Texts and Materials in Data Protection and Digital Human Rights

Contents

Contents	5
1. Introduction	6
Part I: Digital Human Rights	8
2. Revisiting Foundations of Human Rights Law in a Digital Context	10
3. Right to Privacy	39
4. Right to Freedom of Expression & Thought	66
5. Right to be Free from Discrimination	98
6. Right to a Fair Trial	119
7. Rights to Political Participation and Free Elections	131
8. Right to the Freedom of Assembly	146
Part II: Data Protection and the GDPR	154
9. Data Protection as a Fundamental Right	156
10. GDPR - Scope and Objectives	170
11. GDPR - Principles and Actors	194
12. GDPR - Rights and Obligations	219
13. GDPR - The enforcement mechanism	241
14. GDPR - Data Transfers to third countries	266
15. Personal data and Law Enforcement Activities	279
16. Modern Challenges and Final Reflections	298

TEXTS AND MATERIALS IN DATA PROTECTION AND DIGITAL HUMAN RIGHTS

JONIDA MILAJ AND MANDO RACHOVITSA

University of Groningen Press



Texts and Materials in Data Protection and Digital Human Rights Copyright © by Mando Rachovitsa, Jonida Milaj is licensed under a Creative Commons Attribution 4.0 International License, except where otherwise noted.

CONTENTS

1. Introduction 1

Part I: Digital Human Rights

2. Revisiting Foundations of Human Rights Law in a Digital Context 5
3. Right to Privacy 34
4. Right to Freedom of Expression & Thought 61
5. Right to be Free from Discrimination 93
6. Right to a Fair Trial 114
7. Rights to Political Participation and Free Elections 126
8. Right to the Freedom of Assembly 141

Part II: Data Protection and the GDPR

9. Data Protection as a Fundamental Right 151
10. GDPR - Scope and Objectives 165
11. GDPR - Principles and Actors 189
12. GDPR - Rights and Obligations 214
13. GDPR - The enforcement mechanism 236
14. GDPR - Data Transfers to third countries 261
15. Personal data and Law Enforcement Activities 274
16. Modern Challenges and Final Reflections 293

1. INTRODUCTION

Introduction to the book 'Cases and Materials in Data Protection and Digital Human Rights'

This is a Cases and Material textbook curating sources on Data Protection and digital Human Rights law. The textbook aims at providing a "one-stop shop" for students, researchers and practitioners studying these dynamic areas of law. The book is designed and written primarily with students of the LLB programme in Technology law (Faculty of Law, University of Groningen) in mind. The need for this textbook as an educational tool came up when we (Dr Jonida Milaj and Dr Mando Rachovitsa) started teaching a course dedicated to Data protection and digital Human Rights law. We soon realised that there is no equivalent textbook in the market that places together the relevant sources in a structured fashion. Thus, we decided to cover this gap.

With that being said, this textbook is equally relevant to any student or to anybody who has an interest in these areas. It was important to us to have online open access educational material that can be accessible to everybody around the world and that can be easily updated given the quick developments in the field. The textbook is licensed under a Creative Commons Attribution 4.0 International License, except where otherwise noted. Finding sufficient openly accessible sources for this project (to the extent possible) had its challenges but it was worthwhile. We would like to thank authors and artists who gave permission to use their work.

The book can be read and used online. There is also the option for the reader to export it in a PDF format.

Part I on Digital Human Rights is written and curated by Dr Mando Rachovitsa (Associate Professor on Human Rights Law, School of Law, University of Nottingham). This part focuses on relevant Human Rights that have been affected by the development of technology and the digital society.

Part II on Data Protection is written and curated by Dr Jonida Milaj (Associate Professor on Technology Law, Faculty of Law, University of Groningen). In this part of the book, a shift is made from the discussion of human rights to fundamental rights. The focus is on the right to data protection. The chapters provide the relevant EU legal provisions and case law with a focus on the use of personal data in the internal market as well as their use by law enforcement authorities. The sources and materials presented are complemented with exercises and points for reflection. Furthermore, extra reading materials for in depth understanding of the topics covered are

suggested.

It needs to be clarified that this textbook has primarily a European scope. This does not suggest in any way that there are no interesting developments in the areas of digital human rights and data protection from all regions of the world. We simply had to make certain choices with regards to the scope of the book also in light of space and time limitations.

For Part II of the book, we are in debt to our student assistant, Anastasya Lukmanova, for her hard work and creativity in designing and putting together the relevant materials in the format of this digital book.

We would like to thank Groningen University Press for their support provided throughout this project.

For us, this book is a living educational tool that exists in close symbiosis with the needs of the students. Feedback and suggestions on the book are always welcome and the authors would be happy to hear from you.

Jonida Milaj and Mando Rachovitsa
Groningen & Nottingham
September 2025

PART I: DIGITAL HUMAN RIGHTS

2. REVISITING FOUNDATIONS OF HUMAN RIGHTS LAW IN A DIGITAL CONTEXT

Outline of chapter

This chapter revisits the basics of international human rights law while introducing how human rights law functions in the digital environment and AI systems. More specifically, this chapter addresses:

- values and principles underlying human rights law and the sources of human rights law (sections 2.1, 2.2)
- how human rights law progressively develops, including in the digital sphere and AI systems (section 2.3)
- the requirements according to which restrictions to human rights are lawful under human rights law (section 2.4)
- how human rights may be protected in different ways under different treaties, instruments and regimes (section 2.5)
- what the personal and territorial scope of States' obligations under human rights law is (section 2.6)
- what the human rights obligations of business actors are (section 2.7)
- whether the use of certain technologies and/or AI Systems is incompatible with the exercise of human rights (section 2.8)

Basic understanding of human rights law is a pre-requisite

- Please make sure to refresh your existing knowledge on human rights (read respective

chapter from an International Law textbook; for example, Klabbers, International Law, 2016, ch 6)

- Chapter on International Human Rights Law, in S González Hauck et al., Public International Law: A Multi-perspective Approach (Routledge 2024) 531-616

(2.1) Values and Principles of International Human Rights Law

(2.1.1) Ideals of human rights law: Universal Declaration of Human Rights Law

Certain of these aspirations and ideals are embodied in the first international instrument on human rights – the Universal Declaration of Human Rights (UDHR). Although the UDHR is non-binding, it is a notable document of political and normative significance.

> Whereas recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world (preamble, para 1)
>
> All human beings are born free and equal in dignity and rights.
>
> They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood (Article 1 UDHR)

(2.1.2) Universality and interdependence of human rights law

A cardinal tenet of human rights law is that all human rights are universal, indivisible and interdependent and interrelated. All human rights are of equal value (there is no hierarchy) and the effective exercise of one depends on another. According to the 1993 Vienna Declaration and Programme of Action

> 5. All human rights are universal, indivisible and interdependent and interrelated. The international community must treat human rights globally in a fair and equal manner, on the same footing, and with the same emphasis. While the significance of national and regional particularities and various historical, cultural and religious backgrounds must be borne in mind, it is the duty of States, regardless of their political, economic and cultural systems, to promote and protect all human rights and fundamental freedoms.

(2.2) Sources of International Human Rights Law

The sources of human rights law answer the question of 'where do we go to "find" human rights law?'. Since international human rights law is a branch of international law, they share the same sources. The three main sources are: a) international treaties (also known as conventions, covenants, agreements); b) customary international law; c) and general principles of law. These days international treaties monopolise our focus since they have developed human rights exponentially and in a detailed fashion. There are two more sources (known as subsidiary sources) which do not create law but help us interpret and apply the law: judgments by national and international courts and influential scholarly work. Finally, other authorities may not be law-creating or legally binding, but they contribute to the development of human rights (e.g., resolutions by the UN General Assembly or by the Parliamentary Assembly of the Council of Europe, General Comments by UN human rights treaty bodies).

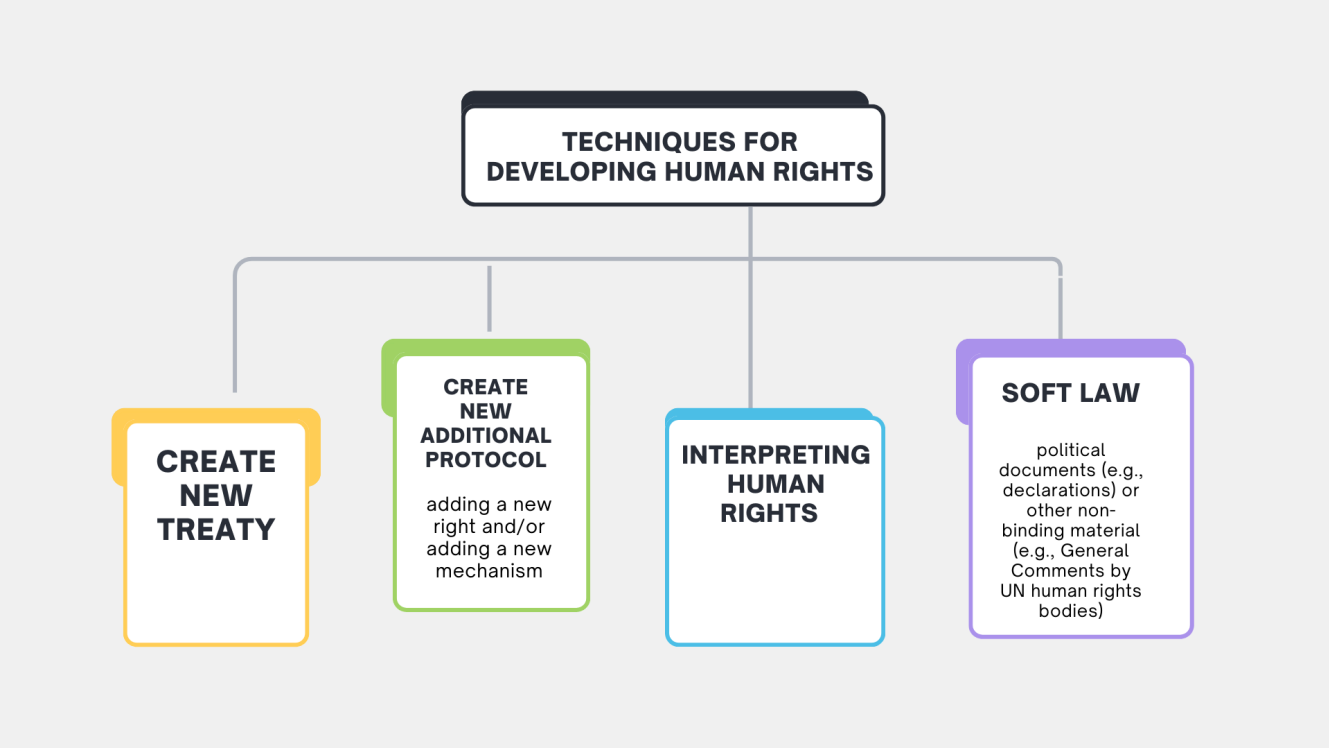
(2.2.1) Article 38(1) of the International Court of Justice Statute

According to Article 38(1) of the International Court of Justice Statute, which is accepted by States to reflect the sources of international law:

> The Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply:
>
> a. international conventions, whether general or particular, establishing rules expressly recognized by the contesting states;
>
> b. international custom, as evidence of a general practice accepted as law;
>
> c. the general principles of law recognized by civilized nations;
>
> d. subject to the provisions of Article 59, judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law.

(2.3) Techniques for the Progressive Development of Human Rights Law

Human rights law progresses in many ways. Looking back, the development of human rights over the last 80 years has been extraordinary – that is if we take the 1948 UDHR as a critical milestone. The obvious question to ask is how it is possible for human rights law to continuously evolve notwithstanding that many human rights treaties date from the '60s and '70s. The techniques and tools that are available to develop human rights may be summarised as follows.

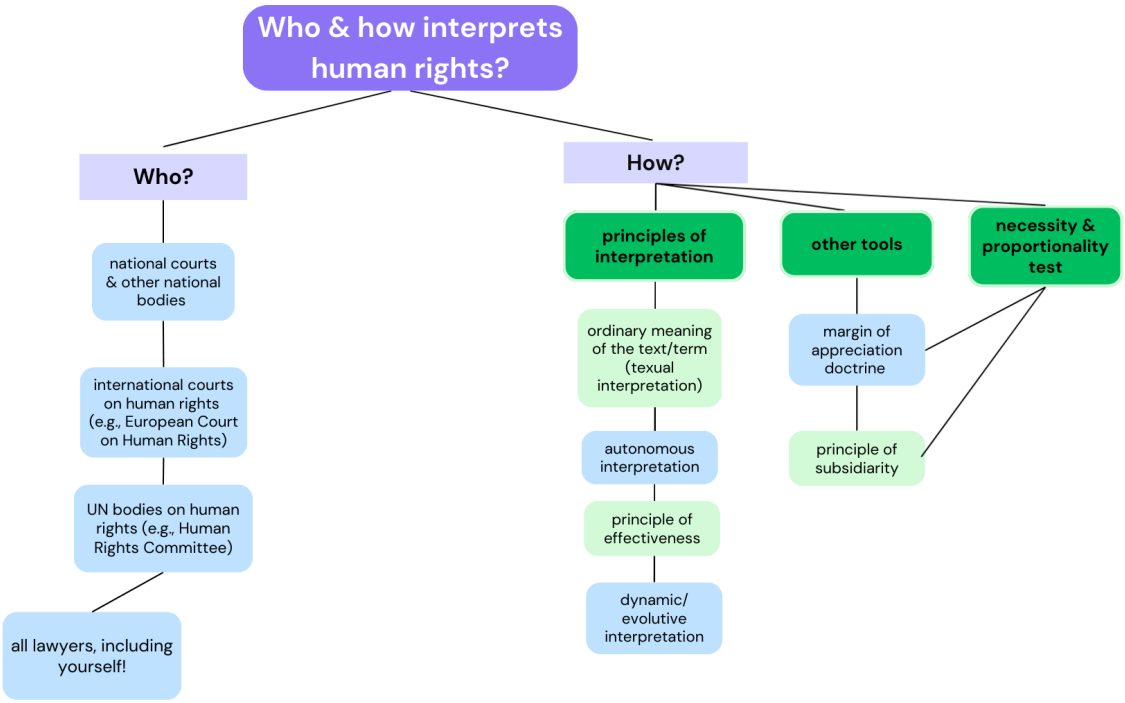


An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://opentextbooks.rug.nl/dataprotectionanddigitalhumanrights/?p=5#h5p-8

(2.3.1) Principles of interpretation in human rights law

The European Court of Human Rights (and other international human rights courts and bodies) applies a series of principles of interpretation which are not found in the text of human rights treaties.

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://opentextbooks.rug.nl/dataprotectionanddigitalhumanrights/?p=5#h5p-10



(2.3.2) Developing existing human rights law to apply in the digital sphere and AI systems

Watch the video:

One or more interactive elements has been excluded from this version of the text. You can view them online here: https://opentextbooks.rug.nl/dataprotectionanddigitalhumanrights/?p=5#oembed-1

(2.3.2.1) Human rights law applies offline and online

UN Human Rights Council, Res 20/08, The promotion, protection and enjoyment of human rights on the Internet, 16 July 2012

1. *Affirms* that the same rights that people have offline must also be protected online.

(2.3.2.2) Human rights must be respected throughout the life cycle of AI systems

UNGA Res 78/265, Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development, UN Doc A/RES/78/265, 1 April 2024

5. *Emphasizes* that human rights and fundamental freedoms must be respected, protected and promoted throughout the life cycle of artificial intelligence systems, calls upon all Member States and, where applicable,

> other stakeholders to refrain from or cease the use of artificial intelligence systems that are impossible to operate in compliance with international human rights law or that pose undue risks to the enjoyment of human rights, especially of those who are in vulnerable situations [...]
>
> [6] [...] (k) Promoting transparency, predictability, reliability and understandability throughout the life cycle of artificial intelligence systems that make or support decisions impacting end-users, including providing notice and explanation, and promoting human oversight, such as, for example, through review of automated decisions and related processes or, where appropriate and relevant, human decision-making alternatives or effective redress and accountability for those adversely impacted by automated decisions of artificial intelligence systems;
>
> (l) Strengthening investment in developing and implementing effective safeguards, including risk and impact assessments, throughout the life cycle of artificial intelligence systems to protect the exercise of and mitigate against the potential impact on the full and effective enjoyment of human rights and fundamental freedoms;
>
> [...]

(2.3.2.3) General Comments by UN human rights treaty bodies developing the scope of existing rights

General Comments are not legally binding. However, they are an authoritative tool for promoting clarity on, and expanding the scope of, UN human rights treaties.

Committee on the Rights of the Child, General Comment No 25 (2021) on children's rights in relation to the digital environment, 2 March 2021

> 7. In the present general comment, the Committee explains how States parties should implement the Convention in relation to the digital environment and provides guidance on relevant legislative, policy and other measures to ensure full compliance with their obligations under the Convention and the Optional Protocols thereto in the light of the opportunities, risks and challenges in promoting, respecting, protecting and fulfilling all children's rights in the digital environment.
>
> [...]
>
> 42. States parties should prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling. Practices that rely on neuromarketing, emotional analytics, immersive advertising and advertising in virtual and augmented reality environments to promote products, applications and services should also be prohibited from engagement directly or indirectly with children.

(2.3.2.4) New treaties on human rights and AI

Council of Europe, Framework Convention on AI, Human Rights, Democracy and the Rule of Law, CETS No 225 (concluded 5 September 2024)

A noteworthy development is the recent conclusion of the Council of Europe Framework Convention on AI, Human Rights, Democracy and the Rule of Law (AI Convention). This is the first international treaty regulating AI with its main aim to ensure that AI activities are fully consistent with human rights as well as democracy and the rule of law. The AI Convention does not create new human rights, but it reinforces the role of existing human rights law in addressing AI challenges. The choice of a legally binding international instrument came, however, at a trade-off. Being a framework convention, it establishes broad commitments for

state parties leaving more detailed regulation to subsequent agreements, non-binding instruments, or national legislation.

> **Article 1 – Object and purpose**
>
> 1 The provisions of this Convention aim to ensure that activities within the lifecycle of artificial intelligence systems are fully consistent with human rights, democracy and the rule of law.
>
> 2 Each Party shall adopt or maintain appropriate legislative, administrative or other measures to give effect to the provisions set out in this Convention. These measures shall be graduated and differentiated as may be necessary in view of the severity and probability of the occurrence of adverse impacts on human rights, democracy and the rule of law throughout the lifecycle of artificial intelligence systems. This may include specific or horizontal measures that apply irrespective of the type of technology used.
>
> 3 In order to ensure effective implementation of its provisions by the Parties, this Convention establishes a follow-up mechanism and provides for international co-operation.
>
> **Article 4 – Protection of human rights**
>
> Each Party shall adopt or maintain measures to ensure that the activities within the lifecycle of artificial intelligence systems are consistent with obligations to protect human rights, as enshrined in applicable international law and in its domestic law.
>
> **Article 5 – Integrity of democratic processes and respect for the rule of law**
>
> 1 Each Party shall adopt or maintain measures that seek to ensure that artificial intelligence systems are not used to undermine the integrity, independence and effectiveness of democratic institutions and processes, including the principle of the separation of powers, respect for judicial independence and access to justice.
>
> 2 Each Party shall adopt or maintain measures that seek to protect its democratic processes in the context of activities within the lifecycle of artificial intelligence systems, including individuals' fair access to and participation in public debate, as well as their ability to freely form opinions

(2.3.2.5) Criticism to the AI Convention for not including new rights

Explanatory memorandum by Ms Thórhildur Sunna Ævarsdóttir, Rapporteur, Committee on Legal Affairs and Human Rights, Report, Draft Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, Doc. 15971, 16 April 2024

> 38. [...] I believe that the drafters have missed an opportunity to include new rights, rights that could flow from already existing rights (human dignity, personal autonomy, right to respect for private life) but adapted or specifically tailored to an AI context. For instance, when examining the brain-computer interface technology, the Assembly called on member States to consider establishing new "neurorights", such as cognitive liberty, mental privacy and mental integrity.

(2.3.2.6) Ethical-based frameworks and the human rights-based approach to AI

A Rachovitsa, 'AI and Human Rights', in C Kerrigan (ed), Artificial Intelligence – Law and Regulation (2nd ed, Edward Elgar, 2025)

> Until recently, the relevance of human rights law to risks associated with AI did not feature as a primary concern

in policy and law-making. There are more than 50 AI governance initiatives on a global and regional level, led by States, industry or multiple stakeholders most of which are non-binding. Certain notable, intergovernmental policy frameworks are the 2019 OECD Recommendation on Artificial Intelligence, the 2021 UNESCO Recommendation on the Ethics of Artificial Intelligence and the 2023 Hiroshima AI Process, which set out ethical principles for responsible stewardship of trustworthy AI.

A certain measure of convergence exists regarding these ethical principles. They typically feature transparency, explainability, accountability, safety and security. [...] Some of these also refer to more human rights-like principles and concepts: the principles of fairness and non-discrimination; human-centred values; the right to privacy and data protection; and human-centricity in the design, development and deployment of advanced AI systems. These principles are undoubtedly valuable as they lay out ethical frameworks, build political consensus among States and other actors and even have a certain bearing on human rights protection. Yet, they fall short of bringing international human rights *law* to the foreground. [...] The above policy initiatives reference ethical, non-binding principles and do not explicitly refer to human rights law per se which consists of the rights of individuals and respective obligations of States as well as remedies and redress.

Questions

1. Do we need *new* digital human rights tailored to digital circumstances and/or AI systems? Can you think of specific examples of novel human rights?
2. Evaluate advantages and disadvantages of concluding a new treaty on human rights and new technologies/AI (e.g., the AI Convention) vis-à-vis progressively developing human rights law in other ways.
3. Why the AI Convention purports to protect human rights as well as democracy and the rule of law? Can you think of examples of algorithmic harms that may be not captured by "human rights law" but may be covered by "democracy" or "rule of law"?

(2.4) Restricting Human Rights

States may interfere with the effective exercise of a given human right and restrict it. Human rights are not absolute and may be subject to restrictions, as indicated in human rights treaties.

