autorité de surveillance à la suite de l'introduction de l'obligation de signaler les cyberattaques. Ce

2120 CF, *CSN*, 2023, p. 26.

2121 FF 2023 84, p. 49 ss ; MEYER/MÉTILLE, *Loi fédérale sur la sécurité de l'information : version 2.0*, 2022, N 46.

2122 FF 2023 84, p. 26.

rôle doit être renforcé, surtout si des exigences minimales de cybersécurité viennent à être introduites. Les compétences de surveillance de l'OFCS peuvent s'inspirer des compétences d'autorités similaires dans l'UE.

L'analyse des compétences de l'OFCS doit tenir compte de la réorganisa- 1420
tion de la cybersécurité au sein de la Confédération en cours. Actuellement, l'OFCS et le service spécialisé de la Confédération pour la sécurité de l'information se partagent les compétences entre la cybersécurité et la sécurité de l'information. GovCERT appuie les deux entités lorsque leurs fonctions ont une composante cyber, mais l'équipe d'intervention est gérée par l'OFCS. La transformation du NCSC en OFCS confirme que ce dernier demeure l'autorité principale pour la cybersécurité en Suisse. Le nouveau service spécialisé de la Confédération semble disposer davantage de compétences pour la sécurité de l'information pour les autorités et organisations de la Confédération, ce qui permet à l'OFCS de conserver les compétences du NCSC pour la cybersécurité des infrastructures critiques. Pour ce cercle restreint, la collaboration entre le nouveau service spécialisé et l'OFCS sera importante. Les questions d'attribution des compétences entre le nouvel office pour la cybersécurité et le nouveau Secrétariat d'État à la politique de sécurité (SEPOS) devront encore faire l'objet de discussion au niveau des autorités et la répartition des compétences devra se faire de la façon la plus logique et adéquate, à la lumière de considérations comme l'importance de ne pas perdre de temps par les échanges entre les autorités compétentes, ou le nécessité de maintenir la confiance donnée à l'OFCS par les infrastructures critiques[2123].

Les questions de confiance de la part des infrastructures critiques de- 1421
vront en effet être particulièrement analysées. Bien que le pouvoir législatif craignît que les organisations transmettent moins volontiers des informations au NCSC sur une base volontaire si celui-ci détient davantage de compétences de surveillance[2124], une telle collaboration est déjà susceptible d'être compromise avec la décision de l'intégrer au DDPS. Par conséquent, l'on ne saurait suivre cette opinion ; il convient selon nous d'assumer la décision quant au rôle important de l'OFCS dans le domaine de la cybersécurité (spécialement auprès des infrastructures critiques) et de tenter au mieux de maintenir la

2123 Une autre question intéressante aurait trait à la position de l'autorité compétente au sein de l'administration, à laquelle l'on pourrait préférer une position indépendante comme celle de la PFPDT. Cette question reste ici ouverte, ne nécessitant pas d'être tranchée par la présente étude. Nous pouvons en tout cas déplorer la perte de compétences de l'OFCS au profit du service spécialisé de la Confédération pour la sécurité de l'information, cf. WINGEIER Christian, *Der Bundesrat entmachtet das NCSC*, 8 novembre 2022 (consulté le 20.3.2024). Sur des questions de confiance dans l'OFCS, cf. ANZ Philipp, *Beim NCSC häufen sich die Kündigungen*, 7 décembre 2023 (consulté le 20.3.2024).

2124 FF 2023 84, p. 13.

confiance des infrastructures critiques. Différents mécanismes peuvent être utiles à cette fin, à l'instar des garde-fous dont dispose le NCSC, des accords de confidentialité, de l'utilisation du protocole TLP, du secret de fonction et d'autres outils[2125].

1422 La question des ressources est finalement aussi centrale, dès lors que le travail que doit effectuer l'OFCS peut exiger des ressources importantes[2126]. La réorganisation de la cybersécurité au sein de la Confédération devrait permettre l'utilisation de ressources en suffisance pour que le nouvel office puisse apporter son soutien et contrôler la mise en œuvre de la réglementation auprès de l'ensemble des infrastructures critiques en Suisse sans se limiter aux plus importantes, à condition que les tâches de l'OFCS et du service spécialisé de la Confédération pour la sécurité de l'information soient clarifiées. Trier les tâches selon de justes priorités pourra également contribuer à une bonne gestion des ressources. À titre de comparaison, l'art. 11 par. 3 *in fine* Directive SRI2 indique que les CSIRT se fondent sur les risques pour trier leurs actions en fonction des priorités[2127]. Il peut être délicat pour l'OFCS et GovCERT de trier les dossiers à traiter, mais une telle approche, fondée sur la gravité et la probabilité des risques nous semblerait consister en une approche judicieuse probablement déjà suivie dans la pratique des autorités.