To take an example, the right to respect for private and family life is protected in the ECHR by Article 8:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Paragraph 1 of the provision formulates the rule, the protective scope of the right. Paragraph 2 provides the exception to the rule, namely **the requirements for an interference with the exercise of this right to be lawful**:

a) it needs to be 'in accordance with the law'

b) it needs to serve one of the specifically mentioned legitimate aims, namely 'in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'

c) it needs to be 'necessary in a democratic society'.

Therefore, a restriction to a given right may be imposed and is lawful under human rights law as long as said restriction is provided by law, serves one of the legitimate aims exhaustively enumerated in the respective provision and is necessary and proportionate to the aim that it is pursued. In most cases, the third requirement is decisive.

Exceptionally, certain human rights are not subject to restrictions. For example, the right to be free from torture, inhuman or degrading treatment or punishment or the right to freedom of thought.

(2.5) Different protection of human rights under different treaties, instruments and regimes

The protection of human rights differs across different treaties. One reason is that treaties differ as to their material scope, since they include different rights in their text. Moreover, there is the possibility that two treaties/instruments contain the same right but the protective scope of that right or the requirements for restricting it are formulated in different ways. It is also significant how courts and other bodies interpret and apply the treaties that they supervise. For example, the UN Human Rights Committee's approach to interpreting 'everyone' under the ICCPR is to include only physical persons whereas the ECtHR's approach is to interpret 'everyone' under the ECHR to include both physical persons and legal entities. One needs to

be aware and cautious of how a given human right may enjoy different levels of protection across different treaties/regimes, especially when assessing the necessity and proportionality of a restriction and the factors that are weighed therein.

(2.5.1) Exercise: comparing the protection accorded under the ECHR and the EU Charter of Fundamental Rights

Can you identify from the EU Charter's provisions quoted below considerations that are important in the context of EU law but not necessarily in the ECHR?

Article 51 EU Charter – Field of application

1. The provisions of this Charter are addressed to the institutions, bodies, offices and agencies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law. They shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective powers and respecting the limits of the powers of the Union as conferred on it in the Treaties.

2. The Charter does not extend the field of application of Union law beyond the powers of the Union or establish any new power or task for the Union, or modify powers and tasks as defined in the Treaties.

Article 52 EU Charter – Scope and interpretation of rights and principles

1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

2. Rights recognised by this Charter for which provision is made in the Treaties shall be exercised under the conditions and within the limits defined by those Treaties. [...]

Article 53 EU Charter – Level of protection

Nothing in this Charter shall be interpreted as restricting or adversely affecting human rights and fundamental freedoms as recognised, in their respective fields of application, by Union law and international law and by international agreements to which the Union or all the Member States are party, including the European Convention for the Protection of Human Rights and Fundamental Freedoms, and by the Member States' constitutions.

—

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://opentextbooks.rug.nl/dataprotectionanddigitalhumanrights/?p=5#h5p-11

(2.6) Scope of Human Rights Obligations

This section clarifies two aspects of the scope of human rights obligations, namely the personal scope and territorial scope.

(2.6.1) Personal scope of human rights obligations

The personal scope of human rights obligations answers two questions:

- Who has the right to be protected?
- Who bears the responsibility to protect human rights?

(2.6.1.1) States are bound to protect the human rights of individuals

The answer to the question of who has the right to be protected in human rights law is: all individuals. The answer to the question of who bears the responsibility to protect human rights is that States and state authorities are responsible for protecting human rights. This means that States are not, in principle, responsible for protecting individuals from private actors. Human rights law essentially sets up and regulates a specific relationship between individuals and the State.

Article 2(1) ICCPR

Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

Article 1 ECHR

The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention.

(2.6.1.2) Holding States responsible for acts/omissions of non-state actors – the due diligence standard

Although human rights obligations bound only States, in certain circumstances, States may be required to enact special measures to protect human rights also from the actions/omissions of private actors. Human rights bodies and courts have developed their approaches as to when States have such a due diligence obligation.

(2.6.1.2.1) The UN Human Rights Committee regarding State parties' obligations to exercise due diligence

UN Human Rights Committee, General Comment No 31 on the nature of the general legal obligation imposed on States Parties to the Covenant: International Covenant on Civil and Political Rights (2004)

> 8. The article 2, paragraph 1, obligations are binding on States and do not, as such, have direct horizontal effect as a matter of international law. The Covenant cannot be viewed as a substitute for domestic criminal or civil law. However the positive obligations on States Parties to ensure Covenant rights will only be fully discharged if individuals are protected by the State, not just against violations of Covenant rights by its agents, but also against acts committed by private persons or entities that would impair the enjoyment of Covenant rights in so far as they are amenable to application between private persons or entities take appropriate measures or to exercise due diligence to prevent, punish, investigate or redress the harm caused by such acts by private persons or entities.

(2.6.1.2.2) The European Court of Human Rights develops the "Osman test" on due diligence

ECtHR, Osman v United Kingdom, App no 23452/94, 28 October 1998 (Grand Chamber)

> 115. The Court notes that the first sentence of Article 2 § 1 enjoins the State not only to refrain from the intentional and unlawful taking of life, but also to take appropriate steps to safeguard the lives of those within its jurisdiction [...]. It is common ground that the State's obligation in this respect extends beyond its primary duty to secure the right to life by putting in place effective criminal-law provisions to deter the commission of offences against the person backed up by law-enforcement machinery for the prevention, suppression and sanctioning of breaches of such provisions. It is thus accepted by those appearing before the Court that Article 2 of the Convention may also imply in certain well-defined circumstances a positive obligation on the authorities to take preventive operational measures to protect an individual whose life is at risk from the criminal acts of another individual. [...]
>
> 116. For the Court and bearing in mind the difficulties involved in policing modern societies, the unpredictability of human conduct and the operational choices which must be made in terms of priorities and resources, such an obligation must be interpreted in a way which does not impose an impossible or disproportionate burden on the authorities.
>
> [...]
>
> In the opinion of the Court where there is an allegation that the authorities have violated their positive obligation to protect the right to life in the context of their above-mentioned duty to prevent and suppress offences against the person [...], it must be established to its satisfaction that the authorities knew or ought to have known at the time of the existence of a real and immediate risk to the life of an identified individual or individuals from the criminal acts of a third party and that they failed to take measures within the scope of their powers which, judged reasonably, might have been expected to avoid that risk. [...]

(2.6.1.2.3) The Court of Justice of the Economic Community of West African States fleshes out the due diligence standard

According to the Court, States' obligation to take measures includes the obligation to introduce legislation,

create bodies and procedures to implement legislation and take concrete measures for preventing harm or ensuring accountability, if such harm has occurred.

Court of Justice of the Economic Community of West African States (ECOWAS), SERAP v Federal Republic of Nigeria, Judgment no ECW/CCJ/JUD/18/12, 14 December 2012

> [...]
>
> 95. From the submissions of both Parties, it has emerged that the Niger Delta is endowed with arable land and water which the communities use for their social and economic needs; several multinational and Nigerian companies have carried along oil prospection as well as oil exploitation which caused and continue to cause damage to the quality and productivity of the soil and water; the oil spillage, which is the result of various factors including pipeline corrosion, vandalisation, bunkering, etc. appears for both sides as the major source and cause of ecological pollution in the region. It is a key point that the Federal Republic of Nigeria has admitted that there has been in Niger Delta occurrences of oil spillage with devastating impact on the environment and the livelihood of the population throughout the time.
>
> [...]
>
> 98. As such, the heart of the dispute is to determine whether in the circumstances referred to, the attitude of the Federal Republic of Nigeria, as a party to the African Charter on Human and Peoples' Rights, is in conformity with the obligations subscribed to in the terms of Article 24 of the said instrument, which provides: *"All peoples shall have the right to a general satisfactory environment favourable to their development"*.
>
> 99. The scope of such a provision must be looked for in relation to Article 1 of the Charter, which provides: *"The Member States of the Organization of African Unity parties to the present Charter shall recognise the rights, duties and freedoms enshrined in this Charter and shall undertake to adopt legislative or other measures to give effect to them."*
>
> [...]
>
> 101. Article 24 of the Charter thus requires every State to take every measure to maintain the quality of the environment understood as an integrated whole, such that the state of the environment may satisfy the human beings who live there, and enhance their sustainable development.
>
> [...]
>
> 103. Among these measures, the Court takes note of the numerous laws passed to regulate the extractive oil and gas industry and safeguard their effects on the environment, the creation of agencies to ensure the implementation of the legislation, and the allocation to the region, 13% of resources produced there, to be used for its development.
>
> [...]
>
> 105. This means that the adoption of the legislation, no matter how advanced it may be, or the creation of agencies inspired by the world's best models, as well as the allocation of financial resources in equitable amounts, may still fall short of compliance with international obligations in matters of environmental protection if these measures just remain on paper and are not accompanied by additional and concrete measures aimed at preventing the occurrence of damage or ensuring accountability, with the effective reparation of the environmental damage suffered.
>
> [...]
>
> 111. And it is precisely this omission to act, to prevent damage to the environment and to make accountable the offenders, who feel free to carry on their harmful activities, with clear expectation of impunity, that characterises the violation by the Federal Republic of Nigeria of its international obligations under Articles 1 and 24 of the African Charter on Human and Peoples' Rights.

[...]

(2.6.2) Territorial scope of human rights obligations

The territorial scope of human rights obligations clarifies *where* human rights need to be protected. It seems straightforward that a human rights treaty applies within the territory of a State party. But what about situations outside the territory of a State party? Are there scenarios that a State may be responsible for protecting human rights outside of its territory?

(2.6.2.1) Article 2(1) International Covenant on Civil and Political Rights

> Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant.

(2.6.2.2) UN Human Rights Committee, General Comment No 31 (2004)

> 10. States Parties are required by article 2, paragraph 1, to respect and to ensure the Covenant rights to all persons who may be within their territory and to all persons subject to their jurisdiction. This means that a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party.

(2.6.2.3) UN Human Rights Council, Res 42/15, The Right to Privacy in the Digital Age, 26 September 2019

> *Emphasizing* that unlawful or arbitrary surveillance and/or interception of communications, the unlawful or arbitrary collection of personal data or unlawful or arbitrary hacking and the unlawful or arbitrary use of biometric technologies, as highly intrusive acts, violate or abuse the right to privacy, can interfere with other human rights, including the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association, and may contradict the tenets of a democratic society, including when undertaken extraterritorially or on a mass scale

(2.6.2.4) Article 1 European Convention on Human Rights

> The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention.

(2.6.2.5) The ECtHR's first opportunity to consider and decide whether an interference with an applicant's electronic communications falls within the jurisdiction of a State

ECtHR, Wieder and Guarnieri v United Kingdom, App nos 64371/16 and 64407/16, 12 September 2023

> 1. The principal issue to be addressed in the present case is whether, for the purposes of a complaint under Article 8 of the Convention, persons outside a Contracting State fall within its territorial jurisdiction if their electronic communications were (or were at risk of being) intercepted, searched and examined by that State's intelligence agencies operating within its borders.

[...]

6. The first applicant is an IT professional and independent researcher. He has worked for commercial data centres and news organisations.

7. The second applicant is a privacy and security researcher and the creator of an open source malware analysis system. He has researched and published extensively on privacy and surveillance with Der Spiegel and The Intercept.

[...]

12. The applicants in the present case lodged applications with the [Investigatory Powers Tribunal (IPT)] with the aid of a standard application form made available on Privacy International's website. They alleged that the respondent Government and/or the security services had breached Articles 8 and 10 of the Convention because they had and/or continued to intercept, solicit, obtain, process, use, store and/or retain their information and/or communications; and because their information and/or communications were accessible to the respondent Government as part of datasets maintained wholly or in part by other Governments' intelligence agencies; and that the Government and/or security services might have acted unlawfully under domestic law by intercepting, soliciting, accessing, obtaining, processing, storing or retaining their information and/or communications in breach of their own internal policies and procedures.

[...]

74. The Government asserted that the interception of communications by a Contracting State did not fall within that State's jurisdictional competence for the purposes of Article 1 of the Convention when the sender or recipient complaining of a breach of their Article 8 rights was outside the territory of the Contracting State.

75. The Government argued that a State's jurisdiction within the meaning of Article 1 of the Convention was primarily territorial. Any other basis of jurisdiction was exceptional and required special justification in the particular circumstances [...]. In Al-Skeini and Others v. the United Kingdom [GC], no. 55721/07, §§ 133-42, ECHR 2011 the Grand Chamber had set out three exceptions to the territorial basis of jurisdiction: State agent authority and control; effective control over an area; and the Convention legal space ("espace juridique"). [...]

76. For the Government, the interception of communications and related communications data would not involve the exercise of authority and control over the individual whose privacy was interfered with. Given that intercepted communications nevertheless continued on to the recipient, GCHQ could not be said to have exercised full authority and control over those communications, much less over the sender or recipient.

77. The Government further argued that [since] the applicants had not been physically present in the United Kingdom at any relevant point, any interference with their privacy or freedom of expression must have taken place outside the United Kingdom. In this regard, the Government disputed that the interference with the applicants' rights under Article 8 of the Convention was the interception, extraction, filtering, storage, analysis and dissemination of intercepted content and related communications data. For the Government, a person's private life was a matter of personal autonomy. Interferences with, and effects upon, his private life were therefore not abstract concepts which could be separated from the individual, but rather events which happened to the individual. That was so even if the originating cause of the impact or interference took place in a different State. The interference happened to the individual, and thus took place where the individual was located. [...]

79. For the Government, there was nothing absurd about individuals outside the United Kingdom falling outside that State's territorial jurisdiction. On the contrary, it was simply a natural consequence of the territorial nature of jurisdiction. The very fact that the Convention was not universal meant that jurisdictional lines had to be drawn, and some individuals would fall outside those lines. Such an outcome would not lead to the inevitable conclusion that controls over extraterritorial acts were lacking.

[...]

81. The applicants argued that their communications and/or related communications data fell within the United Kingdom's jurisdiction for the purposes of Article 1 of the Convention. In their opinion, where interception, storage, processing and interrogation of communications was carried out by the Contracting State on its own territory, it fell within its jurisdictional competence for two reasons.

82. First, where a Contracting State intercepted communications and/or related communications data within its own borders, the resulting interference with Convention rights was within that State's jurisdiction, even if the victim was abroad at the moment of interference. For the applicants, this was consistent with the Court's approach to jurisdiction in respect of other Convention rights, including Article 1 of Protocol No. 1 [...], Article 6 [...], Article 13 [...] and Article 5 [...]. They argued that the same approach should apply under Article 8 of the Convention; as with the interference with property, when "correspondence" was intercepted, opened, and read by a Contracting State, the interference took place within the jurisdiction of that State. Any other outcome would render Convention rights illusory in practice.

83. Secondly, the applicants contended that the activity fell within the scope of one of the recognised exceptions to territoriality. When a State carried on secret surveillance in its territory it exercised authority and control over the victim whose communications were intercepted. In the United Kingdom, surveillance was carried out with legal authority and the intelligence agencies assumed full control over intercepted communications. There was no principled basis for holding that "State agent authority and control" required physical control and power over individuals abroad.

84. Finally, the applicants submitted that the consequences would be absurd if they were not within the United Kingdom's jurisdiction for the purposes of Article 1 of the Convention merely because they were not present within its territory at the moment when interception occurred. It would mean that Contracting States could conduct mass surveillance of everyone outside their territory, including their own citizens and citizens of all other Council of Europe Contracting States, and share intelligence obtained in respect of those individuals, without complying with any of the safeguards required by Article 8 of the Convention. It would also mean that if the communications of a person habitually resident in the United Kingdom were intercepted while he was temporarily out of the country, and analysed after his return, the State would have jurisdiction in respect of the analysis but not in respect of the original interception. There was no rational basis for this distinction, which made little sense in view of the fact that the proliferation of online communications had deprived national borders of their meaning.

[...]

(β) Application of the general principles to the facts of the present case

88. To date, the Court has not had the opportunity to consider the question of jurisdiction in the context of a complaint concerning an interference with an applicant's electronic communications. In Bosak and Others v. Croatia (nos. 40429/14 and 3 others, 6 June 2019) the Court did not consider whether the interception of the communications of the two applicants who were living in the Netherlands fell within Croatia's jurisdiction for the purposes of Article 1 of the Convention, perhaps because those applicants' telephone conversations were intercepted and recorded by the Croatian authorities on the basis of secret surveillance orders lawfully issued against another applicant, who lived in Croatia and with whom they had been in contact. While the question of jurisdiction was alluded to in Weber and Saravia v. Germany (dec.), no. 54934/00, § 72, ECHR 2006-XI and in Big Brother Watch and Others [..], in neither case was it necessary to decide the issue.

89. The applicants in the present case have not suggested that they were themselves at any relevant time in the United Kingdom or in an area over which the United Kingdom exercised effective control. Rather, they contend either that the acts complained of – being the interception, extraction, filtering, storage, analysis and dissemination of their communications by the United Kingdom intelligence agencies pursuant to the section

8(4) [of the Regulation of Investigatory Powers Act 2000] regime [...] – nevertheless fell within the respondent Government's territorial jurisdiction, or, in the alternative, that one of the exceptions to the principle of territoriality applied.

90. In Big Brother Watch and Others the Court identified four stages to the bulk interception process: the interception and initial retention of communications and related communications data; the searching of the retained communications and related communications data through the application of specific selectors; the examination of selected communications/related communications data by analysts; and the subsequent retention of data and use of the "final product", including the sharing of data with third parties [...]. Although it did not consider that the interception and initial retention constituted a particularly significant interference, in its view the degree of interference with individuals' Article 8 rights increased as the bulk interception process progressed [...]. The principal interference with the Article 8 rights of the sender or recipient was therefore the searching, examination and use of the intercepted communications.

91. In the context of the section 8(4) regime each of the steps which constituted an interference with the privacy of electronic communications, being the interception and, more particularly, the searching, examining and subsequent use of those intercepted communications, were carried out by the United Kingdom intelligence agencies acting – to the best of the Court's knowledge – within United Kingdom territory.

92. It is the Government's contention that any interference with the applicants' private lives occasioned by the interception, storage, searching and examination of their electronic communications could not be separated from their person and would therefore have produced effects only where they themselves were located – that is, outside the territory of the United Kingdom.

[...]

94. Turning to the facts of the case at hand, the interception of communications and the subsequent searching, examination and use of those communications interferes both with the privacy of the sender and/or recipient, and with the privacy of the communications themselves. Under the section 8(4) regime the interference with the privacy of communications clearly takes place where those communications are intercepted, searched, examined and used and the resulting injury to the privacy rights of the sender and/or recipient will also take place there.

95. Accordingly, the Court considers that the interference with the applicants' rights under Article 8 of the Convention took place within the United Kingdom and therefore fell within the territorial jurisdiction of the respondent State. As such, it is not necessary to consider whether any of the exceptions to the territoriality principle are applicable.

(2.7) Are Private/Business Actors Responsible for Human Rights Violations?

Private actors, including business actors, can play a significant role in ensuring the effective exercise of human rights. The greatest part of the technological infrastructure is being designed, developed, deployed in the realm of privatisation via a web of contracts and without public law guarantees. Despite the corporations' paramount role, their activities are very little grounded in (human rights) law. Private actors and corporations are not

bound by human rights treaty obligations. Corporations are expected to abide by non-binding frameworks concerning the mitigation of the human rights' impacts of their activities, such as the UN Guiding Principles on Business and Human Rights. Yet business corporations are still bound by the domestic law of the State within the jurisdiction of which they operate and provide their products/services. This means that human rights related issues may come into play before domestic courts and that corporations may have obligations pursuant to legislation introduced by domestic law (or EU law).

(2.7.1) The UN Guiding Principles on Business and Human Rights

You may read the UN Guiding Principles on Business and Human Rights.

(2.7.1.1) Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Freedom of expression, states and the private sector in the digital age, 11 May 2016

> 9. Human rights law does not as a general matter directly govern the activities or responsibilities of private business. A variety of initiatives provide guidance to enterprises to ensure compliance with fundamental rights. The Human Rights Council endorsed the Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (see A/HRC/17/4 and A/HRC/17/31). Reflecting existing human rights law, the Guiding Principles reaffirm that States must ensure that not only State organs but also businesses under their jurisdiction respect human rights.
>
> 10. The Guiding Principles provide a framework for the consideration of private business responsibilities in the information and communications technology sector worldwide, independent of State obligations or implementation of those obligations. For instance, the Guiding Principles assert a global responsibility for businesses to avoid causing or contributing to adverse human rights impacts through their own activities, and to address such impacts when they occur and seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts.
>
> 11. Due diligence, according to the Guiding Principles, enables businesses to identify, prevent, mitigate and account for how they address their adverse human rights impacts [...] In the digital environment, human rights impacts may arise in internal decisions on how to respond to government requests to restrict content or access customer information, the adoption of terms of service, design and engineering choices that implicate security and privacy, and decisions to provide or terminate services in a particular market.
>
> 12. As a matter of transparency, the Guiding Principles state that businesses should be prepared to communicate how they address their human rights impacts externally, particularly when concerns are raised by or on behalf of affected stakeholders [...] Meaningful disclosures shed light on, among other things, the volume and context of government requests for content removals and customer data, the processes for handling such requests, and interpretations of relevant laws, policies and regulations. Corporate transparency obligations may also include a duty to disclose processes and reporting relating to terms of service enforcement and private requests for content regulation and user data.
>
> 13. Finally, the responsibility to respect involves attention to the availability of remedies — from moral remedies to compensation and guarantees of non-repetition — when the private actor has caused or contributed to adverse impacts.

(2.7.1.2) Business and Human Rights in Technology Project

According to the Business and Human Rights in Technology Project (B-Tech Project), which tailors the UN Guiding Principles to digital technologies, due diligence should apply to the conceptualisation, design and testing phases of new products – as well as the underlying data sets and algorithms.

You can read more about the B-Tech Project here.

(2.7.2) Privatisation of the Effective Exercise of Human Rights

Due to the private nature of the products and serviced offered, the effective exercise of human rights is also subject to privatisation. An individual does not have a legal claim vis-à-vis a business actor for protecting/violating their human rights – human rights apply only in the relationship between State-individual. The relationship between an individual and a business actor is subject to other areas of law, such as contract or tort law. The terms of service of a product/service that we use qualifies as a contract.

(2.7.2.1) Terms of Service

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Freedom of expression, states and the private sector in the digital age, 11 May 2016

> 52. Terms of service, which individuals typically must accept as a condition to access a platform, often contain restrictions on content that may be shared. These restrictions are formulated under local laws and regulations and reflect similar prohibitions, including those against harassment, hate speech, promotion of criminal activity, gratuitous violence and direct threats. Terms of service are frequently formulated in such a general way that it may be difficult to predict with reasonable certainty what kinds of content may be restricted. The inconsistent enforcement of terms of service has also attracted public scrutiny. Some have argued that the world's most popular platforms do not adequately address the needs and interests of vulnerable groups; for example, there have been accusations of reluctance "to engage directly with technology-related violence against women, until it becomes a public relations issue". At the same time, platforms have been criticized for overzealous censorship of a wide range of legitimate but (perhaps to some audiences) "uncomfortable" expressions. Lack of an appeals process or poor communication by the company about why content was removed or an account deactivated adds to these concerns. Terms of service that require registration linked to an individual's real name or evidence to demonstrate valid use of a pseudonym can also disproportionately inhibit the ability of vulnerable groups or civil society actors in closed societies to use online platforms for expression, association or advocacy
>
> [...]
>
> Remedies and enforcement of terms of service
>
> 69. To enforce terms of service, companies may not always have sufficient processes to appeal content removal or account deactivation decisions where a user believes the action was in error or the result of abusive flagging campaigns. Further research that examines best practices in how companies communicate terms of service enforcement decisions and how they implement appeals mechanisms may be useful.
>
> [...]
>
> 71. The appropriate role of the State in supplementing or regulating corporate remedial mechanisms also requires closer analysis. Civil proceedings and other judicial redress are often available to consumers adversely affected by corporate action, but these are often cumbersome and expensive. Meaningful alternatives may include complaint and grievance mechanisms established and run by consumer protection bodies and industry regulators. Several States also mandate internal remedial or grievance mechanisms: India, for example, requires

corporations that possess, deal with or handle sensitive personal data to designate grievance officers to address "any discrepancies and grievances [...] with respect to processing of information".

For example, if you watch YouTube, your rights are conditioned to the YouTube's Terms of Service. These terms of Service consist of a series of terms and policies:

Applicable Terms

Your use of the Service is subject to these terms, the YouTube Community Guidelines and the Policy, Safety and Copyright Policies (together, the "Agreement"). Your Agreement with us will also include the Advertising on YouTube Policies if you provide advertising or sponsorships to the Service or incorporate paid promotions in your Content.

Policies overview

Viewers and creators around the world use YouTube to express their ideas and opinions freely, and we believe that a broad range of perspectives ultimately makes us a stronger and more informed society, even if we disagree with some of those views. That's why we have policies to help build a safer community.

- **Community Guidelines**
- **Copyright**
- **Monetisation policies**
- **Legal removals**

Community Guidelines

- Spam and deceptive practices (e.g., fake engagement)
- Sensitive content (e.g., child safety, nudity and sexual content, suicide and self-harm, vulgar language)
- Violent or dangerous content (e.g., harassment and cyberbullying, harmful or dangerous content, hate speech, violent criminal organisations, violent or graphic content)
- Misinformation (e.g., medical or elections misinformation)

(2.7.2.2) Creating novel private "adjudicative" bodies

A novel example of setting up external bodies to scrutinise technologies and AI systems is creation of the META Oversight Board. The Board decides appeals brought by individuals against META's content

enforcement decisions. Given the fact that these remedies belong in the realm of private governance, it is an open question whether they qualify as adequate and effective remedies.

Oversight Board Charter, September 2019

> [...]
>
> The purpose of this charter is to establish the framework for creating such an institution: the Oversight Board. The purpose of the board is to protect free expression by making principled, independent decisions about important pieces of content and by issuing policy advisory opinions on Facebook's content policies. The board will operate transparently and its reasoning will be explained clearly to the public, while respecting the privacy and confidentiality of the people who use Facebook, Inc.'s services, including Instagram (collectively referred to as "Facebook"). It will provide an accessible opportunity for people to request its review and be heard.
>
> [...]
>
> Article 2. Authority to Review
>
> People using Facebook's services and Facebook itself may bring forward content for board review. The board will review and decide on content in accordance with Facebook's content policies and values.
>
> Section 2. Basis of decision-making
>
> Facebook has a set of values that guide its content policies and decisions. The board will review content enforcement decisions and determine whether they were consistent with Facebook's content policies and values. For each decision, any prior board decisions will have precedential value and should be viewed as highly persuasive when the facts, applicable policies, or other factors are substantially similar.
>
> When reviewing decisions, the board will pay particular attention to the impact of removing content in light of human rights norms protecting free expression.
>
> [...]

Decisions by the META Oversight Board are discussed in sections **(4.3.3), (5.5.2).**

(2.7.3) Corporations and their activities are subject to domestic law

(2.7.3.1) Civil litigation before domestic courts to enforce terms of service – How human rights law may still be partly relevant

Business actors/corporations are bound by the domestic law of the State within the jurisdiction of which they operate and provide their products/services. For instance, AI systems are deployed and used pursuant to contracts, such as, for example, contract terms, terms of services and policies of social media platforms which users accept when signing up for using their services. In case of a breach of contract, an individual may be able to bring civil proceedings before domestic courts under contract or tort law. In certain instances, human rights

law may also come into play, subject to the specific requirements under domestic law, such as the standard of reasonableness/fairness under Dutch civil law (tort).

(2.7.3.1.1) Amsterdam District Court, FvD c.s. v Google Ireland Ltd, Case number C/13/704886 / KG ZA 21-621, Judgment in summary proceedings, 15 September 2021 (civil law) (in Dutch) (unofficial translation)

The case was brought by the Forum for Democracy (FvD), a Dutch political party.

> 3.2. FvD(s) [Forum for Democracy] based their claims in particular on the following statements:
>
> – the expressions in the Video do not contain any content that may lead to significant risk of serious harm and, in that respect, do not violated the Terms of Service, the Community Guidelines and/or Covid Policies;
>
> – insofar as the expressions are contrary to the views of the WHO and the RIVM, the policy to prohibit it goes too far, because it creates an impermissible interference with the freedom of expression of FvD et al., also against the background of YouTube's monopoly position and claimant 3's position as a politician. FvD is effectively silenced, making it impossible to criticize controversial government politics. Thus, by removing the Video, YouTube acted in violation of standards of reasonableness and fairness and unlawful towards FvD et al. The interests of FvD et al. in reinstating the Video outweigh YouTube's right of ownership and the public health interests served by a strict application of the Covid policy.
>
> 3.3. Google puts forward a reasoned defence. It argues that YouTube was justified in removing the Video pursuant to the Terms of Service and the Covid Policy and further relies on its property rights and the right of freedom of business.
>
> 4 The assessment
>
> 4.1. First and foremost, YouTube and FvD et al are private parties. FvD et al. accepted the Terms of Service when creating their YouTube accounts. An agreement has been concluded between the parties, on the basis of which FvD et al. are in principle bound by the Terms of Service, the Community Guidelines and the Covid Policy.
>
> 4.2. Google rightly takes the position that the statements of claimant 3 ... are at odds with various provisions ... from the Covid Policy and can be regarded as a violation thereof. This applies in particular to the provisions dealing with face masks, social distancing and the comparison with influenza, as well as the provisions prohibiting claiming that vaccines do not reduce the risk of COVID-19 and claiming that ivermectin or hydroxychloroquine are effective treatments for Covid-19. Even taking into account the provocative style peculiar to claimant 3, the use of terms such as "a collective psychosis" "a flu variation, "utterly nonsensical distancing lines", "experimental injections" versus "first-line drugs, such as ivermectin", can only be seen as a violation of those provisions. Unlike FvD et al. argue, these expressions cannot (obviously) be seen as 'imagery'. That claimant 3, as FvD et al. argue, "does not strictly speaking question the effectiveness of the distancing rules" can – also in light of his own statements, attitude in public and other public performances – hardly be taken seriously.
>
> 4.3. This leads to the (interim) conclusion that, for the time, the statements of claimant 3 in the Video are in breach of Covid Policy, and YouTube's removal is in line with the Terms of Service and therefore in breach the agreement between the parties.
>
> 4.4. The foregoing does not alter the fact that there may be grounds to consider the removal of the Video unacceptable or unlawful according to the standards of reasonableness and fairness. In this context, FvD et al. have invoked their freedom of expression.

4.5. As considered in previous judgments of the judge in preliminary relief proceedings of this District Court1, Article 10 of the ECHR, which establishes the right to freedom of expression, may have an effect on private law relations, for example through the interpretation of open norms of private law, such as the obligation to act in accordance with the standards of reasonableness and fairness when performing a contract. The same applies to the open norm included in Article 6:162 of the Ducth Civil Code (tort): an act or omission contrary to "what is proper in social intercourse according to unwritten law" is also regarded as a tort. The court must assess whether these standards have been met. In that assessment, the following applies as a starting point.

4.6. Everyone's right to freedom of expression is not unlimited and does not mean that Google is unquestionably bound to tolerate the statements of FvD et al. that violate its Covid policy on its platform. By virtue of its property rights and the right to freedom of enterprise, Google may, in principle, set rules that apply to its YouTube platform, including the rule that content that violates its Covid policy will be removed. Google explained that the Covid policy aims to prevent the spread of harmful and dangerous medical misinformation on YouTube. Since Google cannot enter into medical discussions itself, it aligns itself with the scientific consensus as it is propagated by the WHO and by national organizations such as the RIVM. The Covid policy is partly based on a European Union Communication of 10 June 2020 that aimed at combating misinformation about Covid-19, as well as the European Commission's *Code of Practice* of October 2018 on combating online disinformation. With Google's Covid policy following the guidelines of such health organizations and various governments, the starting point should be that it is not acting unreasonably, but on the contrary, that it is acting in a way that is "befitting unwritten law in society".

4.7. Furthermore, everyone's right to freedom of expression does not imply a right to the forum of his or her choice. FvD et al. acknowledges this in itself, but has emphasized the circumstance that YouTube has a huge reach and that research shows that a substantial part of the public also uses that channel for news coverage. According to this research, this applies in particular to younger people, who are an important part of the (potential) electorate of FvD and claimant 3. According to FvD et al., YouTube is in fact indispensable for bringing the critical views as expressed in the Video to the attention of this audience. Other social media are less suitable for this because of their design (you have to be a member of Facebook) and/or its volatile nature (Twitter, Instagram), or are relatively unknown (Bitchute and Utreon).

4.8. It should be accepted that FvD et al. being able to use a channel like YouTube is of great importance in today's society to be able so as to convey a message. However, this does not mean that YouTube has a social *'must-carry'* obligation for critical voices/political expressions. No such an obligation is included in the (European) proposal for the Digital Service Act (the Digital Service Act) either. In light of the ECHR's Appleby judgment of May 6, 2003 2, the bar for government intervention, or the courts, in the freedom of internet platforms to moderate the content they publish is high. Only if the obstacles make *"any effective* exercise" impossible, or if *"the essence of the right has been* destroyed", is the government (court) obliged to intervene. It is therefore only if the effective exercise of the freedom of expression is prevented, or if the essence of the right to freedom of expression is destroyed, that there is reason to intervene. That high bar is not met here.

[...]

(2.7.3.2) Corporations are subject to obligations introduced by EU law

An example of an obligation imposed on specific corporations (e.g., providers of very large online platforms and providers of very large online search engines) under EU law is:

Article 34(1), Risk Assessment, Digital Services Act Regulation

Providers of very large online platforms and of very large online search engines shall diligently identify, analyse and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services.

They shall carry out the risk assessments by the date of application referred to in Article 33(6), second subparagraph, and at least once every year thereafter, and in any event prior to deploying functionalities that are likely to have a critical impact on the risks identified pursuant to this Article. This risk assessment shall be specific to their services and proportionate to the systemic risks, taking into consideration their severity and probability, and shall include the following systemic risks:

(a) the dissemination of illegal content through their services;

(b) any actual or foreseeable negative effects for the exercise of fundamental rights, in particular the fundamental rights to human dignity enshrined in Article 1 of the Charter, to respect for private and family life enshrined in Article 7 of the Charter, to the protection of personal data enshrined in Article 8 of the Charter, to freedom of expression and information, including the freedom and pluralism of the media, enshrined in Article 11 of the Charter, to non-discrimination enshrined in Article 21 of the Charter, to respect for the rights of the child enshrined in Article 24 of the Charter and to a high-level of consumer protection enshrined in Article 38 of the Charter;

(c) any actual or foreseeable negative effects on civic discourse and electoral processes, and public security;

(d) any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being

Rights & obligations under different documents			
Legal/ethical document	**Obligations for states**	**Obligations for private actors**	**Rights for individuals**
Human rights law treaties	✓	✗	✓
EU Charter on Fundamental Rights	✓	can be	✓
UN Guiding Principles on Business & Human Rights (ethical document)	✗	✗	✗
Domestic law provisions (e.g., tort law, contract law, consumer law)	depends	✓	✓
EU Digital Services Act	✓	✓	✗
EU AI Act	✓	✓	✗
Framework AI Convention	✓	depends (in principle, no)	✗

(2.8) Are Certain AI Systems Incompatible with the Exercise of Human Rights?

The development and/or use of certain AI systems by public and/or the private actors alike pose novel challenges to human autonomy and dignity. In certain cases, these technologies and systems may be impossible to operate in compliance with international human rights law or may pose undue risks to the enjoyment of human rights. Scenarios on prohibiting the use of certain AI systems and the different human rights that may be engaged are discussed in subsequent chapters (see (3.5.3), (4.4) and chapter 7).

States share some of their concerns in political documents in the UN General Assembly (2.8.1) and the

UN Human Rights Council (2.8.2). However, there is distinctive reluctance in formulating consensus on the precise criteria for such systems to be incompatible with the exercise of human rights. The recently concluded Council of Europe, Framework Convention on AI, Human Rights, Democracy and the Rule of Law fell short of expectations in this regard (2.8.3). Article 16(6) leaves discretion to State parties to assess the need for banning certain AI systems and does not provide clear criteria or guidance to this end. The EU AI Act is the only legally binding instrument at the moment that prohibits the development and/or use of certain AI systems (2.8.4).

Although presently States are hesitant to pronounce (either under domestic or international law) certain technologies and AI systems in abstracto incompatible with human rights, these systems and practices may be found, in the specific circumstances of cases, disproportionate or unnecessary to the aims that they purport to serve.

(2.8.1) UNGA Res 78/265, Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development, 1 April 2024, UN Doc A/RES/78/265

> Emphasizes that human rights and fundamental freedoms must be respected, protected and promoted throughout the life cycle of artificial intelligence systems, calls upon all Member States and, where applicable, other stakeholders to refrain from or cease the use of artificial intelligence systems that are impossible to operate in compliance with international human rights law or that pose undue risks to the enjoyment of human rights, especially of those who are in vulnerable situations, and reaffirms that the same rights that people have offline must also be protected online, including throughout the life cycle of artificial intelligence system
>
> [...]

(2.8.2) UN Human Rights Council, Res 54/21, The Right to Privacy in the Digital Age, UN Doc A/HRC/RES/54/21, 12 October 2023

> 3. *Also recalls* the increasing impact of new and emerging technologies, such as those developed in the fields of surveillance, artificial intelligence, automated decision-making and machine-learning, and of profiling, tracking and biometrics, including facial recognition, without human rights safeguards, present to the full enjoyment of the right to privacy and other human rights, and acknowledges that some applications may not be compatible with international human rights law

(2.8.3) Article 16(6) – Risk and impact management framework, Council of Europe, Framework Convention on AI, Human Rights, Democracy and the Rule of Law

> Each Party shall assess the need for a moratorium or ban or other appropriate measures in respect of certain uses of artificial intelligence systems where it considers such uses incompatible with the respect for human rights, the functioning of democracy or the rule of law.

(2.8.4) Prohibited AI systems under the EU AI Act

The EU AI Act provides in Article 5 prohibited AI systems concerning the development and/or deployment of AI systems both in the public and private sectors. Such AI systems raise serious concerns due to their highly intrusive nature and broad impact on many people. Examples of such systems include aspects of:

- manipulation and exploitation of vulnerabilities (Article 5(1)(a) and (b))
- social scoring practices (Article 5(1)(c))
- predictive policing (Article 5(1)(d))
- creation or expansion of facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage (Article 5(1)(e))
- sentiment detection (Article 5(1)(f))
- biometric categorisation systems that categorise individuals based on their biometric data so as to deduce or infer sensitive characteristics (Article 5(1)(g))
- real-time remote biometric identification systems in publicly accessible spaces for law-enforcement purposes (Article 5(1)(h))

It needs to be clarified that the AI Act does **not** create rights for individuals. It rather imposes due diligence and transparency obligations on private and public actors when they develop and/or deploy certain AI systems.

The European Commission has published Guidelines on prohibited artificial intelligence practices established by the EU AI Act, C(2025) 884 final, 4 February 2025

(2.8.5) Exercise: GPT-4Chan – Assessing the development of certain advanced AI systems as incompatible with human rights

GPT-4Chan, is a controversial Large Language Model (LLM) that was developed and deployed by YouTuber and AI researcher Yannic Kilcher in June 2022. The LLM generates text-based input having

been trained on a dataset of millions of posts from the /pol/ board of 4chan, an anonymous online forum known for hosting hateful and extremist content. The model was trained to mimic the style and tone of /pol/ users, producing text that is often intentionally offensive to groups (racist, sexist, homophobic, etc.) and nihilistic.

- Further reading: A Kurenkov, Lessons from the GPT-4Chan Controversy, The Grandient, 12 June 2022

Do you think that the development of GPT-4Chan (and not merely its use/deployment) could be incompatible with human rights?

Further readings

- K Yeung, Study on Responsibility and AI (Council of Europe, 2019)
- A Rachovitsa, 'AI and Human Rights', in C Kerrigan (ed), Artificial Intelligence – Law and Regulation (Edward Elgar, 2025)
- SA Teo, 'How Artificial Intelligence Systems Challenge the Conceptual Foundations of the Human Rights Legal Framework' (2022) 40 Nordic Journal of Human Rights 216
- L McGregor et al, 'International Human Rights Law as a Framework for Algorithmic Accountability' (2019) 68 International & Comparative Law Quarterly
- B Custers, 'New Digital Rights: Imagining Additional Fundamental Rights for the Digital Era' (2022) 44 Computer Law & Security Review 1
- E Aizenberg, J van der Hoven, 'Designing for Human Rights in AI', Jul–Dec 2020 Big Data & Society 1.
- A Quintavalla, J Temperman (eds), Artificial Intelligence and Human Rights (OUP 2023)

3. RIGHT TO PRIVACY

Outline of the chapter

This chapter sets out some of the prominent challenges that new technologies and AI systems pose to the right to privacy. In particular, the chapter addresses:

- what the protective scope of the right to privacy encompasses (section 3.2)
- the restrictions that may be imposed to the right to privacy (section 3.3)
- the broad construction of 'private life' under the ECHR, including in a public context (section 3.2.2)
- the role of encryption as an element ensuring the confidentiality of communications (section 3.2.4)
- how the ECtHR addresses the risks ensuing from mass surveillance regimes (section 3.4)
- the conditions upon which biometric recognition systems are compatible with human rights law and the AI Act (section 3.5)

(3.1) Relevant law

Article 17 ICCPR International Covenant on Civil and Political Rights

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

Article 10 ECHR European Convention on Human Rights – Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety

or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 7 EU Charter on Fundamental Rights – Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

(3.2) What is Privacy? The Elusive Protective Scope of the Right to Privacy

(3.2.1) Clarifying the scope of protection of Article 17 ICCPR

(3.2.1.1) Unlawful or arbitrary interference

UN Human Rights Committee, General Comment No 16, Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, UN Doc HRI/GEN/1/Rev.1 (1994)

1. Article 17 provides for the right of every person to be protected against arbitrary or unlawful interference with his privacy, family, home or correspondence as well as against unlawful attacks on his honour and reputation. In the view of the Committee this right is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons. The obligations imposed by this article require the State to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right.

[...]

3. The term "unlawful" means that no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant.

4. The expression "arbitrary interreference" is also relevant to the protection of the of the right provided for in Article 17. In the Committee's view the expression "arbitrary interreference" can also extend to interference provided for under the law. The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances.

[...]

8. Even with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorized interference must be made only by the authority designated under the law, and on a case-by-case basis [...]

(3.2.1.2) Protected categories



An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://opentextbooks.rug.nl/dataprotectionanddigitalhumanrights/?p=36#h5p-12

(3.2.2) The notion of 'private life' under the ECHR

The ECtHR adopt a broad conceptualisation of the notion of 'private life' in its case law.

(3.2.2.1) The broad notion of 'private life'

ECtHR, S. and Marper v UK, App no 30562/04 and 30566/04, 4 December 2008 (Grand Chamber)

> 66. The Court notes that the concept of "private life" is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person [...]. It can therefore embrace multiple aspects of the person's physical and social identity [...]. Elements such as, for example, gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by Article 8 [...]. Beyond a person's name, his or her private and family life may include other means of personal identification and of linking to a family [...]. Information about the person's health is an important element of private life [...]. The Court furthermore considers that an individual's ethnic identity must be regarded as another such element [...]. The concept of private life moreover includes elements relating to a person's right to their image [...]

(3.2.2.2) The social aspect of 'private life'

Private life is a notion that is **primarily intended** to ensure the development, without outside interference, of the personality of each individual. In this sense, private life is primarily designed to protect the individual in their private sphere/space from the State interfering.

However, the ECtHR adds a social aspect to protecting private life, including **the right for an individual to establish and develop relationships with others and with the outside world**.

ECtHR, Von Hannover v Germany (no 2), Applications nos 40660/08 and 60641/08, 7 February 2012 (Grand Chamber)

> 95. The [...] concept of private life extends to aspects relating to personal identity, such as a person's name, photo, or physical and moral integrity; the guarantee afforded by Article 8 of the Convention is primarily intended to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings. There is thus a zone of interaction of a person with others, even in a public context, which may fall within the scope of private life.