III. Une conclusion au chapitre 10

1423 De nombreuses questions découlent de la position des prestataires de gestion de cyberincidents. Ces questions sont finalement plus larges et ne se limitent pas à ces expertes. Du côté des prestataires privées, la cybersécurité des prestataires de gestion de cyberincidents doit être appréhendée plus largement et viser également les autres fournisseuses de services informatiques. Du côté de GovCERT, les questions soulevées ne concernent pas uniquement l'équipe d'intervention, mais portent sur les compétences de l'OFCS, auquel est intégrée GovCERT.

1424 Les prestataires de gestion de cyberincidents doivent être responsables de leur cybersécurité et de la cybersécurité des prestations qu'elles offrent,

2125 L'on pourrait même imaginer préciser d'autres dispositions, à l'instar de l'art. 6 LRens, pour que des autorités comme le SRC ne puissent pas obtenir dans des circonstances trop floues des informations détenues par l'OFCS.

2126 OFCS, *Rapport concernant les analyses de données effectuées après la cyberattaque contre l'entreprise Xplain*, 2024, p. 7 et 11.

2127 Et cela devrait être prévu dans l'ordonnance à venir du moins dans l'assistance en cas de cyberattaque, cf. art. 8 P-OCyS.

ce qui passe par l'introduction d'exigences légales. Les prestataires de gestion de cyberincidents ont deux casquettes : elles font partie des fournisseuses de services numériques de sécurité, constituant elles-mêmes des organisations actives dans le sous-secteur critique des services informatiques et, partant, des infrastructures critiques. Si la proposition législative du chapitre 9 est suivie et que des exigences minimales légales de cybersécurité pour les infrastructures critiques sont introduites, un niveau minimal de cybersécurité supplémentaire devrait être assuré par les fournisseuses de services informatiques, dont les prestataires de gestion de cyberincidents.

Ces organisations ne doivent pas uniquement sécuriser leur infrastructure, mais également les prestations qu'elles fournissent à leur clientèle. Il n'existe à l'heure actuelle pas de réglementation pour ce faire dans le domaine de la cybersécurité. Partant, des exigences légales supplémentaires doivent être introduites. Ces exigences doivent s'appliquer aux prestataires de gestion de cyberincidents en tenant compte de la diversité de structures d'organisations existantes, de la diversité de leurs prestations et du fait que l'ensemble des fournisseuses de services informatiques est concerné (I.A). La Confédération est compétente pour légiférer sur la cybersécurité des prestations qu'elles offrent en vertu de l'art. 95 Cst. et, potentiellement, de l'art. 97 Cst. (I.B). La loi devant contenir ces exigences supplémentaires est la LSI (I.C). La loi doit prévoir une obligation générale de cybersécurité dans les prestations. Cette obligation doit ensuite être concrétisée dans des actes d'exécution, par exemple sous la forme d'exigences relatives à la séparation des systèmes informatiques de la prestataire de services informatiques de ceux de sa clientèle, d'obligations de gérer les vulnérabilités ou d'obligations de protéger la disponibilité des fonctions essentielles de leur clientèle. Des obligations, telles qu'une obligation de transparence, doivent également figurer dans les bases légales applicables (I.D). Le présent chapitre a aussi permis d'examiner comment le cadre légal pouvait clarifier le statut des pirates éthiques, qui sont des prestataires de services informatiques particulières. Le piratage éthique occupe une place importante dans la cybersécurité. Les pirates éthiques endossent un rôle susceptible d'entrer dans le sous-secteur critique des services informatiques. La proposition législative du chapitre 10 permettrait de les soumettre à des exigences de cybersécurité, afin d'éviter les risques de cyberincidents dans leur pratique. Cela étant, les questions principales concernant le piratage éthique ont trait à la responsabilité des pirates éthiques et de leur statut privilégié auprès de l'OFCS. La loi peut contribuer à améliorer la sécurité juridique en faveur des pirates éthiques, ce qui permettrait de clarifier leur statut et de renforcer leur collaboration avec l'OFCS. Au-delà de ces précisions, il est naturellement nécessaire de prévoir les mécanismes appropriés pour permettre

1425

que la loi soit adéquatement contrôlée, de la même manière que pour le contrôle du respect des exigences minimales de cybersécurité applicables aux infrastructures critiques (I.E).