The Court, in the Von Hannover case, stresses that Article 8 also ensures the development, without outside interference, of the personality of each individual in his relations with other human beings. In other words, the Court acknowledges that individuals develop their personality also when approaching others in order to establish and develop relationships with them and with the outside world. One's private life is protected in this social and public context too. The Court uses various terms to capture this, such as the right to lead a "private social life" or 'a zone of interaction' of a person with others.

(3.2.2.3) When do private life considerations arise in a public context?

Having clarified that private life includes the right for an individual to establish and develop relationships with others and with the outside world, the question now is how we ascertain whether an interference with private life exists when we are in public.

The main criterion that the Court employs to assess whether there is an interference with private life in public is the **creation of a systematic or permanent record of personal data.**

Examples of creating permanent records: photographs, voice samples, fingerprints

Examples of creating systematic records: compiling data/datasets (in a manner or degree beyond that normally foreseeable)



An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://opentextbooks.rug.nl/dataprotectionanddigitalhumanrights/?p=36#h5p-13



An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://opentextbooks.rug.nl/dataprotectionanddigitalhumanrights/?p=36#h5p-14

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://opentextbooks.rug.nl/dataprotectionanddigitalhumanrights/?p=36#h5p-15

(3.2.2.3.1) ECtHR, Glukhin v Russia, App no 11519/20, 4 July 2023

64. The [...] concept of "private life" is a broad term not susceptible to exhaustive definition. It can embrace multiple aspects of the person's physical and social identity.It is not limited to an "inner circle" in which the individual may live his or her own personal life without outside interference, but also encompasses the right to lead a "private social life", that is, the possibility of establishing and developing relationships with others and the outside world. It does not exclude activities taking place in a public context. There is thus a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life".

[...]

66. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor in this assessment. As to the monitoring of an individual's actions using photographic or video devices, the Convention institutions have taken the view that the monitoring of the actions and movements of an individual in a public place using a camera which did not record the visual data does not constitute in itself a form of interference with private life. Private-life considerations may arise, however, once any systematic or permanent record of such personal data comes into existence, particularly pictures of an identified person. A person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers. The right of each person to the protection of his or her image is thus one of the essential components of personal development and presupposes the right to control the use of that image. While in most cases the right to control such use involves the possibility for an individual to refuse publication of his or her image, it also covers the individual's right to object to the recording, conservation and reproduction of the image by another person [...]

67. The Court has previously found that the collection and storing of data by the authorities on particular individuals constituted an interference with those persons' private lives, even if that data concerned exclusively the person's public activities [...], such as participation in anti-government demonstrations; [...] recording by CCTV cameras in a public place and the subsequent disclosure of the video-footage to the media; [...] and video surveillance of amphitheatres at a public university [...].

(3.2.2.3.2) Protection of 'private life' extends to processing or publishing publicly accessible taxation data in a manner/degree beyond normally foreseeable

Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, App no 931/13, 27 June 2017 (Grand Chamber)

> 134. The fact that information is already in the public domain will not necessarily remove the protection of Article 8 of the Convention. [...]
>
> [...]
>
> 136. [...] where there has been compilation of data on a particular individual, processing or use of personal data or publication of the material concerned in a manner or degree beyond that normally foreseeable, private life considerations arise [...]

(3.2.2.4) Exercise: Privacy as secrecy or privacy as protecting trust and confidentiality?

ECtHR, Rotaru v Romania, App no 28341/95, 4 May 2000 (Grand Chamber)

> 43. [...] public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past.
>
> 44. [...] [This information included] various pieces of information about the applicant's life, in particular his studies, his political activities and his criminal record, some of which had been gathered more than fifty years earlier. [...]

Partly dissenting opinion of Judge Bonello, in Rotaru v Romania

> 1. [...] I cannot endorse the applicability of Article 8.
> 2. Article 8 protects the individual's private life. At the core of that protection lies the right of every person to have the more intimate segments of his being excluded from public inquisitiveness and scrutiny. There are reserved zones in our person and in our spirit which the Convention requires should remain locked. It is illegitimate to probe for, store, classify or divulge data which refer to those innermost spheres of activity, orientation or conviction, sheltered behind the walls of confidentiality.
> 3. On the other hand, activities which are, by their very nature, public and which are actually nourished by publicity, are well outside the protection of Article 8.

Concurring opinion of Judge Yudkivska, joined by judge Bošnjak, in ECtHR, Benedik v. Slovenia, App no 62357/14, 24 April 2018

It is argued that in order to protect privacy in the modern era we must reconsider the outdated understanding of it as mere secrecy, and move toward legal protection of trust and confidentiality and of the right to control how information is disseminated and used. As judges we are entrusted with the task of rethinking the privacy paradigm in cases such as the present one.

Questions:

- How do you assess Judge Bonello's view that private life protects only what is 'sheltered behind the walls of confidentiality' and not in public?
- In contrast, Judge Yudkivska speaks of reconsidering the outdated understanding of privacy as mere secrecy and that we should move instead towards a new paradigm of protecting trust and confidentiality. What do you think she means?

(3.2.3) The relationship between privacy and data protection

ECtHR, Glukhin v Russia, App no 11519/20, 4 July 2023

75. The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article.

[...]

77. In the context of the collection and processing of personal data, it is therefore essential to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data, and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.

(3.2.4) Confidentiality of communications and encryption

According to the ECtHR, confidentiality of communications is an essential element of the right to respect for private life and correspondence, as enshrined in Article 8 ECHR.

(3.2.4.1) Encryption as a technical tool to protect the confidentiality of communications

UN Human Rights Council Res 47/16, The promotion, protection and enjoyment of human rights on the Internet, UN Doc A/HRC/RES/47/16, 7 July 2021

Emphasizing that, in the digital age, technical solutions to secure and protect the confidentiality of digital

communications, including measures for encryption and anonymity, are important to ensure the enjoyment of all human rights offline and online

(3.2.4.2) A statutory obligation to decrypt end-to-end encrypted communications weakens the encryption mechanism for all users and it is a disproportionate restriction

ECtHR, Podchasov v Russia, App no 33696/19, 13 February 2024

- The applicant was a user of Telegram, a messaging application which is used free of charge by millions of people in Russia and worldwide.
- This was the first opportunity for the ECtHR to decide on the statutory requirement for Internet providers to give state authorities information necessary to decrypt electronic messages.
- The judgment is well-informed and well-articulated on legal and technical developments in this area.

7. On 12 July 2017 the Federal Security Service ("the FSB") required Telegram Messenger LLP to disclose technical information which would facilitate "the decryption of communications [...] in respect of Telegram users who were suspected of terrorism-related activities". [...]

8. Telegram Messenger LLP refused to comply with the disclosure order, arguing that it was technically impossible to execute it without creating a backdoor that would weaken the encryption mechanism for all users. [...] The company was fined by the Meshchanskiy District Court of Moscow [...]. Subsequently, [...] the Taganskiy District Court of Moscow ordered the blocking of the Telegram application in Russia. Both judgments were upheld on appeal.

[....]

65. [...] the Court reiterates that confidentiality of communications is an essential element of the right to respect for private life and correspondence, as enshrined in Article 8. Users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, although such a guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others [...]

[...]

76. As regards the requirement to submit to the security services information necessary to decrypt electronic communications if they are encrypted, the Court observes that international bodies have argued that encryption provides strong technical safeguards against unlawful access to the content of communications and has therefore been widely used as a means of protecting the right to respect for private life and for the privacy of correspondence online. In the digital age, technical solutions for securing and protecting the privacy of electronic communications, including measures for encryption, contribute to ensuring the enjoyment of other fundamental rights, such as freedom of expression [...]. Encryption, moreover, appears to help citizens and businesses to defend themselves against abuses of information technologies, such as hacking, identity and personal data theft, fraud and the improper disclosure of confidential information. This should be given due consideration when assessing measures which may weaken encryption.

77. [...] It appears that in order to enable decryption of communications protected by end-to-end encryption, such as communications through Telegram's "secret chats", it would be necessary to weaken encryption for all users. These measures allegedly cannot be limited to specific individuals and would affect everyone indiscriminately, including individuals who pose no threat to a legitimate government interest. Weakening encryption by creating backdoors would apparently make it technically possible to perform routine, general and

indiscriminate surveillance of personal electronic communications. Backdoors may also be exploited by criminal networks and would seriously compromise the security of all users' electronic communications. [...]

78. The Court accepts that encryption can also be used by criminals, which may complicate criminal investigations [...] However, it takes note in this connection of the calls for alternative "solutions to decryption without weakening the protective mechanisms, both in legislation and through continuous technical evolution" [...]

79. [...] In the present case the ICO's statutory obligation to decrypt end-to-end encrypted communications risks amounting to a requirement that providers of such services weaken the encryption mechanism for all users; it is accordingly not proportionate to the legitimate aims pursued.

(3.2.5) Evolution of technologies and the changing threshold for the existence of an interference with the right to privacy

ECtHR, S. and Marper v UK, App no 30562/04 and 30566/04, 4 December 2008 (Grand Chamber)

58. The applicants complained under Article 8 of the Convention about the retention of their fingerprints, cellular samples and DNA profiles pursuant to section 64(1A) of the Police and Criminal Evidence Act 1984.

[...]

67. The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 [...]. The subsequent use of the stored information has no bearing on that finding [...]. However, in determining whether the personal information retained by the authorities involves any of [...] private-life aspects [...], the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained [...]

Cellular samples and DNA profiles

[...]

71. The Court maintains its view that an individual's concern about the possible future use of private information retained by the authorities is legitimate and relevant to a determination of the issue of whether there has been an interference. Indeed, bearing in mind the rapid pace of developments in the field of genetics and information technology, the Court cannot discount the possibility that in the future the private-life interests bound up with genetic information may be adversely affected in novel ways or in a manner which cannot be anticipated with precision today. [...]

72. Legitimate concerns about the conceivable use of cellular material in the future are not, however, the only element to be taken into account in the determination of the present issue. In addition to the highly personal nature of cellular samples, the Court notes that they contain much sensitive information about an individual, including information about his or her health. Moreover, samples contain a unique genetic code of great relevance to both the individual and his relatives.

[...]

75. [As regards DNA profiles] the Court observes [...] that the profiles contain substantial amounts of unique personal data. While the information contained in the profiles may be considered objective and irrefutable [...], their processing through automated means allows the authorities to go well beyond neutral identification. [...] In the Court's view, the DNA profiles' capacity to provide a means of identifying genetic relationships between individuals [...] is in itself sufficient to conclude that their retention interferes with the right to the private life of the individuals concerned. The frequency of familial searches, the safeguards attached thereto and the likelihood

of detriment in a particular case are immaterial in this respect [...] This conclusion is similarly not affected by the fact that, since the information is in coded form, it is intelligible only with the use of computer technology and capable of being interpreted only by a limited number of persons.

See also discussion below **(3.4.3)** on the evolving technology of metadata and its legal treatment

(3.3) Restricting the Right to Privacy

A restriction to the right to privacy may be imposed as long as this restriction

a) is provided by law

b) serves one of the legitimate purposes exhaustively enumerated in the respective provision; and

c) and is necessary in a democratic society.

- **Read**: Article 8(2) ECHR (see 3.1)

(3.3.1) Legislator's obligation to provide a framework for reconciling the various claims which compete for protection even in the sphere of the relations of individuals

ECtHR, K.U. v Finland, App no 2872/02, 2 December 2008

40. [...] the applicant, a minor of 12 years at the time, was the subject of an advertisement of a sexual nature on an Internet dating site. The identity of the person who had placed the advertisement could not, however, be obtained from the Internet service provider due to the legislation in place at the time.

[...]

42. The Court reiterates that, although the object of Article 8 is essentially to protect the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life [...]

43. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves. [...]

44. The limits of the national authorities' margin of appreciation are nonetheless circumscribed by the Convention provisions. In interpreting them, since the Convention is first and foremost a system for the

protection of human rights, the Court must have regard to the changing conditions within Contracting States and respond, for example, to any evolving convergence as to the standards to be achieved.

[...]

46. [...] For the Court, States have a positive obligation inherent in Article 8 of the Convention to criminalise offences against the person, including attempted offences, and to reinforce the deterrent effect of criminalisation by applying criminal-law provisions in practice through effective investigation and prosecution [...]. Where the physical and moral welfare of a child is threatened, such injunction assumes even greater importance. The Court notes in this connection that sexual abuse is unquestionably an abhorrent type of wrongdoing, with debilitating effects on its victims. Children and other vulnerable individuals are entitled to State protection, in the form of effective deterrence, from such grave types of interference with essential aspects of their private lives

[...]

49. The Court considers that practical and effective protection of the applicant required that effective steps be taken to identify and prosecute the perpetrator, that is, the person who placed the advertisement. In the instant case, such protection was not afforded. An effective investigation could never be launched because of an overriding requirement of confidentiality. Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others. Without prejudice to the question whether the conduct of the person who placed the offending advertisement on the Internet can attract the protection of Articles 8 and 10, having regard to its reprehensible nature, it is nonetheless the task of the legislator to provide the framework for reconciling the various claims which compete for protection in this context. Such framework was not, however, in place at the material time [...]

50. The Court finds that there has been a violation of Article 8 of the Convention in the present case.

(3.4) Mass Surveillance

(3.4.1) Adjusting the victim requirement in cases of secret, mass surveillance

ECtHR, Roman Zakharov v Russia, App no 47143/06, 4 December 2015 (Grand Chamber)

The applicant alleged that the system of secret interception of mobile-telephone communications in Russia violated his right to respect for his private life and correspondence, and that he did not have any effective remedy in that respect. However, the applicant was not in position to prove that he has been a victim (directly affected) and thus that an interference had taken place.

The Court held that the victim requirement had to be adjusted in cases of secret, mass surveillance. The Court instead examines:

- the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it; and
- whether the domestic system affords an effective remedy to the person who suspects that (s)he was

subjected to secret surveillance.

163. The Court observes that the applicant in the present case claims that there has been an interference with his rights as a result of the mere existence of legislation permitting covert interception of mobile-telephone communications and a risk of being subjected to interception measures, rather than as a result of any specific interception measures applied to him.

[...]

164. The Court has consistently held in its case-law that the Convention does not provide for the institution of an actio popularis and that its task is not normally to review the relevant law and practice in abstracto, but to determine whether the manner in which they were applied to, or affected, the applicant gave rise to a violation of the Convention [...]. Accordingly, in order to be able to lodge an application in accordance with Article 34, an individual must be able to show that he was "directly affected" by the measure complained of. This is indispensable for putting the protection mechanism of the Convention into motion, although this criterion is not to be applied in a rigid, mechanical and inflexible way throughout the proceedings [...]

[...]

168. In other cases the Court reiterated [...] that the mere existence of laws and practices which permitted and established a system for effecting secret surveillance of communications entailed a threat of surveillance for all those to whom the legislation might be applied. This threat necessarily affected freedom of communication between users of the telecommunications services and thereby amounted in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them [...]

[...]

171. [...] Accordingly, the Court accepts that an applicant can claim to be the victim of a violation occasioned by the mere existence of secret surveillance measures, or legislation permitting secret surveillance measures, if the following conditions are satisfied. Firstly, the Court will take into account the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his communications intercepted. Secondly, the Court will take into account the availability of remedies at the national level and will adjust the degree of scrutiny depending on the effectiveness of such remedies. [...] Where the domestic system does not afford an effective remedy to the person who suspects that he was subjected to secret surveillance, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified [...]. In such circumstances the threat of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right guaranteed by Article 8. There is therefore a greater need for scrutiny by the Court, and an exception to the rule denying individuals the right to challenge a law in abstracto is justified. In such cases the individual does not need to demonstrate the existence of any risk that secret surveillance measures were applied to him. By contrast, if the national system provides for effective remedies, a widespread suspicion of abuse is more difficult to justify. In such cases, the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures only if he is able to show that, due to his personal situation, he is potentially at risk of being subjected to such measures.

[...]

(3.4.2) Assessing mass surveillance regimes against human rights safeguards

In 2013, Edward Snowden – a former (NSA) intelligence contractor and whistleblower – leaked classified documents revealing the existence of global surveillance programmes run by the National Security Agency in the USA and the General Communications Headquarters in the UK. These programmes enabled access to global internet traffic, calling records, and huge volumes of other digital communications content. Since then, concerns regarding mass surveillance have been amplified.

In her 2014 Report on The right to privacy in the digital age, the UN High Commissioner for Human Rights stressed that covert governmental mass surveillance practices were 'emerging as a dangerous habit rather than an exceptional measure'. Today, governmental mass surveillance practices and data retention regimes – either overt or covert – are well-established and mainstream vindicating the point that they are not an exceptional measure but a dangerous habit

(3.4.2.1) UN General Assembly, Res 68/167, The Right to Privacy in the Digital Age, UN Doc A/RES/68/167, 18 December 2013

> 4. Calls upon all States:
>
> (c) to review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law

(3.4.2.2) ECtHR, Big Brother Watch and Others v United Kingdom, App nos 58170/13, 62322/14 and 24960/15, 25 May 2021 (Grand Chamber)

The case concerned the bulk interception regime operated in the UK, including the programmes of surveillance and intelligence sharing between the UK and the USA. The applicants brought claims regarding Articles 8, 10, 6, and 14 in conjunction with Articles 8 and 10. The complaints concerned **3 different surveillance regimes**:

1. the bulk interception of communications;
2. the receipt of intercept material from foreign governments and intelligence agencies;
3. the obtaining of communications data from communication service providers.

A notable point that should be made is that the Court accepted that Contracting States' bulk interception regimes are '**a valuable technological capacity** to identify new threats in the digital domain' (para 323). The framing of a bulk interception regime as a valuable technological capacity normalises mass surveillance. Moreover, ECtHR assesses compliance by reference to the existence of safeguards against arbitrariness and abuse, on the basis of limited information about the manner in which those regimes operate.

The Court's assessment

Preliminary remarks

322. The present complaint concerns the bulk interception of cross-border communications by the intelligence services. While it is not the first time the Court has considered this kind of surveillance [...], in the course of the proceedings it has become apparent that the assessment of any such regime faces specific difficulties. In the current, increasingly digital, age the vast majority of communications take digital form and are transported across global telecommunications networks using a combination of the quickest and cheapest paths without any meaningful reference to national borders. Surveillance which is not targeted directly at individuals therefore has the capacity to have a very wide reach indeed, both inside and outside the territory of the surveilling State. Safeguards are therefore pivotal and yet elusive. Unlike the targeted interception which has been the subject of much of the Court's case-law, and which is primarily used for the investigation of crime, bulk interception is also – perhaps even predominantly – used for foreign intelligence gathering and the identification of new threats from both known and unknown actors. When operating in this realm, Contracting States have a legitimate need for secrecy which means that little if any information about the operation of the scheme will be in the public domain, and such information as is available may be couched in terminology which is obscure and which may vary significantly from one State to the next.

The existence of an interference

[...]

325. [...] the Court considers that the stages of the bulk interception process which fall to be considered can be described as follows:

(a) the interception and initial retention of communications and related communications data (that is, the traffic data belonging to the intercepted communications);

(b) the application of specific selectors to the retained communications/related communications data;

(c) the examination of selected communications/related communications data by analysts; and

(d) the subsequent retention of data and use of the "final product", including the sharing of data with third parties.

[...]

330. [...] Article 8 applies at each of the above stages. While the initial interception followed by the immediate discarding of parts of the communications does not constitute a particularly significant interference, the degree of interference with individuals' Article 8 rights will increase as the bulk interception process progresses. In this regard, the Court has clearly stated that even the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 [...], and that the need for safeguards will be all the greater where the protection of personal data undergoing automatic processing is concerned [...]

Whether the interference was justified

- **General principles relating to secret measures of surveillance, including the interception of communications**

[...]

333. The meaning of "foreseeability" in the context of secret surveillance is not the same as in many other fields. In the special context of secret measures of surveillance, such as the interception of communications, "foreseeability" cannot mean that individuals should be able to foresee when the authorities are likely to resort to such measures so that they can adapt their conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed

rules on secret surveillance measures, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures [...]. Moreover, the law must indicate the scope of any discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.

[...]

335. [...] In its case-law on the interception of communications in criminal investigations, the Court has developed the following minimum requirements that should be set out in law in order to avoid abuses of power: **(i)** the nature of offences which may give rise to an interception order; **(ii)** a definition of the categories of people liable to have their communications intercepted; **(iii)** a limit on the duration of interception; **(iv)** the procedure to be followed for examining, using and storing the data obtained; **(v)** the precautions to be taken when communicating the data to other parties; and **(vi)** the circumstances in which intercepted data may or must be erased or destroyed [...]

336. Review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights. In a field where abuse in individual cases is potentially so easy and could have such harmful consequences for democratic society as a whole, the Court has held that it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure [...]

[...]

338. As to the question whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim, the Court has recognised that the national authorities enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security [...]

339. However, this margin is subject to European supervision embracing both legislation and decisions applying it. In view of the risk that a system of secret surveillance set up to protect national security (and other essential national interests) may undermine or even destroy the proper functioning of democratic processes under the cloak of defending them, the Court must be satisfied that there are adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law. [...]

- **The approach to be followed in bulk interception cases**

348. It is clear that the first two of the six "minimum safeguards" [see paragraph 335] which the Court, in the context of targeted interception, has found should be defined clearly in domestic law in order to avoid abuses of power [...], are not readily applicable to a bulk interception regime. Similarly, the requirement of "reasonable suspicion", which can be found in the Court's case-law on targeted interception in the context of criminal investigations is less germane in the bulk interception context, the purpose of which is in principle preventive, rather than for the investigation of a specific target and/or an identifiable criminal offence. Nevertheless, the

Court considers it imperative that when a State is operating such a regime, domestic law should contain detailed rules on when the authorities may resort to such measures. In particular, domestic law should set out with sufficient clarity the grounds upon which bulk interception might be authorised and the circumstances in which an individual's communications might be intercepted. The remaining four minimum safeguards defined by the Court in its previous judgments — that is, that domestic law should set out a limit on the duration of interception, the procedure to be followed for examining, using and storing the data obtained, the precautions to be taken when communicating the data to other parties, and the circumstances in which intercepted data may or must be erased or destroyed — are equally relevant to bulk interception.

349. [...] In the context of bulk interception the importance of supervision and review will be amplified, because of the inherent risk of abuse and because the legitimate need for secrecy will inevitably mean that, for reasons of national security, States will often not be at liberty to disclose information concerning the operation of the impugned regime.

350. Therefore, in order to minimise the risk of the bulk interception power being abused, the Court considers that the process must be subject to "end-to-end safeguards", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent ex post facto review. [...]

351. Turning first to authorisation, the Grand Chamber agrees with the Chamber that while judicial authorisation is an "important safeguard against arbitrariness" it is not a "necessary requirement" [...]. Nevertheless, bulk interception should be authorised by an independent body; that is, a body which is independent of the executive.

352. Furthermore, in order to provide an effective safeguard against abuse, the independent authorising body should be informed of both the purpose of the interception and the bearers or communication routes likely to be intercepted. This would enable the independent authorising body to assess the necessity and proportionality of the bulk interception operation and also to assess whether the selection of bearers is necessary and proportionate to the purposes for which the interception is being conducted.

353. The use of selectors – and strong selectors in particular – is one of the most important steps in the bulk interception process, as this is the point at which the communications of a particular individual may be targeted by the intelligence services. However, while some systems allow for the prior authorisation of categories of selectors [...], the Court notes that the Governments of both the United Kingdom and the Netherlands have submitted that any requirement to explain or substantiate selectors or search criteria in the authorisation would seriously restrict the effectiveness of bulk interception [...]

354. Taking into account the characteristics of bulk interception [...], the large number of selectors employed and the inherent need for flexibility in the choice of selectors, which in practice may be expressed as technical combinations of numbers or letters, the Court would accept that the inclusion of all selectors in the authorisation may not be feasible in practice. Nevertheless, given that the choice of selectors and query terms determines which communications will be eligible for examination by an analyst, the authorisation should at the very least identify the types or categories of selectors to be used.

355. Moreover, enhanced safeguards should be in place when strong selectors linked to identifiable individuals are employed by the intelligence services. The use of every such selector must be justified – with regard to the principles of necessity and proportionality – by the intelligence services and that justification should be scrupulously recorded and be subject to a process of prior internal authorisation providing for separate and objective verification of whether the justification conforms to the aforementioned principles.

356. Each stage of the bulk interception process – including the initial authorisation and any subsequent renewals, the selection of bearers, the choice and application of selectors and query terms, and the use, storage, onward transmission and deletion of the intercept material – should also be subject to supervision by an independent authority and that supervision should be sufficiently robust to keep the "interference" to what is "necessary in a democratic society" [...]

357. Finally, an effective remedy should be available to anyone who suspects that his or her communications have been intercepted by the intelligence services, either to challenge the lawfulness of the suspected interception or the Convention compliance of the interception regime. In the targeted interception context, the Court has repeatedly found the subsequent notification of surveillance measures to be a relevant factor in assessing the effectiveness of remedies before the courts and hence the existence of effective safeguards against the abuse of surveillance powers. However, it has acknowledged that notification is not necessary if the system of domestic remedies permits any person who suspects that his or her communications are being or have been intercepted to apply to the courts; in other words, where the courts' jurisdiction does not depend on notification to the interception subject that there has been an interception of his or her communications [...]

[...]

361. In assessing whether the respondent State acted within its margin of appreciation [...] the Court will examine whether the domestic legal framework clearly defined:

1. the grounds on which bulk interception may be authorised;
2. the circumstances in which an individual's communications may be intercepted;
3. the procedure to be followed for granting authorisation;
4. the procedures to be followed for selecting, examining and using intercept material;
5. the precautions to be taken when communicating the material to other parties;
6. the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;
7. the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;
8. the procedures for independent ex post facto review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.

(3.4.3) Communications-related data (metadata)

What is metadata? Watch the video Metadata Explained, by Privacy International



One or more interactive elements has been excluded from this version of the text. You can view them online here: https://opentextbooks.rug.nl/dataprotectionanddigitalhumanrights/?p=36#oembed-1

(3.4.3.1) Examples of metadata

Metadata is all non-content related data.

Phone calls

- data to trace and identify the source of a communication and its destination
- date, time, duration and type of a communication
- users' communication equipment
- location of mobile communication equipment
- name and address of a subscriber
- the calling telephone number and the number called

Telecommunication services

- IP address for Internet services
- websites visited
- connections to websites
- email addresses
- mapping of social networks
- location tracking
- mapping of communication patterns
- insights into who they have interacted with

(3.4.3.2) The evolving technology of metadata and the human rights protection

- **metadata as an evolving technology and seriousness of interference with privacy**

Metadata and the technologies related to it are evolving through time. The technological capacity to create metadata, storing capacity as well as processing power enable the creation and analysis of a large amount of data/personal information. Metadata can also be processed and analysed easier that content because of its formatting. Due to the radical increase of digital communications and these technological advances over the past two decades, communications-related data, taken as a whole, now reveal an intimate portrait of a person (e.g., private live, behaviour, relationships, preferences, identity). The interference with the right to privacy can be particularly serious; many times, equally serious (if not more serious) compared to the content of communications.

- **response by human rights law**

The evolving seriousness of the interferences posed by the collection, storing and analysis of metadata dictates that the human rights law standard of assessing compliance with the right to privacy is expected to adjust. The material below gives a snapshot of this evolution from a human rights law point of view. The UN High Commissioner for Human Rights in the 2014 report contests the arguments regularly made by many states at that time that the interception/collection of metadata, as opposed to the content of the communication, does not on its own constitute an interference with privacy. In the same year (2014), the CJEU, in the Digital Rights case, emphasises that interception/collection of metadata, can qualify as a serious interference with privacy. The ECtHR reaches the same conclusion in its 2021 judgment in the Big Brother case. The ECtHR articulates much more clearly the seriousness of the interference (in the recent (2024) judgments). Interestingly, the ECtHR accepts that safeguards applicable to metadata do not have to be identical in every respect to those governing the content of communications.

(3.4.3.2.1) Report of the Office of the UN High Commissioner for Human Rights, The right to privacy in the digital age, UN Doc A/HRC/27/37, 30 June 2014

> 19. [...] It has been suggested that the interception or collection of data about a communication, as opposed to the content of the communication, does not on its own constitute an interference with privacy. From the perspective of the right to privacy, this distinction is not persuasive. The aggregation of information commonly referred to as "metadata" may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication.

(3.4.3.2.2) Court of Justice of the European Union, Digital Rights Ireland and Seitinger and Others, C-293/12 and C-594/12, 8 April 2014 (Grand Chamber)

> 26. [...] [The data which providers of publicly available electronic communications services or of public communications networks must retain, pursuant to Articles 3 and 5 of Directive 2006/24] data make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.
>
> 27. Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.
>
> [...]
>
> 29. The retention of data for the purpose of possible access to them by the competent national authorities, as provided for by Directive 2006/24, directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 of the Charter. Furthermore, such a retention of data also falls under Article 8 of the

Charter because it constitutes the processing of personal data within the meaning of that article and, therefore, necessarily has to satisfy the data protection requirements arising from that article [...]

[...]

37. [...] The interference caused by Directive 2006/24 with the fundamental rights laid down in Articles 7 and 8 of the Charter is [...] wide-ranging, and it must be considered to be particularly serious. Furthermore, [...] the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.

(3.4.3.2.3) ECtHR, Škoberne v Slovenia, App no 19920/20, 15 February 2024

133. [...] telecommunications data [...], when linked to a subscriber or a user, can reveal intimate pictures of his or her life through the mapping of social networks, location tracking, the mapping of communication patterns, and insight into who they have interacted with [...]. In the Court's view, the systemic surveillance entailed by the mandatory retention of telecommunications data presents an impediment to the enjoyment of the privacy rights of all users of telecommunication services. The existence of large collections of telecommunications data and the ongoing retention of such data could understandably generate a sense of vulnerability and exposure and could prejudice persons' ability to enjoy privacy and the confidentiality of correspondence, to develop relations with others and to exercise other fundamental rights. In this regard the Court also refers to the observations made by the CJEU in Digital Rights Ireland and Others [...]

134. [...] the Court finds that the interference constituted by the data retention under consideration was of a serious nature. It must now determine whether the means provided under the impugned legislation for the achievement of the legitimate aims [...] complied with the requirements of the principle of the rule of law and remained in all respects within the bounds of what was necessary in a democratic society.

(3.4.3.2.4) ECtHR, Pietrzak and Bychawska-Siniarska and Others v Poland, App nos 72038/17, 25237/18, 28 May 2024 (in French) (unofficial translation)

249. [...] The acquisition of associated communications data in the context of bulk interception can be just as intrusive as the acquisition of the content of communications, and therefore the interception, retention, and searches of such data must be analyzed in light of the same safeguards as those applicable to the content of communications, without it being necessary for the legal provisions governing the processing of such data to be identical in every respect to those governing the processing of the content of communications [...]

(3.4.3.2.5) Not all metadata is the same: interference, while not trivial, rather limited

ECtHR, Breyer v Germany, App no 50001/12, 20 January 2020

The case concerned the statutory obligation imposed on service providers to store personal data of users of prepaid mobile telephone SIM cards and make them available to authorities upon request.

90. The Court acknowledges that pre-registration of mobile-telephone subscribers strongly simplifies and

accelerates investigation by law-enforcement agencies and can thereby contribute to effective law enforcement and prevention of disorder or crime. [...] The Court reiterates that in a national security context, national authorities enjoy a certain margin of appreciation when choosing the means for achieving a legitimate aim and notes that according to the comparative-law report, there is no consensus between the member States as regards the retention of subscriber information of prepaid SIM card customers [...]

91. The question, however, remains whether the interference was proportionate and struck a fair balance between the competing public and private interests.

92. [...] The Court has to establish the level of interference with the applicants' right to private life. [...] Only a limited data set was stored. These data did not include any highly personal information or allow the creation of personality profiles or the tracking of the movements of mobile-telephone subscribers. Moreover, no data concerning individual communication events were stored. The level of interference therefore has to be clearly distinguished from the Court's previous cases that concerned, for example, "metering" [...], geolocation [...] or the storage of health or other sensitive data [...] Moreover, the case has to be distinguished from cases in which the registration in a particular database led to frequent checks or further collection of private information [...].

[...]

95. In sum, the Court concludes that the interference was, while not trivial, of a rather limited nature.

(3.4.4) Exercise: In addition to the right to privacy, what other rights may also be affected by mass surveillance practices?

Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, UN Doc A/HRC/27/37, 30 June 2014

> 14. [...] other rights also may be affected by mass surveillance, the interception of digital communications and the collection of personal data. These include the rights to freedom of opinion and expression [...]; to freedom of peaceful assembly and association; and to family life – rights all linked closely with the right to privacy and, increasingly, exercised through digital media. Other rights, such as the right to health, may also be affected by digital surveillance practices, for example where an individual refrains from seeking or communicating sensitive health-related information for fear that his or her anonymity may be compromised. There are credible indications to suggest that digital technologies have been used to gather information that has then led to torture and other ill-treatment. Reports also indicate that metadata derived from electronic surveillance have been analysed to identify the location of targets for lethal drone strikes.
>
> [...]
>
> 20. [...] Even the mere possibility of communications [data] [...] being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and

association. The very existence of a mass surveillance programme thus creates an interference with privacy.

(3.5) Biometric/Facial Recognition and the Right to Privacy

(3.5.1) Explaining biometric recognition

- **What is biometric recognition?**

Biometric recognition technologies detect, capture, and transform physical characteristics or behavioural traits into machine-readable biometric data.

- physical characteristics include facial features (eye distance and size, nose length), fingerprints, iris, voice
- behavioural characteristics include keystroke, gait or voice recognition

- **What is facial recognition technology?**

Facial recognition technology (FRT) is a type of biometric recognition. It compares digital images of a person's face to a database of faces, either live or from images and videos.

- **What is live recognition technology?**

Live facial recognition (LFR) is a technology that uses AI to compare live camera footage of people's faces against a database, typically a watchlist of individuals of interest. This allows for real-time identification of people and can be used in various contexts.

(3.5.2) ECtHR, Glukhin v Russia, App no 11519/20, 4 July 2023

The case concerns the applicant's administrative conviction for his failure to notify the authorities of his intention to hold a solo demonstration using a "quickly (de)assembled object". During the investigation, the

police used live facial recognition technology to process the applicant's personal data. Glukhin v Russia is the first international judgment on facial recognition. The ECtHR:

- stressed that new technologies (live and automated facial recognition) are **highly intrusive**
- highlighted the **chilling effect** that the use of such technologies has on the effective exercise of human rights (e.g., freedom of expression or right to assembly)

Nonetheless, the ECtHR did not engage at all with the question of whether, in certain circumstances, facial/biometric recognition systems may be incompatible with the right to privacy.

> 68. In the present case, during routine monitoring of the internet the police discovered photographs and a video of the applicant holding a solo demonstration published on a public Telegram channel. They made screenshots of the Telegram channel, stored them and allegedly applied facial recognition technology to them to identify the applicant. Having identified the location on the video as one of the stations of the Moscow underground, the police also collected video-recordings from CCTV surveillance cameras installed at that station, as well as at two other stations through which the applicant had transited. They made screenshots of those video-recordings and stored them. They also allegedly used the live facial recognition CCTV cameras installed in the Moscow underground to locate and arrest the applicant several days later with the aim of charging him with an administrative offence. The screenshots of the Telegram channel and of the video-recordings from the CCTV surveillance cameras were subsequently used in evidence in the administrative-offence proceedings against the applicant [...]
>
> 72. [...] the Court accepts in the particular circumstances of the case that facial recognition technology was used [...].
>
> 73. The Court concludes that the processing of the applicant's personal data in the framework of the administrative-offence proceedings against him, including the use of facial recognition technology – firstly, to identify him from the photographs and the video published on Telegram and, secondly, to locate and arrest him later while he was travelling on the Moscow underground – amounted to an interference with his right to respect for his private life within the meaning of Article 8 § 1 of the Convention.
>
> [...]
>
> 75. The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article. The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police [...], and especially where the technology available is continually becoming more sophisticated [...]. The protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests [...]
>
> 76. Personal data revealing political opinions, such as information about participation in peaceful protests, fall within the special categories of sensitive data attracting a heightened level of protection [...]
>
> 77. In the context of the collection and processing of personal data, it is therefore essential to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality

of data, and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.

[...]

83. The Court has strong doubts that the domestic legal provisions meet the "quality of law" requirement. It notes, in particular, that the domestic law permits the processing of biometric personal data "in connection with the administration of justice" [...] This legal provision is widely formulated. [...] The domestic law does not contain any limitations on the nature of situations which may give rise to the use of facial recognition technology, the intended purposes, the categories of people who may be targeted, or the processing of sensitive personal data. Furthermore, the Government did not refer to any procedural safeguards accompanying the use of facial recognition technology in Russia, such as the authorisation procedures, the procedures to be followed for examining, using and storing the data obtained, any supervisory control mechanisms or the available remedies.

84. The Court will further proceed on the assumption that the contested measures pursued the legitimate aim of the prevention of crime.

[...]

86. In determining whether the processing of the applicant's personal data was "necessary in a democratic society", the Court will first assess the level of the actual interference with the right to respect for private life [...]. It notes that the police collected and stored the applicant's digital images and used them to extract and process the applicant's biometric personal data with the aid of facial recognition technology: first, to identify him from the photographs and the video published on Telegram and, secondly, to locate and arrest him while he was travelling on the Moscow underground. The Court considers these measures to be particularly intrusive, especially in so far as live facial recognition technology is concerned [...]. A high level of justification is therefore required in order for them to be considered "necessary in a democratic society", with the highest level of justification required for the use of live facial recognition technology. Moreover, the personal data processed contained information about the applicant's participation in a peaceful protest and therefore revealed his political opinion. They accordingly fell within the special categories of sensitive data attracting a heightened level of protection [...]

87. In the assessment of the "necessity in a democratic society" of the processing of personal data in the context of investigations, the nature and gravity of the offences in question is one of the elements to be taken into account [...]. The domestic law permits the processing of biometric personal data in connection with the investigation and prosecution of any offence, irrespective of its nature and gravity.

88. The Court observes that the applicant was prosecuted for a minor offence consisting of holding a solo demonstration without prior notification – an offence classified as administrative rather than criminal under the domestic law. He was never accused of committing any reprehensible acts during his demonstration, such as the obstruction of traffic, damage to property or acts of violence. It was never claimed that his actions presented any danger to public order or transport safety. The Court has already found that the administrative-offence proceedings against the applicant breached his right to freedom of expression [...]. It considers that the use of highly intrusive facial recognition technology to identify and arrest participants in peaceful protest actions could have a chilling effect in relation to the rights to freedom of expression and assembly.

89. In such circumstances, the use of facial recognition technology to identify the applicant from the photographs and the video published on Telegram – and a fortiori the use of live facial recognition technology to locate and arrest him while he was travelling on the Moscow underground – did not correspond to a "pressing social need".

90. In the light of all the above considerations, the Court concludes that the use of highly intrusive facial recognition technology in the context of the applicant's exercising his Convention right to freedom of expression

is incompatible with the ideals and values of a democratic society governed by the rule of law, which the Convention was designed to maintain and promote. The processing of the applicant's personal data using facial recognition technology in the framework of administrative-offence proceedings – firstly, to identify him from the photographs and the video published on Telegram and, secondly, to locate and arrest him while he was travelling on the Moscow underground – cannot be regarded as "necessary in a democratic society".

91. There has accordingly been a violation of Article 8 of the Convention.

See also R. (on the application of Edward Bridges) v Chief Constable of S. Wales Police [2020] EWCA Civ 1058 (Ed Bridges)

- the Court of Appeal found the South Wales Police's use of automated facial recognition technology breached the rights to privacy and equality

(3.5.3) Prohibition of the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement under the EU AI Act

(3.5.3.1) Article 5(1)(h) EU AI Act

The following AI practices shall be prohibited:

(h) the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, unless and in so far as such use is strictly necessary for one of the following objectives:

(i) the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons

(ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack

(iii) the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years

Point (h) of the first subparagraph is without prejudice to Article 9 of Regulation (EU) 2016/679 for the processing of biometric data for purposes other than law enforcement.

(3.5.3.2) Rationale underpinning the prohibition in Article 5(1)(h) EU AI Act

Commission Guidelines on prohibited artificial intelligence practices established by the EU AI Act, C(2025) 884 final, 4 February 2025

(293) Recital 32 AI Act acknowledges the intrusive nature of real-time RBI systems in publicly accessible

spaces for law enforcement purposes to the rights and freedoms of persons concerned, to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance, and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights. Technical inaccuracies of AI systems intended for the remote biometric identification of natural persons can lead to biased results and entail discriminatory effects.

Such possibly biased results and discriminatory effects are particularly relevant with regard to age, ethnicity, race, sex or disabilities. In addition, the immediacy of the impact and the limited opportunities for further checks or corrections in relation to the use of such systems operating in real-time carry heightened risks for the rights and freedoms of the persons concerned in the context of, or impacted by, law enforcement activities

(294) However, where the use of such systems is strictly necessary to achieve a substantial public interest and where the situations in which such use may occur are exhaustively listed and narrowly defined, that use outweighs the risks to fundamental rights (Recital 33 AI Act). To ensure that such systems are used in a 'responsible and proportionate manner', their use is subject to the safeguards and the specific obligations and requirements in Article 5(2)-(7) AI Act.

(3.5.3.3) Understanding the prohibition

Article 5(1)(h) AI Act prohibits:



An interactive H5P element has been excluded from this version of the text. You can view it online here:

https://opentextbooks.rug.nl/dataprotectionanddigitalhumanrights/?p=36#h5p-16

The prohibition in Article 5(1)(f) AI Act does **not** apply to the labelling or filtering of lawfully acquired datasets in the area of law enforcement.

(3.5.3.4) Exceptions to the prohibition

Article 5(1)(h)(i)-(iii) provides 3 exceptions to the general prohibition on the use of real-time RBI in publicly accessible spaces for law enforcement purposes:

a) the targeted search of victims of three specific serious crimes and missing persons

b) the prevention of imminent threats to life or physical safety or a genuine threat of terrorist attacks

c) the localisation and identification of suspects and offenders of certain serious crimes (as listed in Annex II to the AI Act)

These exceptions

- are prescribed exhaustively
- need to be strictly necessary
- must fulfill the conditions and safeguards set out in Article 5(2) to 5(7) AI Act
- have to be grounded in respective national legislation

Where a Member State authorises the use of real-time RBI systems in publicly accessible spaces for law enforcement purposes for any of these three objectives, the rules for high-risk AI systems apply to that use.

Further reading / resource

- DJ Solove, 'A Taxonomy of Privacy' (2006) 154 U. Pa. L. Rev. 477
- DJ Solove and NM Richards, 'Privacy's Other Path: Recovering the Law of Confidentiality' (2007) 96 Geo. L. J. 123
- A Rachovitsa & N Johann, 'The Use of AI in the Digital Welfare State and Lessons Learned from the SyRI Case' (2022) 22 Human Rights Law Review 1
- Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics' (2017) 30 Philosophy & Technology 478
- D Murray, 'Police Use of Retrospective Facial Recognition Technology: A Step Change in Surveillance Capability Necessitating an Evolution of the Human Rights Law Framework' (2023) Modern Law Review 1
- Have a look at the work of the UN Special Rapporteur on the right to privacy, including the annual thematic reports.
- On **children's rights in relation to the digital environment**, read the Committee on the Rights of the Child, General Comment No 25 (2021).
- For a **gender perspective on privacy and technology**, read this report by the UN Special Rapporteur on the right to privacy, UN Doc A/HRC/40/63, 27 February 2019
- On **data colonialism,** Nick Couldry and Ulises A. Mejias, 'Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject' (2019) 20 Television & New Media, 2019

4. RIGHT TO FREEDOM OF EXPRESSION & THOUGHT

Outline of this chapter

This chapter explains how the right to freedom of expression applies to the online environment as well as AI systems. More specifically, this chapter addresses:

- what the protective scope of the right to freedom of expression includes (section 4.1)
- the restrictions that may be imposed on the right of freedom of expression and what the requirements are for said restrictions to be lawful under human rights law (section 4.2)
- how the private governance of content regulation works and how human rights law is relevant (section 4.3)
- whether certain AI systems can be incompatible with the freedom of thought and individual autonomy (section 4.4)

(4.1) Protective Scope of the Right to Freedom of Expression

(4.1.1) Relevant law

Article 10 ECHR European Convention on Human Rights

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such

formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary

Article 19 ICCPR International Covenant on Civil and Political Rights

1. Everyone shall have the right to hold opinions without interference.

2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

(a) For respect of the rights or reputations of others

(b) For the protection of national security or of public order (ordre public), or of public health or morals.