1426 Les propositions législatives des chapitres 9 et 10 permettraient d'imposer la sécurité de l'entier du cycle de vie de systèmes d'IA aux différentes intervenantes, du moins lorsque des infrastructures critiques exploitent les systèmes d'IA. En tout cas, la fabrication et le développement de tels systèmes seraient encadrés par la loi. Ces propositions permettraient également d'appréhender légalement la responsabilité des infrastructures critiques qui utilisent des solutions en nuage. L'adoption des propositions législatives de la présente étude permettrait de conférer une cybersécurité plus étendue à l'IdO. Ces propositions s'appliqueraient de façon complémentaire à l'OST, à la LSPro et à la LPD. L'introduction d'exigences légales supplémentaire de la cybersécurité des prestataires informatiques permettrait plus spécifiquement d'assurer que la fournisseuse de solution infonuagique mette en place des mesures permettant d'assurer la cybersécurité de sa solution. Finalement, la chaîne d'approvisionnement est omniprésente sous de différentes formes et sa sécurité constituent des éléments cruciaux. Certains secteurs ont réglementé des aspects de cybersécurité susceptibles de s'appliquer aux différentes intervenantes dans une chaîne d'approvisionnement. Les propositions législatives de la présente étude permettraient néanmoins un pas en avant important pour responsabiliser ces intervenantes, en partant de la conception de logiciels et de matériel informatique jusqu'à l'exploitation et la fin de vie d'un produit informatique ou d'une prestation. En parallèle, des mécanismes extralégaux existent et doivent être encouragés (I.F) [2128].

1427 Les bases légales pour GovCERT et l'autorité dans laquelle elle œuvre diffèrent de ce qui est prévu ou qui doit être prévu pour les autres prestataires de gestion de cyberincidents (II.A). Les questions relatives à GovCERT interrogent également quant au rôle de l'OFCS (II.B). Le droit suisse est plus limitatif que le droit européen pour leurs compétences et ce dernier peut servir d'inspiration pour examiner comment les bases légales existantes en Suisse peuvent mieux appréhender le mandat de GovCERT et celui de l'OFCS (II.C). Des modifications sont nécessaires pour permettre un soutien plus important par l'OFCS des infrastructures critiques, pour qu'il puisse mieux guider les infrastructures critiques par l'adoption d'instruments à leur attention et pour que son rôle d'autorité de surveillance soit plus assumé (II.D).

2128 La Suisse doit continuer à prendre en considération comme point de comparaison les avancées législatives européennes, dans la mesure où l'UE adopte différentes réglementations et directives sur les mêmes sujets. Voir à titre d'exemples la Loi sur la cyberrésilience (*Cyber Resilience Act*, CRA) ou le Règlement européen sur l'intelligence artificielle.

Les propositions législatives du chapitre 10 sont à concevoir conjointement à l'introduction d'exigences minimales de cybersécurité pour les infrastructures critiques du chapitre 9. Cet ensemble de recommandations permettrait d'utiliser la réglementation correctement à titre d'incitation pour améliorer la cybersécurité des infrastructures critiques en Suisse. Il permettrait également de responsabiliser les différentes intervenantes dans la cybersécurité de ces organisations et de mobiliser leurs ressources. Cet ensemble de propositions peut avoir un impact plus large encore que sur la cybersécurité des infrastructures critiques. Nous avons pu voir à titre d'exemple que l'introduction d'exigences supplémentaires aux fournisseuses de services informatiques peut servir à les responsabiliser dans les prestations qu'ils offrent également à d'autres clientes que des infrastructures critiques. En outre, la réglementation de la cybersécurité des infrastructures critiques et des prestations offertes par des prestataires informatiques permettent d'appréhender des aspects de technologies soulevant à l'heure actuelle de multiples questions. 1428

La cybersécurité des infrastructures critiques est un élément primordial dans la société à l'heure actuelle. Les infrastructures critiques sont essentielles à la société et nécessitent d'être sécurisées. De nombreux processus au sein de ces autorités et organisations étant numérisés, la cybersécurité doit aujourd'hui en particulier être assurée. La réglementation permet d'apporter une partie de la solution en servant d'incitation à l'amélioration de la cybersécurité. Les propositions de la présente étude permettent au cadre réglementaire d'assurer sa fonction dans ce contexte et, ce faisant, de contribuer substantiellement à l'amélioration de la cybersécurité des infrastructures critiques. 1429