(4.1.2) Clarifying the scope of protection of Article 19 ICCPR

(4.1.2.1) UN Human Rights Committee, General Comment No 34, Article 19: Freedoms of opinion and expression, UN Doc CCPR/C/GC/34, 12 September 2011

[...]

2. Freedom of opinion and freedom of expression are indispensable conditions for the full development of the person. They are essential for any society. They constitute the foundation stone for every free and democratic society. [...]

3. [...] The freedoms of opinion and expression form a basis for the full enjoyment of a wide range of other human rights. For instance, freedom of expression is integral to the enjoyment of the rights to freedom of assembly and association, and the exercise of the right to vote.

[...]

11. Paragraph 2 requires States parties to guarantee the right to freedom of expression, including the right to seek, receive and impart information and ideas of all kinds regardless of frontiers. This right includes the expression and receipt of communications of every form of idea and opinion capable of transmission to others, subject to the provisions in article 19, paragraph 3, and article 20. It includes political discourse, commentary on one's own and on public affairs, canvassing, discussion of human rights, journalism, cultural and artistic expression, teaching, and religious discourse. It may also include commercial advertising. The scope of paragraph 2 embraces even expression that may be regarded as deeply offensive, although such expression may be restricted in accordance with the provisions of article 19, paragraph 3 and article 20.

12. Paragraph 2 protects all forms of expression and the means of their dissemination. Such forms include spoken, written and sign language and such non-verbal expression as images and objects of art.23 Means of expression include books, newspapers, pamphlets, posters, banners, dress and legal submissions. They include all forms of audio-visual as well as electronic and internet-based modes of expression.

[...]

15. States parties should take account of the extent to which developments in information and communication technologies, such as internet and mobile based electronic information dissemination systems, have substantially changed communication practices around the world. There is now a global network for exchanging ideas and opinions that does not necessarily rely on the traditional mass media intermediaries. States parties should take all necessary steps to foster the independence of these new media and to ensure access of individuals thereto.

(4.1.3) Protection of Internet-based modes of expression

ECtHR, Times Newspapers Ltd (Nos. 1 and 2) v The United Kingdom, App nos. 3002/03 and 23676/03, 10 March 2009

27. The Court has consistently emphasised that Article 10 guarantees not only the right to impart information but also the right of the public to receive it [...]. In the light of [the Internet's] accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information in general.

(4.1.4) Internet access as a human right or as an enabler of exercising freedom of expression?

Community Court of Justice of the Economic Community of West African States (ECOWAS), Amnesty International & Ors v The Togolese Republic, 25 *June 2020*

38. Access to internet is not *stricto senso* a fundamental human right but since internet service provides a platform to enhance the exercise of freedom of expression, it then becomes a derivative right that it is a component to the exercise of the right to freedom of expression. It is a vehicle that provides a platform that will enhance the enjoyment of the right to freedom of expression. Right to internet access is closely linked to the right of freedom of speech which can be seen to encompass freedom of expression as well. Since access to internet is complementary to the enjoyment of the right to freedom of expression, it is necessary that access to internet and the right to freedom of expression be deemed to be an integral part of human right that requires protection by law and makes its violation actionable. In this regard, access to internet being a derivative right and at the same time component part of each other, should be jointly treated as an element of human right to which states are under obligation to provide protection for in accordance with the law just in the same way as the right to freedom of expression is protected.

(4.1.5) States' obligations and bridging divides

How do we think about the effective exercise of the right to freedom of expression "on the ground"? How different individuals are affected in being able to access the Internet and technological systems or being able to effectively use them?

(4.1.5.1) Global and gender divides

UN Human Rights Council, Res 47/16, The promotion, protection and enjoyment of human rights on the Internet, UN Doc A/HRC/RES/47/16, 7 July 2021

> 3. *Also condemns unequivocally* online attacks against women, including sexual and gender-based violence and abuse of women, in particular where women journalists, media workers, public officials or others engaging in public debate are targeted for their expression, and calls for gender-sensitive responses that take into account the particular forms of online discrimination
>
> [...]
>
> 8. *Calls upon* all States to bridge the digital divides, including the gender digital divide, and to enhance the use of information and communications technology, in order to promote the full enjoyment of human rights for all

(4.1.5.2) Participation of persons with disabilities

UN Human Rights Council, Res 38/7, The promotion, protection and enjoyment of human rights on the Internet, UN Doc A/HRC/RES/38/7, 17 July 2018

> 7. *Encourages* all States to take appropriate measures to promote, with the participation of persons with disabilities, the design, development, production and distribution of information and communications technology and systems, including assistive and adaptive technologies, that are accessible to persons with disabilities.

(4.2) Restrictions to the Right of Freedom of Expression

A restriction to freedom of expression may be imposed **as long as** said restriction

a) is provided by law

b) serves one of the legitimate purposes exhaustively enumerated in the respective provision and

c) is necessary in a democratic society.

- **Read**: Article 19(3) ICCPR and Article 10(2) ECHR

(4.2.1) Conditions to be met for the restrictions to be lawful

UN Human Rights Committee, General Comment No 34, Article 19: Freedoms of opinion and expression, UN Doc CCPR/C/GC/34, 12 September 2011

21. [...] when a State party imposes restrictions on the exercise of freedom of expression, these may not put in jeopardy the right itself. The Committee recalls that the relation between right and restriction and between norm and exception must not be reversed. [...]

22. Paragraph 3 lays down specific conditions and it is only subject to these conditions that restrictions may be imposed: the restrictions must be "provided by law"; they may only be imposed for one of the grounds set out in subparagraphs (a) and (b) of paragraph 3; and they must conform to the strict tests of necessity and proportionality. Restrictions are not allowed on grounds not specified in paragraph 3, even if such grounds would justify restrictions to other rights protected in the Covenant. Restrictions must be applied only for those purposes for which they were prescribed and must be directly related to the specific need on which they are predicated.

25. For the purposes of paragraph 3, a norm, to be characterized as a "law", must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public. [...]

27. It is for the State party to demonstrate the legal basis for any restrictions imposed on freedom of expression. [...]

28. The first of the legitimate grounds for restriction listed in paragraph 3 is that of respect for the rights or reputations of others. The term "rights" includes human rights as recognized in the Covenant and more generally in international human rights law. For example, it may be legitimate to restrict freedom of expression in order to protect the right to vote under article 25, as well as rights article under 17 [...] Such restrictions must be constructed with care: while it may be permissible to protect voters from forms of expression that constitute intimidation or coercion, such restrictions must not impede political debate, including, for example, calls for the boycotting of a non-compulsory vote. The term "others" relates to other persons individually or as members of a community. Thus, it may, for instance, refer to individual members of a community defined by its religious faith or ethnicity.

29. The second legitimate ground is that of protection of national security or of public order (ordre public), or of public health or morals.

30. Extreme care must be taken by States parties to ensure that treason laws and similar provisions relating to national security, whether described as official secrets or sedition laws or otherwise, are crafted and applied in a manner that conforms to the strict requirements of paragraph 3. [...]

31. On the basis of maintenance of public order (ordre public) it may, for instance, be permissible in certain circumstances to regulate speech-making in a particular public place. [...]

32. The Committee observed in general comment No. 22, that "the concept of morals derives from many social, philosophical and religious traditions; consequently, limitations... for the purpose of protecting morals must be based on principles not deriving exclusively from a single tradition". Any such limitations must be understood in the light of universality of human rights and the principle of non-discrimination.

33. Restrictions must be "necessary" for a legitimate purpose. The Committee observed in general comment No. 27 that "restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve their protective function; they must be proportionate to the interest to be protected [...]

35. When a State party invokes a legitimate ground for restriction of freedom of expression, it must

demonstrate in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat.

43. Any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3. [...]

(4.2.2) States' obligations when blocking and filtering content online

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Freedom of expression, states and the private sector in the digital age, UN Doc A/HRC/32/38, 11 May 2016

46. States often block and filter content with the assistance of the private sector. Internet service providers may block access to specific keywords, web pages or entire websites. On platforms that host content, the type of filtering technique depends on the nature of the platform and the content in question. Domain name registrars may refuse to register those that match a government blacklist; social media companies may remove postings or suspend accounts; search engines may take down search results that link to illegal content. The method of restriction required by Governments or employed by companies can raise both necessity and proportionality concerns, depending on the validity of the rationale cited for the removal and the risk of removal of legal or protected expression.

(4.2.3) Assessing whether the individual's conviction to paying a fine for sharing a link on social media was a necessary restriction to Article 19 ICCPR

Views adopted by the UN Human Rights Committee, Pavel Katorzhevsky v Belarus, communication no. 3095/2018, UN Doc CCPR/C/139/D/3095/2018, 13 October 2023

[...]

7.2 The Committee notes the author's allegations that the authorities violated his rights under article 19 of the Covenant, as he was convicted and fined for sharing a link on the social media network VKontakte to an article entitled "Idiocy and fake honour to the victims of war in a capital city gymnasium". [...]

[...]

7.4 [...] The Committee also notes that when convicting the author, the national courts referred to the decision of the Central District Court of Minsk of 10 November 2016 by which all "informational products" (which include posts to websites and social media platforms) published on vk.com/rdbelarus were declared to be extremist materials and were included in the State List of Extremist Materials.

7.5 [...] The Committee observes that, as acknowledged by the State party [...], all the informational products (posts) that were published on the mentioned websites before and after the delivery of the court's decision of 10 November 2016 are automatically declared extremist materials without an individualized assessment of each informational product (post).

7.6 The Committee recalls that any restrictions on the operation of websites, blogs or any other Internet-based, electronic or other such information dissemination systems, including systems to support such communication, such as Internet service providers or search engines, are only permissible to the extent that they are compatible with article 19 (3) of the Covenant. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3.

7.7 [...] The Committee reiterates that even if the sanctions imposed on the author were permitted under domestic law, the State party must show that they were necessary for one of the legitimate aims set out in article 19 (3). The Committee further observes that the State party has failed to invoke any specific grounds related to the author to support the necessity of the restrictions imposed on him, as is required under article 19 (3) of the Covenant.

7.8 In particular, the Committee notes that the court decisions made no individualized assessment of the author's case and have not provided any explanation as to why the conviction and fine imposed on him were necessary and the least intrusive among the measures which might achieve the relevant protective function and were proportionate to the interest to be protected. It therefore considers that the author's right to freedom of expression under article 19 (2) of the Covenant has been violated.

(4.2.4) Actio popularis is not allowed in human rights law: conceptualising the victim status requirement under the ECHR in case of collateral effects of a blocking measure

ECtHR, Cengiz and Others v Turkey, App nos. 48226/10 and 14027/11, 1 December 2015

3. Relying on Article 10 of the Convention, the applicants complained in particular of a measure that had deprived them of all access to YouTube.

[...]

5. Mr Cengiz [...] is a lecturer at the Law Faculty of İzmir University and is an expert and legal practitioner in the field of freedom of expression. [...] Mr Akdeniz is a professor of law at the Law Faculty of Istanbul Bilgi University. Mr Altıparmak is an assistant professor of law at the Political Science Faculty of Ankara University and director of the university's Human Rights Centre.

The Court's assessment on the victim status of the applicants

47. The Court notes that in a decision adopted on 5 May 2008, the Ankara Criminal Court of First Instance ordered the blocking of access to YouTube under section 8(1)(b), (2), (3) and (9) of Law no. 5651 on the ground that the content of ten video files available on the website in question had infringed Law no. 5816 prohibiting insults to the memory of Atatürk. The first applicant lodged an objection against the blocking order on 21 May 2010, seeking to have it set aside, and the second and third applicants did likewise on 31 May 2010. In their objections they relied on the protection of their right to freedom to receive and impart information and ideas.

48. On 9 June 2010 the Ankara Criminal Court of First Instance, finding that the applicants had not been parties to the case and thus did not have locus standi to challenge such orders, dismissed their objection. In so doing, it noted, among other things, that the blocking order complied with the requirements of the relevant legislation. It also adopted a further decision on 17 June 2010. Attempts by two of the applicants to challenge that decision were to no avail.

49. The Court reiterates at the outset that the Convention does not allow an actio popularis but requires as a condition for the exercise of the right of individual petition that the applicant be able to claim on arguable grounds that he himself has been a direct or indirect victim of a violation of the Convention resulting from an act

or omission which can be attributed to a Contracting State. In Tanrıkulu and Others [...], it found that readers of a newspaper whose distribution had been prohibited did not have victim status. Similarly, in Akdeniz [...], it held that the mere fact that Mr Akdeniz – like the other users of two music-streaming websites in Turkey – was indirectly affected by a blocking order could not suffice for him to be acknowledged as a "victim" within the meaning of Article 34 of the Convention. In view of those considerations, the answer to the question whether an applicant can claim to be the victim of a measure blocking access to a website will therefore depend on an assessment of the circumstances of each case, in particular the way in which the person concerned uses the website and the potential impact of the measure on him. It is also relevant that the Internet has now become one of the principal means by which individuals exercise their right to freedom to receive and impart information and ideas, providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest [...]

50. In the present case, the Court observes that the applicants lodged their applications with it as active YouTube users; among other things, they drew attention to the repercussions of the blocking order on their academic work and to the significant features of the website in question. They stated, in particular, that through their YouTube accounts they used the platform not only to access videos relating to their professional sphere, but also in an active manner, for the purpose of uploading and sharing files of that nature. The second and third applicants also pointed out that they had published videos on their academic activities. In that respect, the case more closely resembles that of Mr Yıldırım, who stated that he published his academic work and his views on various topics on his own website [...], than that of Mr Akdeniz [...], who was acting as a simple website user.

[...]

52. Moreover, as to the importance of Internet sites in the exercise of freedom of expression, the Court reiterates that "[i]n the light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information in general" [...]. In this connection, the Court observes that YouTube is a video-hosting website on which users can upload, view and share videos and is undoubtedly an important means of exercising the freedom to receive and impart information and ideas. In particular, as the applicants rightly noted, political content ignored by the traditional media is often shared via YouTube, thus fostering the emergence of citizen journalism. From that perspective, the Court accepts that YouTube is a unique platform on account of its characteristics, its accessibility and above all its potential impact, and that no alternatives were available to the applicants.

53. Furthermore, the Court observes that, after the applicants lodged their applications, the Constitutional Court examined whether active users of websites such as https://twitter.com and www.youtube.com could be regarded as victims. In particular, in the case concerning the administrative decision to block access to YouTube, it granted victim status to certain active users of the site, among them the second and third applicants. In reaching that conclusion, it mainly had regard to the fact that the individuals concerned, who all had a YouTube account, made active use of the site. In the case of the two applicants in question, it also took into consideration the fact that they taught at universities, carried out research in the field of human rights, used the website to access a range of visual material and shared their research via their YouTube accounts [...] The Court endorses the Constitutional Court's conclusions concerning these applicants' victim status. In addition, it observes that the situation of the first applicant, also an active YouTube user, is no different from that of the other two applicants.

54. To sum up, the Court observes that the applicants are essentially complaining of the collateral effects of the measure taken against YouTube in the context of Internet legislation. Their contention is that, on account

of the YouTube features, the blocking order deprived them of a significant means of exercising their right to freedom to receive and impart information and ideas.

55. Having regard to the foregoing and to the need for flexible application of the criteria for acknowledging victim status, the Court accepts that, in the particular circumstances of the case, the applicants may legitimately claim that the decision to block access to YouTube affected their right to receive and impart information and ideas even though they were not directly targeted by it. It therefore dismisses the Government's preliminary objection as to victim status.

(4.2.5) Principle of legality and safeguards regarding the effects of a wholesale blocking of access to a website: foreseeability; transparency of blocking measures; judicial review

ECtHR, Vladimir Kharitonov v Russia, App no 10795/14, 23 June 2020

34. The applicant has been the owner and administrator of a website featuring content relating to the production and distribution of electronic books, from news to analytical reports to practical guides. The website has existed since 2008 and has been updated several times a week. It has been stored on the servers of a US-based company offering accessible shared web-hosting solutions. The applicant's website has a unique domain name – "www.digital-books.ru" – but shares a numerical network address ("IP address") with many other websites hosted on the same server.

35. In December 2012, the applicant discovered that access to his website had been blocked. This was an incidental effect of a State agency's decision to block access to another website which was hosted on the same server and had the same IP address as the applicant's website. The Court reiterates that measures blocking access to websites are bound to have an influence on the accessibility of the Internet and, accordingly, engage the responsibility of the respondent State under Article 10 [...]

36. The applicant was not aware of the proceedings against the third-party website, the grounds for the blocking measure or its duration. He did not have knowledge of, or control over, when, if ever, the measure would be lifted and access to his website restored. He was unable to share the latest developments and news about electronic publishing, while visitors to his website were prevented from accessing the entire website content. It follows that the blocking measure in question amounted to "interference by a public authority" with the right to receive and impart information, since Article 10 guarantees not only the right to impart information but also the right of the public to receive it [...]. Such interference will constitute a breach of Article 10 unless it is "prescribed by law", pursues one or more of the legitimate aims referred to in Article 10 § 2 and is "necessary in a democratic society" to achieve those aims.

37. The Court reiterates that the expression "prescribed by law" not only refers to a statutory basis in domestic law, but also requires that the law be both adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual to foresee the consequences which a given action may entail. [...]

38. [...] The Court notes with concern that [Russian legislation] allows the authorities to target an entire website without distinguishing between the legal and illegal content it may contain. Reiterating that the wholesale blocking of access to an entire website is an extreme measure which has been compared to banning a newspaper or television station, the Court considers that a legal provision giving an executive agency so broad a discretion carries a risk of content being blocked arbitrarily and excessively.

[...]

41. [Russian legislation] conferred extensive powers on Roskomnadzor in the implementation of a blocking

order issued in relation to a specific website. Roskomnadzor can place a website on the Integrated Register of blocked content, ask the website owner and its hosting service provider to take down the illegal content, and add the website's IP address to the Integrated Register if they refuse to do so or fail to respond. However, the law did not require Roskomnadzor to check whether that address was used by more than one website or to establish the need for blocking by IP address. That manner of proceeding could, and did in the circumstances of the present case, have the practical effect of extending the scope of the blocking order far beyond the illegal content which had been originally targeted [...]. In fact, as the applicant and third-party interveners pointed out, millions of websites have remained blocked in Russia for the sole reason that they shared an IP address with some other websites featuring illegal content [...]

43. Turning next to the issue of safeguards against abuse which domestic legislation must provide in respect of incidental blocking measures, the Court reiterates that the exercise of powers to interfere with the right to impart information must be clearly circumscribed to minimise the impact of such measures on the accessibility of the Internet. In the instant case, Roskomnadzor gave effect to a decision by which a drug-control agency had determined the content of the offending website to be illegal. Both the original determination and Roskomnadzor's implementing orders had been made without any advance notification to the parties whose rights and interests were likely to be affected. The blocking measures had not been sanctioned by a court or other independent adjudicatory body providing a forum in which the interested parties could have been heard. Nor did the Russian law call for any impact assessment of the blocking measure prior to its implementation. [...]

44. As regards the transparency of blocking measures, the Government submitted that the applicant should have consulted Roskomnadzor's website. Indeed, Roskomnadzor provides a web service (http://blocklist.rkn.gov.ru/) which enables anyone to find out whether a website has been blocked and indicates the legal basis, the date and number of the blocking decision and the issuing body. It does not, however, give access to the text of the blocking decision, any indication of the reasons for the measure or information about avenues of appeal. Nor does Russian legislation make any provision for third-party notification of blocking decisions in circumstances where they have a collateral effect on the rights of other website owners. [...]

45. Lastly, as regards the proceedings which the applicant instituted to challenge the incidental effects of the blocking order, there is no indication that the judges considering his complaint sought to weigh up the various interests at stake, in particular by assessing the need to block access to all websites sharing the same IP address. [...] In reaching their decision, the courts confined their scrutiny to establishing that Roskomnadzor had acted in accordance with the letter of the law. However, in the Court's view, a Convention-compliant review should have taken into consideration [...]

46. The Court reiterates that it is incompatible with the rule of law if the legal framework fails to establish safeguards capable of protecting individuals from excessive and arbitrary effects of blocking measures, such as those in issue in the instant case. When exceptional circumstances justify the blocking of illegal content, a State agency making the blocking order must ensure that the measure strictly targets the illegal content and has no arbitrary or excessive effects, irrespective of the manner of its implementation. Any indiscriminate blocking measure which interferes with lawful content or websites as a collateral effect of a measure aimed at illegal content or websites amounts to arbitrary interference with the rights of owners of such websites. [...] Accordingly, the interference was not "prescribed by law" and it is not necessary to examine whether the other requirements of paragraph 2 of Article 10 have been met.

(4.2.6) Are generic Internet/services shutdowns lawful under human rights?

UN Human Rights Council, Res 47/16, The promotion, protection and enjoyment of human rights on the Internet, UN Doc A/HRC/RES/47/16, 7 July 2021

> 11. *Condemns unequivocally* measures in violation of international human rights law that prevent or disrupt an individual's ability to seek, receive or impart information online, including Internet shutdowns and online censorship, calls upon all States to refrain from and to cease such measures, and also calls upon States to ensure that all domestic laws, policies and practices are consistent with their international human rights obligations with regard to freedom of opinion and expression, and of association and peaceful assembly, online.

Case study: #KeepItOn: authorities in Mozambique must stop normalizing internet shutdowns during protests, 8 November 2024

We, the undersigned organizations, and members of the #KeepItOn coalition — a global network of over 334 human rights organizations from 105 countries working to end internet shutdowns — urgently demand that the government of Mozambique put an immediate end to the increasing use of shutdowns amid ongoing protests and police crackdown on protesters in Mozambique. Reports from local rights groups indicate that police have resorted to excessive use of violence resulting in more than 20 deaths and multiple injuries.