Conclusion générale

« Pas de cybersécurité sans sécurité juridique »
Michel Séjean, Code de la cybersécurité, 1ère édition, 2022

Qu'est-ce que la cybersécurité ? Malgré la multitude de définitions existantes, 1430
l'on peut aisément comprendre que la cybersécurité repose sur le concept de sécurité dans le cyberespace. La cybersécurité doit être appréhendée par différentes disciplines. Parmi ses différentes dimensions, l'on retrouve la législation et la réglementation. Le domaine juridique de la cybersécurité se rapproche d'autres domaines juridiques, à l'instar de la cybercriminalité, de la cyberdéfense ou encore de la sécurité de l'information. Cela étant, la réglementation de ce domaine précis est à un état embryonnaire en Suisse, malgré son importance dans la protection du pays contre les cybermenaces.

La cybersécurité correspond à l'état sûr, ce qui implique que les cyber- 1431
menaces, y compris les cyberincidents, doivent être gérées. La cybersécurité est assurée par des compétences appropriées de prévention, de détection et de réaction aux cyberincidents. Il existe de nombreuses mesures techniques et organisationnelles permettant de gérer les cyberincidents rencontrés, qui dépendent de nombreux éléments à l'instar des risques, des besoins de protection, des traitements d'informations et des systèmes informatiques utilisés par des organisations.

La cybersécurité répond à différents enjeux de la pratique. Elle doit tenir 1432
compte de l'importance de sécuriser les informations traitées par des moyens et par des systèmes informatiques, et de l'importance de distinguer en fonction du besoin de protection des différentes informations traitées. La cybersécurité doit également s'adapter aux évolutions technologiques permettant à des attaquantes d'améliorer en continu leurs modes opératoires. Pour que le niveau de cybersécurité soit suffisant, les différentes intervenantes doivent être impliquées et responsabilisées dans les processus et dans les décisions. Il en va typiquement de l'État et de ses autorités, des infrastructures critiques, des autres entreprises de l'économie, des milieux académiques ou encore de la population. Il est également important de s'appuyer lorsque cela est possible sur les évolutions technologiques afin de ne pas freiner l'innovation, tout en portant une attention particulière sur les risques liés à ces nouvelles technologies.

La Suisse souhaite suivre les évolutions technologiques et tirer le meilleur 1433
de la numérisation de la société. C'est pourquoi le pays élabore des stratégies nationales sur différents domaines ayant trait à la numérisation. La Stratégie cadre de la Suisse, la Stratégie Suisse numérique, met un accent sur les aspects sécuritaires liés à la digitalisation. C'est sur la base de cette stratégie que la Cyberstratégie nationale (CSN) a été élaborée. Elle sert de cadre stratégique et

politique à la protection de la Suisse contre les cybermenaces. C'est dans ce cadre que sont évalués les leviers d'action à mobiliser pour atteindre des objectifs en termes de cybersécurité en particulier. Elle contribue, avec d'autres stratégies, à poser les bases pour ce qui doit être fait en Suisse afin de protéger les différents groupes existants au sein de la société.

1434 Parmi ces groupes cibles à protéger, les infrastructures critiques sont particulièrement importantes en Suisse. Elles regroupent les autorités et d'autres organisations considérées comme nécessaires pour le bien-être de la population ou l'économie nationale. La Suisse leur donne un statut particulier, de la même façon qu'à l'étranger, car une partie importante de la population ou des intérêts particuliers de la société dépendent de leur bon fonctionnement. C'est pourquoi leur cybersécurité doit en particulier être assurée. Alors que leur niveau est souvent considéré comme insuffisant, des incitations notamment juridiques doivent exister pour qu'elles améliorent leur cybersécurité.

1435 Le cadre légal suisse impose à certaines infrastructures critiques des exigences en matière de cybersécurité. Les autorités et les organisations de la Confédération sont par exemple soumises à un catalogue d'exigences en termes de sécurité de l'information et de sécurité des moyens informatiques. Les domaines se recoupent avec le domaine de la cybersécurité. De la même manière, certains sous-secteurs englobés par le secteur critique de l'approvisionnement en énergie élaborent actuellement des bases légales pour que les organisations fournissant des prestations dans ces sous-secteurs soient soumises à des exigences de cybersécurité. Le cadre légal se développe peu à peu. En revanche, trop nombreuses sont les infrastructures critiques qui ne sont pas soumises à des exigences minimales de cybersécurité, à des exigences trop limitées ou uniquement à des normes non contraignantes ne permettant pas d'inciter suffisamment les organisations à atteindre un niveau suffisant de cybersécurité. Certaines organisations ignorent par ailleurs être des infrastructures critiques ou ne comprennent pas les exigences auxquelles elles sont soumises. Le cadre légal est disparate et son manque de clarté ainsi que le manque de clarté de la définition d'infrastructure critique sont aujourd'hui problématiques. Bien que la sécurité de l'information et la protection de différentes informations soient en parallèle réglementées, ces instruments juridiques sont trop limités par rapport à la cybersécurité qui demeure lacunaire en droit suisse.

1436 Le manque de réglementation du sous-secteur critique des services informatiques est particulièrement choquant, en particulier pour les prestataires à double casquette y opérant. Elles sont d'une part des infrastructures critiques. D'autre part, elles fournissent des services à de nombreuses organisations, dont des infrastructures critiques qui dépendent d'elles. Les fournisseuses de services numériques de sécurité et les prestataires de gestion de

cyberincidents font partie des organisations actives dans ce sous-secteur critique et ces organisations ne sont à l'heure actuelle soumises à aucune exigence minimale de cybersécurité. La situation est particulièrement problématique, comme nous avons pu le voir en 2023 avec les attaques de différentes prestataires auprès de la Confédération. Si certaines bases légales transversales ont vocation à s'appliquer en fonction la clientèle de ces prestataires, ainsi qu'en fonction des prestations qu'elles fournissent ou des informations qu'elles traitent, la situation demeure insatisfaisante et lacunaire.

1437 Force est de constater que la situation réglementaire doit évoluer. La piste préconisée par la CSN de 2023 consiste en l'examen continu des besoins réglementaires et des lacunes ainsi qu'au comblement ponctuel de celles-ci. C'est ce qui a été fait pour le sous-secteur critique de l'approvisionnement en électricité. Le sous-secteur disposait de normes minimales pour l'utilisation des technologies de l'information et de la communication (TIC), mais l'OFEN a conclu qu'une base légale contraignante manquait et était nécessaire. Dans la mesure où le sous-secteur critique de l'approvisionnement en électricité était l'un des rares en Suisse à disposer d'une norme minimale, il est à prévoir que l'examen des autres secteurs et sous-secteurs critiques aboutira à une conclusion similaire, à savoir que des exigences légales sont nécessaires. En outre, le processus ayant duré plusieurs années avant l'entrée en vigueur de la loi et de l'ordonnance révisées, il est prévisible que la modification d'une situation aujourd'hui insatisfaisante constituera un travail fastidieux et de longue haleine.

1438 Il est aujourd'hui nécessaire d'appréhender la réglementation de la cybersécurité des infrastructures critiques d'une autre façon. Il faut passer par l'introduction d'exigences minimales légales de cybersécurité pour les infrastructures critiques. Bien que la Confédération préfère confirmer la subsidiarité de l'intervention étatique, force est de constater qu'elle détient les compétences pour intervenir et qu'il est nécessaire qu'elle le fasse. Il est possible de s'appuyer sur les efforts entrepris jusqu'à maintenant pour ne pas avoir à adopter une nouvelle loi. En d'autres termes, la LSI sert de base légale adéquate, voire idéale, pour intégrer ces exigences minimales. La loi doit revêtir un niveau de clarté suffisant pour que les organisations assujetties sachent qu'elles le sont. Les exigences concrètement attendues de ces dernières doivent présenter un niveau adéquat de densité normative et s'adapter facilement aux évolutions, ce qui sous-entend que les normes importantes doivent figurer dans la loi, mais que les mesures concrètes vont probablement souvent figurer dans des actes d'exécution de la loi.

1439 Au-delà des exigences minimales de cybersécurité applicables aux infrastructures critiques, les fournisseuses de services informatiques doivent être soumises à des exigences supplémentaires en raison de leur statut particulier.

Les exigences doivent permettre de séparer leurs systèmes de ceux de leur clientèle, d'assurer la cybersécurité des prestations qu'ils fournissent et d'assurer un certain niveau de transparence quant à la qualité de leurs prestations.