Since October 25, 2024, in response to growing protests against disputed election results announced by the Election Commission, authorities in Mozambique have imposed at least five instances of curfew style mobile internet shutdowns with the most recent happening on November 6, alongside social media shutdowns lasting several hours. The recent shutdowns in the country follow a worrying trend that authorities in Mozambique began in October 2023, when they imposed a total internet blackout for at least three hours for the first time during local elections. Mozambican authorities' regular practice of shutting down the internet around elections and in times of political unrest must not be allowed to continue.

Internet shutdowns are a violation of human rights.

[...]

Election-related shutdowns prevent voters, journalists, opposition, and election observers from accessing or sharing essential information, decreasing the fairness, credibility, and transparency of elections. They empower authoritarian regimes to control the narrative throughout the electoral period, undermining the electorate's ability to make informed decisions, access polling resources, and fully shape their nation's future. Now more than ever, when there is unrest due to contested

election results, the government must ensure people have unfettered access to open and secure internet and digital platforms to promote transparency and access pertinent information in a timely manner.

[...]

Restricting access to the internet, mobile devices, and communication platforms during periods of unrest such as conflicts and protests, and moments of national importance such as elections, further puts people at risk and undermines the enjoyment of all other human rights, from education and work to healthcare and public services, as well as free expression and peaceful assembly [...]

Questions to reflect

1. How Internet or services shutdowns impact the effective exercise of human rights? Are they lawful under human rights?
2. Do you agree with how the ECtHR used the concept of an *active YouTube user* in the Cengiz and Others v Turkey case to justify the fact that it adopts a flexible application of the criteria for acknowledging victim status while not permitting an action popularis? Who is an active social media user, in your view? Receiving information does not make someone an active social media user?
3. What is the meaning of collateral effects and how does the ECtHR use this concept in its reasoning?
4. What are measures that States are required to take in order for the collateral effects of a blocking measure of an Internet service/platform to be lawful under Article 10 ECHR?

(4.3) The private governance of content regulation

Content regulation, by platforms and social media form a de facto regime of private censorship. This regime consists of design/engineering choices of technologies embedded in AI systems, policies and terms of service, internal practices as well as moderation and curation practices (section 4.3.1). One of the issues examined here is the conditions upon which states may impose intermediary liability on platforms. The imposition of liability on platforms should not violate the platform's freedom to impart information under Article 10 ECHR. These were the main issues in the Delfi case before the ECtHR (section 4.3.2). Another issue that we highlight is how terms of service and policies as well as internal remedies set up and enforced by business corporations impact the users' right to freedom of expression. We discuss this topic from the view of a private "adjudicative" body (MTA Oversight Board) in the "Two buttons" meme case (section 4.3.3). In that case, the Oversight META Board scrutinised Facebook's policies on satire and Facebook's content moderators' capacity to review content containing satire.

(4.3.1) Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Freedom of expression, states and the private sector in the digital age, UN Doc A/HRC/32/38, 11 May 2016

Internal policies and practices

51. Intermediaries' policies and rules may have significant effects on the freedom of expression. While terms of service are the primary source of regulation, design and engineering choices may also affect the delivery of content.

Terms of service

52. Terms of service, which individuals typically must accept as a condition to access a platform, often contain restrictions on content that may be shared. These restrictions are formulated under local laws and regulations and reflect similar prohibitions, including those against harassment, hate speech, promotion of criminal activity, gratuitous violence and direct threats. Terms of service are frequently formulated in such a general way that it may be difficult to predict with reasonable certainty what kinds of content may be restricted. The inconsistent enforcement of terms of service has also attracted public scrutiny. [...] Lack of an appeals process or poor communication by the company about why content was removed or an account deactivated adds to these concerns. [...]

Design and engineering choices

55. The manner in which intermediaries curate, categorize and rank content affects what information users access and view on their platforms. For example, platforms deploy algorithmic predictions of user preferences and consequently guide the advertisements individuals might see, how their social media feeds are arranged and the order in which search results appear. Other self-regulatory measures, such as "counter speech" initiatives to support anti-terror or anti-harassment messages, also affect the ways in which users might consume and process Internet content concerning sensitive topics. [...]

Remedies

69. To enforce terms of service, companies may not always have sufficient processes to appeal content removal or account deactivation decisions where a user believes the action was in error or the result of abusive flagging

campaigns. Further research that examines best practices in how companies communicate terms of service enforcement decisions and how they implement appeals mechanisms may be useful.

71. The appropriate role of the State in supplementing or regulating corporate remedial mechanisms also requires closer analysis. Civil proceedings and other judicial redress are often available to consumers adversely affected by corporate action, but these are often cumbersome and expensive. Meaningful alternatives may include complaint and grievance mechanisms established and run by consumer protection bodies and industry regulators. Several States also mandate internal remedial or grievance mechanisms. [...]

(4.3.2) Intermediary liability of platforms and state responsibility under human rights law

ECtHR, Delfi AS v. Estonia, App no 64569/09, 16 June 2015 (Grand Chamber)

Delfi is the first case in which the Court was called upon to examine a complaint regarding user-generated expressive activity and platform liability.

In the this case, the majority of the users' comments constituted hate speech and/or speech that directly advocated acts of violence. For this reason, the comments did not enjoy the protection of Article 10 ECHR and thus the freedom of expression of the authors of the comments was not an issue in this case.

The question before the Court was whether the domestic courts' decisions, holding the applicant company liable for these comments posted by third parties, were in breach of the applicant company's freedom to impart information.

3. The applicant company alleged that its freedom of expression had been violated, in breach of Article 10 of the Convention, by the fact that it had been held liable for the third-party comments posted on its Internet news portal.

11. The applicant company is the owner of Delfi, an Internet news portal that published up to 330 news articles a day at the time of the lodging of the application. Delfi is one of the largest news portals on the Internet in Estonia. It publishes news in Estonian and Russian in Estonia, and also operates in Latvia and Lithuania.

[...]

110. The Court notes at the outset that user-generated expressive activity on the Internet provides an unprecedented platform for the exercise of freedom of expression. That is undisputed and has been recognised by the Court on previous occasions [...]. However, alongside these benefits, certain dangers may also arise. Defamatory and other types of clearly unlawful speech, including hate speech and speech inciting violence, can be disseminated like never before, worldwide, in a matter of seconds, and sometimes remain persistently available online. These two conflicting realities lie at the heart of this case. Bearing in mind the need to protect the values underlying the Convention, and considering that the rights under Articles 10 and 8 of the Convention deserve equal respect, a balance must be struck that retains the essence of both rights. Thus, while the Court acknowledges that important benefits can be derived from the Internet in the exercise of freedom of expression, it is also mindful that the possibility of imposing liability for defamatory or other types of unlawful speech must, in principle, be retained, constituting an effective remedy for violations of personality rights.

[...]

117. [...] The applicant company's news portal was one of the biggest Internet media publications in the country; it had a wide readership and there was a known public concern regarding the controversial nature of the

comments it attracted [...]. Moreover, [...] the impugned comments in the present case [...] mainly constituted hate speech and speech that directly advocated acts of violence. [...]

[...]

Necessary in a democratic society

(a) General principles

131. The fundamental principles concerning the question whether an interference with freedom of expression is "necessary in a democratic society" are well established in the Court's case-law [...]

132. Furthermore, the Court has emphasised the essential function the press fulfils in a democratic society. Although the press must not overstep certain bounds, particularly as regards the reputation and rights of others and the need to prevent the disclosure of confidential information, its duty is nevertheless to impart – in a manner consistent with its obligations and responsibilities – information and ideas on all matters of public interest [...].

[...]

136. Moreover, the Court has held that speech that is incompatible with the values proclaimed and guaranteed by the Convention is not protected by Article 10 by virtue of Article 17 of the Convention. The examples of such speech examined by the Court have included statements denying the Holocaust, justifying a pro-Nazi policy, linking all Muslims with a grave act of terrorism, or portraying the Jews as the source of evil in Russia [...]

137. The Court further reiterates that the right to protection of reputation is a right which is protected by Article 8 of the Convention as part of the right to respect for private life [...].

138. When examining whether there is a need for an interference with freedom of expression in a democratic society in the interests of the "protection of the reputation or rights of others", the Court may be required to ascertain whether the domestic authorities have struck a fair balance when protecting two values guaranteed by the Convention which may come into conflict with each other in certain cases, namely, on the one hand, freedom of expression protected by Article 10, and, on the other, the right to respect for private life enshrined in Article 8 [...]

139. The Court has found that, as a matter of principle, the rights guaranteed under Articles 8 and 10 deserve equal respect, and the outcome of an application should not, in principle, vary according to whether it has been lodged with the Court under Article 10 of the Convention by the publisher of an offending article or under Article 8 of the Convention by the person who was the subject of that article. Accordingly, the margin of appreciation should in principle be the same in both cases [...]. Where the balancing exercise between those two rights has been undertaken by the national authorities in conformity with the criteria laid down in the Court's case-law, the Court would require strong reasons to substitute its view for that of the domestic courts [...].

(b) Application of the above principles to the present case

(i) Elements in the assessment of proportionality

140. [...] the applicant company removed the comments once it was notified by the injured party, and described them as "infringing" and "illicit" before the Chamber [...]. Moreover, the Court is of the view that the majority of the impugned comments amounted to hate speech or incitements to violence and as such did not enjoy the protection of Article 10 [...]. Thus, the freedom of expression of the authors of the comments is not in issue in the present case. Rather, the question before the Court is whether the domestic courts' decisions, holding the applicant company liable for these comments posted by third parties, were in breach of its freedom to impart information as guaranteed by Article 10 of the Convention.

[...]

142. [...] In order to resolve the question whether the domestic courts' decisions holding the applicant

company liable for the comments posted by third parties were in breach of its freedom of expression, the [Court] identified the following aspects as relevant for its analysis: the context of the comments, the measures applied by the applicant company in order to prevent or remove defamatory comments, the liability of the actual authors of the comments as an alternative to the applicant company's liability, and the consequences of the domestic proceedings for the applicant company [...]

[...]

(ii) Context of the comments

144. As regards the context of the comments, the Court accepts that the news article about the ferry company, published on the Delfi news portal, was a balanced one, contained no offensive language and gave rise to no arguments regarding unlawful statements in the domestic proceedings. [...] Furthermore, it attaches particular weight, in this context, to the nature of the Delfi news portal. It reiterates that Delfi was a professionally managed Internet news portal run on a commercial basis which sought to attract a large number of comments on news articles published by it. [...] The applicant company had integrated the comments section into its news portal, inviting visitors to the website to complement the news with their own judgments and opinions (comments). According to the findings of the Supreme Court, in the comments section, the applicant company actively called for comments on the news items appearing on the portal. The number of visits to the applicant company's portal depended on the number of comments; the revenue earned from advertisements published on the portal, in turn, depended on the number of visits. Thus, the Supreme Court concluded that the applicant company had an economic interest in the posting of comments. In the view of the Supreme Court, the fact that the applicant company was not the author of the comments did not mean that it had no control over the comments section [...]

145. The Court also notes in this regard that the Rules on posting comments on the Delfi website stated that the applicant company prohibited the posting of comments that were without substance and/or off topic, were contrary to good practice, contained threats, insults, obscene expressions or vulgarities, or incited hostility, violence or illegal activities. Such comments could be removed and their authors' ability to post comments could be restricted. Furthermore, the actual authors of the comments could not modify or delete their comments once they were posted on the applicant company's news portal – only the applicant company had the technical means to do this. In the light of the above [...] the applicant company must be considered to have exercised a substantial degree of control over the comments published on its portal.

(iii) Liability of the authors of the comments

147. In connection with the question whether the liability of the actual authors of the comments could serve as a sensible alternative to the liability of the Internet news portal in a case like the present one, the Court is mindful of the interest of Internet users in not disclosing their identity. Anonymity has long been a means of avoiding reprisals or unwanted attention. As such, it is capable of promoting the free flow of ideas and information in an important manner, including, notably, on the Internet. At the same time, the Court does not lose sight of the ease, scope and speed of the dissemination of information on the Internet, and the persistence of the information once disclosed, which may considerably aggravate the effects of unlawful speech on the Internet compared to traditional media. [...]

148. The Court observes that different degrees of anonymity are possible on the Internet. An Internet user may be anonymous to the wider public while being identifiable by a service provider [...] A service provider may also allow an extensive degree of anonymity for its users, in which case the users are not required to identify themselves at all and they may only be traceable – to a limited extent – through the information retained by Internet access providers.

[...]

(iv) Measures taken by the applicant company

152. The Court notes that the applicant company highlighted the number of comments on each article on its website, and therefore the articles with the most lively exchanges must have been easily identifiable for the editors of the news portal. The article in issue in the present case attracted 185 comments, apparently well above average. The comments in question were removed by the applicant company some six weeks after they were uploaded on the website, upon notification by the injured person's lawyers to the applicant company [...]

153. [...] [Given the fact] that the applicant company must be considered to have exercised a substantial degree of control over the comments published on its portal, the Court does not consider that the imposition on the applicant company of an obligation to remove from its website, without delay after publication, comments that amounted to hate speech and incitements to violence, and were thus clearly unlawful on their face, amounted, in principle, to a disproportionate interference with its freedom of expression.

154. The pertinent issue in the present case is whether the national court's findings that liability was justified, as the applicant company had not removed the comments without delay after publication, were based on relevant and sufficient grounds. With this in mind, account must first be taken of whether the applicant company had put in place mechanisms that were capable of filtering comments amounting to hate speech or speech entailing an incitement to violence.

155. The Court notes that the applicant company took certain measures in this regard. There was a disclaimer on the Delfi news portal stating that the writers of the comments – and not the applicant company – were accountable for them, and that the posting of comments that were contrary to good practice or contained threats, insults, obscene expressions or vulgarities, or incited hostility, violence or illegal activities, was prohibited. Furthermore, the portal had an automatic system of deletion of comments based on stems of certain vulgar words and it had a notice-and-take-down system in place, whereby anyone could notify it of an inappropriate comment by simply clicking on a button designated for that purpose to bring it to the attention of the portal administrators. In addition, on some occasions the administrators removed inappropriate comments on their own initiative.

156. Thus, the Court notes that the applicant company cannot be said to have wholly neglected its duty to avoid causing harm to third parties. Nevertheless, and more importantly, the automatic word-based filter used by the applicant company failed to filter out odious hate speech and speech inciting violence posted by readers and thus limited its ability to expeditiously remove the offending comments. [...] The Court notes that as a consequence of this failure of the filtering mechanism these clearly unlawful comments remained online for six weeks [...]

157. [...] Having regard to the fact that there are ample opportunities for anyone to make his or her voice heard on the Internet, the Court considers that a large news portal's obligation to take effective measures to limit the dissemination of hate speech and speech inciting violence – the issue in the present case – can by no means be equated to "private censorship".

[...]

159. [...] the applicant company has argued [...] that the Court should have due regard to the notice-and-take-down system that it had introduced. If accompanied by effective procedures allowing for rapid response, this system can in the Court's view function in many cases as an appropriate tool for balancing the rights and interests of all those involved. However, in cases such as the present one, where third-party user comments are in the form of hate speech and direct threats to the physical integrity of individuals, as understood in the Court's case-law [...], the Court considers [...] that the rights and interests of others and of society as a whole may entitle Contracting States to impose liability on Internet news portals, without contravening Article 10 of

the Convention, if they fail to take measures to remove clearly unlawful comments without delay, even without notice from the alleged victim or from third parties.

[...]

162. Based on the concrete assessment of the above aspects, taking into account the reasoning of the Supreme Court in the present case, in particular the extreme nature of the comments in question, the fact that the comments were posted in reaction to an article published by the applicant company on its professionally managed news portal run on a commercial basis, the insufficiency of the measures taken by the applicant company to remove without delay after publication comments amounting to hate speech and speech inciting violence and to ensure a realistic prospect of the authors of such comments being held liable, and the moderate sanction imposed on the applicant company, the Court finds that the domestic courts' imposition of liability on the applicant company was based on relevant and sufficient grounds, having regard to the margin of appreciation afforded to the respondent State. Therefore, the measure did not constitute a disproportionate restriction on the applicant company's right to freedom of expression.

Accordingly, there has been no violation of Article 10 of the Convention.

(4.3.3) How terms of service and remedies by business corporations impact the right to freedom of expression: the view from a private "adjudicative" body (META Oversight Board)

META Oversight Board: "Two buttons" meme case, case no: 021-005-FB-UA, 20 May 2021



2. Case description

On December 24, 2020, a Facebook user in the United States posted a comment with an adaption of the "daily struggle" or "two buttons" meme. A meme is a piece of media, which is often humorous, that spreads quickly across the internet. This featured the same-split screen cartoon from the original meme, but with the Turkish flag substituted for the cartoon character's face. The cartoon character has its right hand on its head and appears to be sweating. Above the character, in the other half of the split-screen, there are two red buttons with corresponding statements in English: "The Armenian Genocide is a lie" and "The Armenians were terrorists that deserved it." The meme was preceded by a "thinking face" emoji.

The comment was shared on a public Facebook page that describes itself as forum for discussing religious matters from a secular perspective. It responded to a post containing an image of a person wearing a niqab with overlay text in English: "Not all prisoners are behind bars." At the time the comment was removed, that original post it responded to had 260 views, 423 reactions and 149 comments. A Facebook user in Sri Lanka reported the comment for violating the Hate Speech Community Standard.

Facebook removed the meme on December 24, 2020. Within a short period of time, two content moderators reviewed the comment against the company's policies and reached different conclusions. While the first concluded that the meme violated Facebook's Hate Speech policy, the second determined that the meme violated the Cruel and Insensitive policy. The content was removed and logged in Facebook's systems based on the second review. On this basis, Facebook notified the user that their comment "goes against our Community Standard on cruel insensitive content."

After the user's appeal, Facebook upheld its decision but found that the content should have been removed under its Hate Speech policy. For Facebook, the statement "The Armenians were terrorists that deserved it" specifically violated the prohibition on content claiming that all members of a protected characteristic are criminals, including terrorists. No other parts of the content, such as the claim that the Armenian genocide was a lie, were deemed to be violating. Facebook did not inform the user that it upheld the decision to remove their content under a different Community Standard.

The user submitted their appeal to the Oversight Board on December 24, 2020.

Lastly, in this decision, the Board referred to the atrocities committed against the Armenian people from 1915 onwards as genocide, as this term is commonly used to describe the massacres and mass deportations suffered by Armenians and it is also referred to in the content under review. The Board does not have the authority to legally qualify such atrocities and this qualification is not the subject of this decision.

[...]

4. Relevant standards

The Oversight Board considered the following standards in its decision:

Facebook's Community Standards

Facebook's Community Standards define hate speech as "a direct attack on people based on what we call protected characteristics – race, ethnicity, national origin, religious affiliation, sexual orientation, caste, sex, gender, gender identity, and serious disease or disability." Under "Tier 1," prohibited content ("do not post") includes content targeting a person or group of people on the basis of a protected characteristic with:

- "dehumanizing speech or imagery in the form of comparisons, generalizations, or unqualified behavioral statements (in written or visual form) to or about [...] criminals (including, but not limited to, "thieves", "bank robbers", or saying "All [protected characteristic or quasi-protected characteristic] are 'criminals'").
- speech "[m]ocking the concept, events or victims of hate crimes even if no real person is depicted in an

image."
- speech "[d]enying or distorting information about the Holocaust."

However, Facebook allows "content that includes someone else's hate speech to condemn it or raise awareness." According to the Hate Speech Community Standard's policy rationale, "speech that might otherwise violate our standards can be used self-referentially or in an empowering way. Our policies are designed to allow room for these types of speech, but we require people to clearly indicate their intent. If intention is unclear, we may remove content."

[...]

Human rights standards

The UN Guiding Principles on Business and Human Rights (UNGPs), endorsed by the UN Human Rights Council in 2011, establish a voluntary framework for the human rights responsibilities of private businesses. In 2021, Facebook announced its Corporate Human Rights Policy, where it committed to respecting rights in accordance with the UNGPs. The Board's analysis in this case was informed by the following human rights standards:

1. Freedom of expression [...]
2. The right to non-discrimination [...]
3. The right to be informed in the context of access to justice [...]

User statement

The user stated in their appeal to the Board that "historical events should not be censored." They noted that their comment was not meant to offend but to point out "the irony of a particular historical event." The user noted that "perhaps Facebook misinterpreted this as an attack." [...] The user found Facebook and its policies overly restrictive and argued that "[h]umor like many things is subjective and something offensive to one person may be funny to another."

[...]

8.1.3 Analysis of the combined statements in the meme

The Board is of the view that one should evaluate the content as a whole, including the effect of juxtaposing these statements in a well-known meme. A common purpose of the "daily struggle" or "two buttons" meme is to contrast two different options to highlight potential contradictions or other connotations, rather than to indicate support for the options presented.

For the majority, the exception to the Hate Speech policy is crucial. This exception allows people to "share content that includes someone else's hate speech to condemn it or raise awareness." It also states: "our policies are designed to allow room for these types of speech, but we require people to clearly indicate their intent. If intention is unclear, we may remove content." The majority noted that the content could also fall under the company's satire exception, which is not publicly available.

Assessing the content as a whole, the majority found that the user's intent was clear. They shared the meme as satire to raise awareness about and condemn the Turkish government's efforts to deny the Armenian genocide while, at the same time, justifying the same historic atrocities. The user's intent was not to mock the victims of these events, nor to claim those victims were criminals or that the atrocity was justified. The majority took into account the Turkish government's position on genocide suffered by Armenians from 1915 onwards [...] as well as the history between Turkey and Armenia. In this context, they found that the cartoon character's sweating face replaced with a Turkish flag and the content's direct link to the Armenian genocide, meant the

user shared the meme to criticize the Turkish government's position on this issue. The use of the "thinking face" emoji, which is commonly used sarcastically, alongside the meme, supports this conclusion. [...] It would thus be wrong to remove this comment in the name of protecting Armenians, when the post is a criticism of the Turkish government, in support of Armenians.

As such, the majority found that, taken as a whole, the content fell within the policy exception in Facebook's Hate Speech Community Standard. For the minority, in the absence of specific context, the user's intent was not sufficiently clear to conclude that the content was shared as satire criticizing the Turkish government. Additionally, the minority found that the user was not able to properly articulate what the alleged humor intended to express. Given the content includes a harmful generalization against Armenians, the minority found that it violated the Hate Speech Community Standard.