1440 Et l'État dans tout cela ? L'intervention étatique doit se faire sur plusieurs plans. Premièrement, celui-ci intervient déjà en soutien des infrastructures critiques. Ce rôle collaboratif est important pour permettre un échange d'informations qualitatif et la mise en place de mesures adéquates pour la cybersécurité des infrastructures critiques. La loi doit donc renforcer ce rôle. Deuxièmement, l'État doit intervenir plus largement dans son rôle d'autorité de réglementation. Les autorités compétentes, à savoir principalement le nouvel Office fédéral de la cybersécurité (OFCS), doivent pouvoir adopter des actes permettant de guider les assujetties dans leur mise en œuvre de la loi. L'OFCS est l'autorité la plus à même de détenir les compétences pour appréhender correctement la cybersécurité dans les actes qu'il élabore, dans la mesure où il est l'autorité principale pour la cybersécurité en Suisse. Troisièmement et bien que des réserves puissent exister au sein de la Confédération, l'OFCS se transforme en autorité de surveillance par le biais de l'introduction de l'obligation de signaler les cyberattaques ciblant les infrastructures critiques. L'introduction d'exigences minimales de cybersécurité engendrerait naturellement comme conséquence la nécessité de disposer d'une autorité d'application de la loi et l'OFCS est l'autorité idéale pour ce faire. Partant, les bases légales doivent prévoir l'extension de ses pouvoirs pour ce faire.

1441 Ces propositions législatives permettent d'encadrer la cybersécurité des infrastructures critiques, l'activité des prestataires de gestion de cyberincidents et le rôle de l'État dans la cybersécurité de ces organisations. L'objectif poursuivi ici n'est naturellement pas de freiner l'innovation, mais bien plus de réglementer là où un réel manque de cybersécurité est à déplorer. L'innovation doit se poursuivre, mais la sécurité doit être prise plus sérieusement en compte dès le début du cycle de vie d'un produit ou d'une prestation et durant l'entier de son cycle de vie. La réglementation doit en d'autres termes être utilisée pour permettre d'augmenter la cyberrésilience d'organisations essentielles en Suisse et pour améliorer la faculté du pays à se protéger contre les cybermenaces.

1442 La réglementation de la cybersécurité par le biais des propositions législatives de la présente étude a une portée plus large, en permettant d'appréhender certains aspects de sujets étant aujourd'hui au cœur de débats en Suisse et sur le plan international. Il en va de la sorte pour l'utilisation de technologies spécifiques, à l'instar de l'intelligence artificielle (IA), des solutions d'informatique en nuage ou de l'Internet des objets (IdO), dont les aspects sécuritaires du cycle de vie sont couverts par les propositions de présente étude. Il va de soi

que d'autres aspects échappent à la réglementation pour la cybersécurité et que des réglementations doivent être pensées pour d'autres éventualités. En revanche, les propositions législatives formulées devraient permettre d'assurer un niveau supérieur et suffisant de cybersécurité auprès des infrastructures critiques en Suisse. Les propositions législatives des chapitres précédents visent en premier lieu les infrastructures critiques afin de les responsabiliser dans leurs activités. Ces propositions cherchent également à responsabiliser les fournisseuses de services informatiques, dont en particulier les prestataires de gestion de cyberincidents, ainsi qu'à fournir à l'OFCS les bases légales appropriées pour soutenir les infrastructures critiques, mettre en œuvre la législation et en contrôler l'application. La cybersécurité est l'un des domaines juridiques concernés par la législation sur les technologies en général et elle doit s'insérer et se coordonner avec d'autres instruments réglementaires. Il est important de comprendre dans quelle mesure les propositions législatives de la présente étude couvrent également d'autres domaines et questions, mais il faut aussi réaliser que d'autres normes devront être créées pour couvrir d'autres aspects relatifs aux technologies et qu'un effort de coordination entre différentes normes sera vraisemblablement nécessaire.

Ces propositions législatives représentent aujourd'hui une priorité pour 1443
assurer la dimension de réglementation de la cybersécurité. Le travail requis par ces propositions doit être réalisé conjointement aux efforts pour assurer les autres dimensions de la cybersécurité, en particulier en termes de culture, d'hygiène et de sensibilisation, afin de garantir une cybersécurité holistique, formulation si chère à notre discipline.

Sur l'auteure:
Après ses études auprès de l'Université de Fribourg et de l'Université de Lausanne, Pauline Meyer s'est dédiée à la rédaction d'une thèse de doctorat sur la cybersécurité des infrastructures critiques et la gestion de cyberincidents en droit suisse. Celle-ci sert à analyser le cadre légal suisse pour la cybersécurité et à contribuer à l'élaboration d'un cadre réglementaire visant à la cybersécurité des infrastructures critiques en Suisse.

À la suite de cette thèse de doctorat, Pauline Meyer poursuit son orientation académique en tant que chargée de cours et par la réalisation d'un postdoc. Elle travaille en parallèle comme juriste spécialisée en cybersécurité, cybercriminalité et protection des données et s'implique pour différentes causes liées aux droits humains.

La présente thèse de doctorat a été soutenue le 9 septembre 2024 à la Faculté de droit de l'Université de Lausanne. Le jury, composé de la Professeure Camille Perrier Depeursinge (directrice de thèse), du Professeur Philippe Gilliéron, du Professeur Martin Beyeler et du Professeur David Benhamou, a admis cette thèse avec la mention *summa cum laude*.

sui generis est une association consacrée à la promotion du libre accès à la littérature juridique, aux décisions de justice, aux décisions officielles et aux documents juridiques. Depuis 2014, une revue juridique en libre accès est publiée sous le label *sui generis*. La maison d'édition *sui generis* a été fondée en 2019.

Les ouvrages juridiques qui sont publiés dans cette collection sont mis à la disposition d'un large public et sont publiés à la fois sous forme imprimée et en ligne. La version numérique est accessible librement dans le monde entier (Open Access). Les droits d'auteur appartiennent aux auteurs ; les œuvres sont publiées sous une licence Creative Commons.

Précédemment publiés dans la collection *sui generis* :

060 – Luca Ranzoni: **Gerechte Strafen ohne Gleichheit?**
059 – Delphine Brun: **Dangerosité : du juge influencé par l'expert au juge indépendant**
058 – Olga Uehlinger: **Auswirkungen des BEPS-Projekts der OECD auf die Steuerordnung der Schweiz: Umsetzung des Aktionspunkts 5**
057 – Dana Mareckova: **Blockchain and Collective Rights Management of Copyright and Related Rights at the Global Level**
056 – Saskia Thomi: **Die Verantwortungsgemeinschaft**
055 – Sena Hangartner: **Strafrechtliche Dopingbekämpfung in der Schweiz**
054 – Sonja Mango-Meier: **Verantwortlichkeit des Fahrzeughalters bei geringfügigen Widerhandlungen gegen das schweizerische Strassenverkehrsrecht durch eine unbekannte Täterschaft**
053 – Yannick Weber: **Die Nichtigkeit im öffentlichen Recht**
052 – Arezoo Sang Bastian: **Between Islamic and Secular Law**
051 – APARIUZ XXIV: **Der Prozess**
050 – Ricarda Stoppelhaar: **Die Indirekte Stellvertretung**
049 – Martin Seelmann: **Strafzumessung und Doppelverwertung**
048 – Benjamin Clément: **Die strafbare Unterlassung der allgemeinen Lebensrettungspflicht**
047 – Luca Ruggiero: **Effets non coordonnés dans le contrôle des concentrations horizontales européen**
046 – Miriam Lüdi: **Zielkonflikt zwischen Lärmschutz und Siedlungsverdichtung**
045 – Corina Ingold: **Das Kompensationsprinzip im Schweizer Raumplanungsrecht**

044 – Alex Attinger: **Wirtschaftliche Berechtigung – Konzepte und Dogmatik**
043 – Myriam Christ: **Le profilage dans le cadre d'une procédure d'embauche entre particuliers**
042 – Andreas Wehowsky: **Expedited Procedures in International Commercial Arbitration**
041 – Lukas Valis: **Digitale Ökonomie: Erforderlichkeit sektorspezifischer ex-ante Regulierung?**
040 – Constance Kaempfer: **Les mécanismes de mise en œuvre du droit international par les cantons suisses**
039 – Ruedi Ackermann: **Der Mietvertrag mit mehreren Mietern**
038 – Lukas Hussmann: **International anwendbare Streitgenossenschaftsgerichtsstände**
037 – Nils Reimann: **Foreign Electoral Interference: Normative Implications in Light of International Law, Human Rights, and Democratic Theory**
036 – Jeremias Fellmann: **Das Verbot von extremistischen Organisationen im schweizerischen Recht**
035 – Florent Thouvenin / Eva-Maria Messerle: **Zur Geschichte des Eigengebrauchs im schweizerischen Urheberrecht – Entwicklung, Erkenntnisse, Quellen**
034 – Nora Camenisch: **Journalistische Sorgfalt: Rechtliche und medienethische Anforderungen**
033 – Joséphine Boillat / Stéphane Werly: **20 ans de la transparence à Genève**
032 – Nicolas Leu: **Kritik der objektiven Zurechnung**
031 – Martin Klingler: **Füllung der Gesetzeslücken im schweizerischen Adhäsionsverfahren**
030 – Christoph Mettler: **Der Anscheinsbeweis im schweizerischen Zivilprozess**
029 – Simone Walser / Nora Markwalder / Martin Killias: **Tötungsdelikte in der Schweiz von 1990 bis 2014**
028 – APARIUZ XXIII: **Recht in der Krise**
027 – Maja Łysienia: **Seeking Convergence?**
026 – Marc Thommen: **Introduction to Swiss Law** (2nd edition, 2022)
025 – Severin Meier: **Indeterminacy of International Law?**
024 – Marina Piolino: **Die Staatsunabhängigkeit der Medien**
023 – Reto Pfeiffer: **Vertragliche Rechtsfolge der «Verwendungmissbräuchlicher Geschäftsbedingungen» (Artikel 8 UWG)**

022 – Nicole Roth: **Miteigentum an Grundstücken und einfache Gesellschaft**
021 – Roger Plattner: **Digitales Verwaltungshandeln**
020 – Raphaël Marlétaz: **L'harmonisation des lois cantonales d'aide sociale**
019 – APARIUZ XXII: **Unter Gleichen**
018 – Kristin Hoffmann: **Kooperative Raumplanung: Handlungsformen und Verfahren**
017 – Monika Pfyffer von Altishofen: **Ablehnungs- und Umsetzungsraten von Organtransplantationen**
016 – Valentin Botteron: **Le contrôle des concentrations d'entreprises**
015 – Frédéric Erard: **Le secret médical**
014 – Stephan Bernard: **Was ist Strafverteidigung?**
013 – Emanuel Bittel: **Die Rechnungsstellung im schweizerischen Obligationenrecht**
012 – Christoph Hurni / Christian Josi / Lorenz Sieber: **Das Verfahren vor dem Berner Kindes- und Erwachsenenschutzgericht**
011 – Lorenz Raess: **Court Assistance in the Taking of Evidence in International Arbitration**
010 – David Henseler: **Datenschutz bei drohnengestützter Datenbearbeitung durch Private**
009 – Dominik Elser: **Die privatisierte Erfüllung staatlicher Aufgaben**

Les livres 001 – 008 sont publiés par la maison d'édition *Carl Grossmann*.

Cet ouvrage est publié dans la collection *sui generis*,
éditée par Marc Thommen.

1ère édition 30 avril 2025
© 2025 Pauline Meyer

Cette œuvre a été publiée en Open Access sous une licence Creative Commons, qui oblige d'identifier l'auteur de l'œuvre sous licence en cas de réutilisation (CC BY 4.0 – https://creativecommons.org/licenses/by/4.0).



L'étape de prépresse de cette publication a été soutenue par le Fonds national suisse de la recherche scientifique.

ISBN 978-3-907297-61-2
DOI 10.38107/061
Lectorat : Jean Perrenoud
Graphisme : Müller+Hess, Basel
Imprimerie : Ebner & Spiegel, Ulm
Entrepôt central de distribution dans l'UE : GVA Göttingen,
Anna-Vandenhoeck-Ring 36, 37081 Göttingen, info@gva-verlage.de.

sui generis Verlag, Viaduktstrasse 21, 8005 Zürich
www.suigeneris-verlag.ch, info@suigeneris-verlag.ch

061

LA CYBERSI
INFRASTRU
CRITIQUES
DE CYBERIN
DROIT SUISS

Un besoin de cybersécurité existe aujourd'hui indéniablement en Suisse et en particulier pour les infrastructures critiques, soit essentielles à la population, à la société ou à l'économie nationale. La réglementation fait partie des leviers servant à améliorer leur cybersécurité.

La présente étude poursuit deux objectifs principaux. Premièrement, elle expose une analyse du cadre légal existant à ce jour pour la cybersécurité des infrastructures critiques en droit suisse, et de l'activité des prestataires de gestion de cyberincidents. Deuxièmement, cette étude formule des propositions législatives visant à inciter les infrastructures critiques à améliorer leur cybersécurité, à encadrer la pratique de gestion de cyberincidents et à renforcer le rôle de l'État dans ce domaine majeur pour la société.

sui generis
ISBN 978-3-907297-61-2
DOI 10.38107/061