[...]

8.3 Compliance with Facebook's human rights responsibilities

Freedom of expression (Article 19 ICCPR)

Article 19, para. 2 of the ICCPR provides broad protection for expression of "all kinds," including written and non-verbal "political discourse," as well as "cultural and artistic expression." The UN Human Rights Committee has made clear the protection of Article 19 extends to expression that may be considered "deeply offensive" [...]

In this case, the Board found that the cartoon, in the form of a satirical meme, took a position on a political issue: the Turkish government's stance on the Armenian genocide. The Board noted that "cartoons that clarify political positions" and "memes that mock public figures" may be considered forms of artistic expression protected under international human rights law [...] [...]

While the right to freedom of expression is fundamental, it is not absolute. It may be restricted, but restrictions should meet the requirements of legality, legitimate aim, and necessity and proportionality [...]. Facebook should seek to align its content moderation policies on hate speech with these principles [...]

Legality

Any rules restricting expression must be clear, precise, and publicly accessible [...].Facebook's Community Standards "permit content that includes someone else's hate speech to condemn it or raise awareness," but ask users to "clearly indicate their intent." In addition, the Board also noted that Facebook removed an exception for humor from its Hate Speech policy following a Civil Rights Audit concluded in July 2020. While this exception was removed, the company kept a narrower exception for satire that is currently not communicated to users in its Hate Speech Community Standard.

The Board also noted that Facebook wrongfully reported to the user that they violated the Cruel and Insensitive Community Standard, when Facebook based its enforcement on the Hate Speech policy. The Board found that it is not clear enough to users that the Cruel and Insensitive Community Standard only applies to content that depicts or names victims of harm.

Additionally, the Board found that properly notifying users of the reasons for enforcement action against them would help users follow Facebook's rules. This relates to the legality issue, as the lack of relevant information for users subject to content removal "creates an environment of secretive norms, inconsistent with the standards of clarity, specificity and predictability" which may interfere with "the individual's ability to challenge content actions or follow up on content-related complaints." [...] Facebook's approach to user notice in this case therefore failed the legality test.

Legitimate aim

Any restriction on freedom of expression should also pursue a "legitimate aim." The Board agreed the restriction pursued the legitimate aim of protecting the rights of others [...]

Necessity and proportionality

[...]

A majority of the Board concluded that Facebook's interference with the user's freedom of expression was mistaken. The removal of the comment would not protect the rights of Armenians to equality and non-discrimination. The user was not endorsing the statements contrasted in the meme, but rather attributing them to the Turkish government. They did this to condemn and raise awareness of the government's contradictory and self-serving position. The majority found that the effects of satire, such as this meme, would be lessened if people had to explicitly declare their intent. The fact that the "two buttons" or "daily struggle" meme is usually intended to be humorous, even though the subject matter here was serious, also contributed to the majority's decision.

[...]

the Board was concerned with Facebook content moderators' capacity to review this meme and similar pieces of content containing satire. Contractors should follow adequate procedures and be provided with time, resources and support to assess satirical content and relevant context properly.

While supporting majority's views on protecting satire on the platform, the minority did not believe that the content was satire. The minority found that the user could be embracing the statements contained in the meme, and thus engaging in discrimination against Armenians. Therefore, the minority held that the requirements of necessity and proportionality have been met in this case. [...] The minority found that, similarly, where the satirical nature of the content is not obvious, as in this case, the user's intent should be made explicit. The minority concluded that, while satire is about ambiguity, it should not be ambiguous regarding the target of the attack, i.e., the Turkish government or the Armenian people.

Oversight Board decision

The Oversight Board overturns Facebook's decision to remove the content and requires the content to be restored.

Policy advisory statement

[...]

Include the satire exception, which is currently not communicated to users, in the public language of the Hate Speech Community Standard.

[...]

Make sure that it has adequate procedures in place to assess satirical content and relevant context properly. This includes providing content moderators with: (i) access to Facebook's local operation teams to gather relevant cultural and background information; and (ii) sufficient time to consult with Facebook's local operation teams and to make the assessment. Facebook should ensure that its policies for content moderators incentivize further investigation or escalation where a content moderator is not sure if a meme is satirical or not.

[...]

Questions / Exercises

1. Can you explain and assess in what ways content regulation is subject to private governance?
2. What are States' obligations in supplementing or regulating the private sector?
3. What are the elements that the Court adopted in the Delfi case for assessing the proportionality of the restriction imposed on the applicant company's freedom to impart information under Article 10 ECHR?
4. What were the measures applied by the applicant company (Delfi) in order to prevent or remove defamatory comments in the Delfi case?
5. How does the ECtHR assess the role of the notice-and-take-down system and in what scenarios States may impose liability on Internet news portals, without contravening Article 10 ECHR?
6. Do you agree with how the META Oversight Board in the "Two buttons" meme case weighed the interest of satire under the right to freedom of expression vis-à-vis the prohibition of hate speech?
7. How do you assess the Oversight Board's mandate and work in terms of protecting human rights?
8. Check the recommendation tracker of META's recommendations. Does META enforce the Oversight Board's recommendations?

Fun play: Two Buttons Meme generator

Generate your own two buttons meme

(4.4) Certain AI systems may not be compatible with freedom of thought and individual autonomy

AI systems that engage in practices of manipulation, exploitation of human vulnerabilities or emotion detection/analysis pose unique risks to individual autonomy and human rights. Examples of such AI systems include recommender systems oradvertisements based on targeting techniques optimised to appeal to individuals' or groups' vulnerabilities. Sentiment detection refers to systems that can infer a person's inner emotional state based on physical, physiological or behavioural markers (e.g., facial expressions, vocal tone) and sort them into discrete categories (e.g., angry).

Human rights law has a "toolbox" to unpack these challenges (4.4.2). Different rights may be relevant. The underdeveloped thus far right of freedom of thought has great potential for addressing impermissible interferences with how we form our opinions, process our emotions and make our decisions. The notion of mental integrity or aspects of the right to privacy (mental privacy) may come into play too. Moreover, the principles of human dignity, individual autonomy and self-determination should be brought to the foreground.

At the same time, one should not lose sight of the fact that human rights law may not have the capacity to fully capture and address all novel harms caused by AI systems. Other areas of law may be complementary and relevant, including recent prohibitions of specific AI systems under the EU AI Act, the EU DSA or consumer law (4.4.3).

(4.4.1) Case studies

(4.4.1.1) Sentiment detection: EU's experimentation with iBorderCtrl and lying-detection

D Boffey, EU border 'lie detector' system criticised as pseudoscience, The Guardian, 2 November 2018

The EU has been accused of promoting pseudoscience after announcing plans for a "smart lie-detection system" at its busiest borders to identify illegal migrants. The "lie detector", to be trialled in Hungary, Greece and Latvia, involves the use of a computer animation of a border guard, personalised to the traveller's gender, ethnicity and language, asking questions via a webcam.

The "deception detection" system will analyse the micro-expressions of those seeking to enter

EU territory to see if they are being truthful about their personal background and intentions. Those arriving at the border will be required to have uploaded pictures of their passport, visa and proof of funds. According to an article published by the European commission, the "unique approach to 'deception detection' analyses the micro-expressions of travellers to figure out if the interviewee is lying".

[...]

The project, which has received €4.5m (£3.95m) in EU funding, has been heavily criticised by experts. Bruno Verschuere, a senior lecturer in forensic psychology at the University of Amsterdam, told the Dutch newspaper De Volskrant he believed the system would deliver unfair outcomes. "Non-verbal signals, such as micro-expressions, really do not say anything about whether someone is lying or not," he said. "This is the embodiment of everything that can go wrong with lie detection. There is no scientific foundation for the methods that are going to be used now.

.

(4.4.1.2) YouTube and Snapchat recommender systems

Commission sends requests for information to YouTube, Snapchat, and TikTok on recommender systems under the Digital Services Act, 2 October 2024

Today, the Commission has sent a request for information to YouTube, Snapchat, and TikTok under the Digital Services Act (DSA), asking the platforms to provide more information on the design and functioning of their recommender systems. [...]

YouTube and Snapchat are requested to provide detailed information on the parameters used by their algorithms to recommend content to users, as well as their role in amplifying certain systemic risks, including those related to the electoral process and civic discourse, users' mental well-being (e.g. addictive behaviour and content 'rabbit holes'), and the protection of minors.

(4.4.1.3) Deceptive advertisements and disinformation

Commission opens formal proceedings against Facebook and Instagram under the DSA, Press release, 30 April 2024

The current proceedings will focus on the following areas:

Deceptive advertisements and disinformation. The Commission suspects that Meta does not comply with DSA obligations related to addressing the dissemination of deceptive advertisements, disinformation campaigns and coordinated inauthentic behaviour in the EU. The proliferation of such content may present a risk to civic discourse, electoral processes and fundamental rights, as well as consumer protection.

[...]



Image by ANDRI TEGAR MAHARDIKA from Pixabay

(4.4.2) Relevant human rights law

(4.4.2.1) Right to freedom of thought

Article 19 ICCPR

1. Everyone shall have the right to hold opinions without interference.

Article 10 ECHR

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

Article 10 EU Charter – Freedom of thought, conscience and religion

1. Everyone has the right to freedom of thought, conscience and religion.

(4.4.2.1.1) Freedom not to express one's opinion; coercing the holding or not holding of an opinion

UN Human Rights Committee, General Comment No 34, Article 19: Freedoms of opinion and expression, UN Doc CCPR/C/GC/34, 12 September 2011

9. Paragraph 1 of article 19 requires protection of the right to hold opinions without interference. This is a right to which the Covenant permits no exception or restriction. Freedom of opinion extends to the right to change an opinion whenever and for whatever reason a person so freely chooses. No person may be subject to the impairment of any rights under the Covenant on the basis of his or her actual, perceived or supposed opinions. All forms of opinion are protected, including opinions of a political, scientific, historic, moral or religious nature. It is incompatible with paragraph 1 to criminalize the holding of an opinion. [...]

10. Any form of effort to coerce the holding or not holding of any opinion is prohibited. Freedom to express one's opinion necessarily includes freedom not to express one's opinion.

(4.4.2.1.2) Interim report of the Special Rapporteur on freedom of religion or belief, Ahmed Shaheed, Freedom of thought, UN Doc A/76/380, 5 October 2021

2. Freedom of thought, along with one's conscience and belief, is regarded as part of one's *forum internum* – a person's inner sanctum (mind) where mental faculties are developed, exercised and defined. [...]

4. Articles 4 and 18 of the International Covenant on Civil and Political Rights confirm the right's significance, ascribing it absolute protection, even during public emergencies. Consequently, and unlike *forum externum* (external realm) freedoms that are subject to State limitations, if prescribed by law and necessary to protect public safety, order, health or morals, or the rights of others, States legally cannot ever interfere with freedom of thought. Despite its proclaimed importance and absolute nature, the right's scope and content remain largely underdeveloped and poorly understood. The right receives scant attention in jurisprudence, legislation and scholarship, international and otherwise.

11. What constitutes "thought" not only lacks legal precision, but also scientific and philosophical consensus. Neuroscientists generally agree that thoughts are created when billions of neurons (nerve cells) in the brain [...] But the consensus ends there. Some neuroscientists distinguish "thought" from other cognitive processes, including emotion, based on the primary part of the brain engaged. Others emphasize the complex, highly interrelated nature of anatomical aspects of the brain that support cognitive functions, comparing efforts to "trace a thought from beginning to end" to "asking where the forest begins".

[...]

25. Beyond absolute protection, relatively little is clear about the right's core elements or "attributes". Below, the Special Rapporteur maps four possible attributes of the right based on international human rights jurisprudence and commentary: (a) not being forced to reveal one's thoughts; (b) no punishment and/or sanctions for one's thoughts; (c) no impermissible alteration of one's thoughts; and (d) States fostering an enabling environment for freedom of thought.

[...]

35. A growing body of legal scholarship supports the claim that freedom of thought includes freedom from manipulation. While modification bypasses psychological processes to directly alter biological function, manipulation engages and controls psychological processes. Some scholars define manipulation to induce the formation of "biased mental models [...], knowledge and ideologies", or a form of "cognitive mind control".

[...]

Inference and predictive technologies

68. Several stakeholders assert that the use of predictive technologies by digital technology companies should raise concerns regarding freedom of thought. Predictive systems, by nature, do not reveal "actual" thoughts. Yet armed with vast and growing quantities of personal and non-personal data, such systems can reportedly build sophisticated individualized psychological profiles, which can potentially infer and even modify thoughts in certain circumstances.

69. They also express concern about the proliferation of predictive technologies, such as so-called artificial intelligence-powered polygraphs that make use of artificial intelligence, which feed biometric data (e.g., heart rate, speech patterns and facial features) into "truth detection" algorithms [...] The accuracy and, in some cases, the scientific basis of these technologies is heavily contested. Nonetheless, some argue that irrespective of whether these technologies violate mental privacy, they can and do still result in punishment for inferred thought. For example, Chinese authorities reportedly deploy "emotion detection" technologies to infer "criminal" states of mind among the public, which could lead to administrative or criminal sanctions. Moreover, several corporations and educational institutions allegedly utilize biometric data to infer the thoughts of their employees and students, respectively. Technology that monitors employee brain activity in workplaces is already proliferating, and some scholars postulate that employees might be punished for inferred thoughts, such as thoughts on unionizing.

70. Recent research indicates that result rankings from Internet search engines have a dramatic impact on consumer attitudes, preferences and behaviour – potentially even modifying their very thoughts. For example, five experiments in the United States and India have illustrated the power of search rankings to alter the preferences of undecided voters in democratic elections, noting that many users choose and trust higher-ranked results over lower-ranked results. Research shows these practices could have a significant impact on the users' decision-making processes, including among undecided voters, showing that they can lead to shifts in voting preferences by 20 per cent or more.

[...]

Microtargeting

73. Microtargeting is the use of (often large volumes of) personal data gathered from digital footprints to tailor what individuals or small groups see online. While traditional advertising is mainly informative, modern advertising draws on techniques such as microtargeting and advances in behavioural sciences to examine links between emotional responses and decision-making and play on subconscious desires [...]

(4.4.2.2) Mental integrity

Article 3 EU Charter – Right to the integrity of the person

1. Everyone has the right to respect for his or her physical and mental integrity.
2. In the fields of medicine and biology, the following must be respected in particular:
a) the free and informed consent of the person concerned, according to the procedures laid down by law;
b) the prohibition of eugenic practices, in particular those aiming at the selection of persons;
c) the prohibition on making the human body and its parts as such a source of financial gain;
d) the prohibition of the reproductive cloning of human beings.

Article 5(1) Inter-American Convention on Human Rights

Every person has the right to have his physical, mental, and moral integrity respected.

(4.4.2.3) Human dignity and individual autonomy

Article 7 Framework Convention on AI, Human Rights, Democracy and the Rule of Law

Each Party shall adopt or maintain measures to respect human dignity and individual autonomy in relation to activities within the lifecycle of artificial intelligence systems.

(4.4.3) Prohibited AI Systems under EU Law

(4.4.3.1) Article 5(1)(a), (b) and (g) EU AI Act – Prohibited AI Practices

The following AI practices shall be prohibited:

(a) the placing on the market, the putting into service or the use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm;

(b) the placing on the market, the putting into service or the use of an AI system that exploits any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm;

[...]

(f) the placing on the market, the putting into service for this specific purpose, or the use of AI systems to infer emotions of a natural person in the areas of workplace and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons;

[...]

Further reading: Commission Guidelines on prohibited artificial intelligence practices established by the AI Act

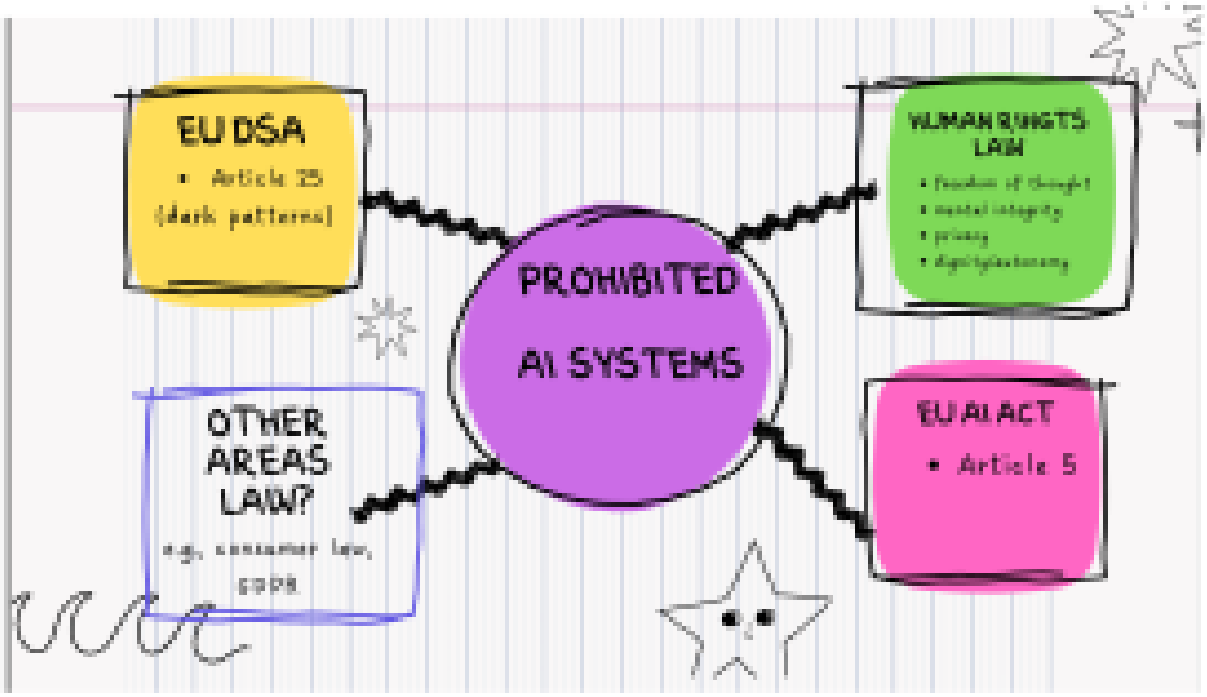
(4.4.3.2) Dark patterns under the Digital Services Act

Article 25(1) Digital Services Act – Online interface design and organisation

> Providers of online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions.

Recital 69, Digital Services Act

> When recipients of the service are presented with advertisements based on targeting techniques optimised to match their interests and potentially appeal to their vulnerabilities, this can have particularly serious negative effects. In certain cases, manipulative techniques can negatively impact entire groups and amplify societal harms, for example by contributing to disinformation campaigns or by discriminating against certain groups. Online platforms are particularly sensitive environments for such practices and they present a higher societal risk. Consequently, providers of online platforms should not present advertisements based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679, using special categories of personal data referred to in Article 9(1) of that Regulation, including by using profiling categories based on those special categories. [...]



Questions

1. The prohibition of AI systems provided in Article 5 the AI Act, includes extensive qualifiers in the text (e.g., *materially* distort, *appreciably* impair, *significant* harms) suggesting a high threshold set to distinguish lawful and legitimate techniques from unlawful, subliminal or purposefully manipulative or deceptive techniques. These qualifiers and other elements in these provisions are highly unclear, and it remains to be seen how they will be interpreted and applied considering how our understanding of the effects of the technologies evolves. Where would you draw the line between lawful/legitimate techniques of influence from unlawful, manipulative or deceptive techniques?
2. The AI Convention is criticised for leaving discretion to State parties to assess the need for banning certain AI systems and for not providing clear criteria to this end (Article 16(4)). Why do you think the AI Convention is silent in this regard?
3. How would you assess the human rights law's potential to capture novel harms stemming from emotion detection and manipulation and exploitation of human vulnerabilities? What

are the rights that may be relevant?

Further readings/resources

- Have a look at the work of the UN Special Rapporteur on freedom of opinion and expression, including the annual thematic reports.
- For a **gender perspective on disinformation** and its implications for the right to freedom of expression, read this report by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc A/78/288, 7 August 2023
- For a discussion of **global threats to freedom of expression arising from the conflict in Gaza**, read this report by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc A/79/319, 23 August 2024
- JP Quintais et al, 'Using Terms and Conditions to apply Fundamental Rights to Content Moderation' (2023) 24 German Law Journal 881
- LR Helfer, & MK Land, '*The Meta Oversight Board's Human Rights Future*' (2023) 44 Cardozo Law Review 2233
- LG Loucaides, 'The Right to Freedom of Thought as Protected by the European Convention on Human Rights' (2012) 1 Cyprus Human Rights Law Review 79
- S Ligthart and others, 'Rethinking the Right to Freedom of Thought: A Multidisciplinary Analysis' (2022) 22 Human Rights Law Review
- D Susser & L Cabrera, 'Brain data in context: are new rights the way to mental and brain privacy?' (2023) 15 AJOB Neuroscience 122
- S. McCarthy-Jones, 'The Autonomous Mind: The Right to Freedom of Thought in the Twenty-First Century' (2019) Frontiers in Artificial Intelligence

5. RIGHT TO BE FREE FROM DISCRIMINATION

Outline of the chapter

This chapter explains the applicability and scope of protection of the right to be free from discrimination. It then proceeds to unpack the relevance and application of the right to AI systems and decision-making processes. More specifically, this chapter addresses:

- the relevant law concerning the right to be free from discrimination (section 5.1)
- the protective scope of non-discrimination (section 5.2)
- the challenges that AI systems bring to conceptualising, detecting and substantiating discriminatory harms and risks (section 5.3)
- States' obligations under the right to be free from discrimination (section 5.4)
- corporations' duties under the right to be free from discrimination (section 5.5)

(5.1) Relevant law

(5.1.1) General clauses on equality and non-discrimination

(5.1.1.1) International Covenant on Civil and Political Rights

Article 2(1)

Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

Article 26

All persons are equal before the law and are entitled without any discrimination to the equal protection of

the law. In this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

(5.1.1.2) Article 14 European Convention on Human Rights – Prohibition of discrimination

The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

(5.1.1.3) Article 1 Additional Protocol 12 to the ECHR – General prohibition of discrimination

1 The enjoyment of any right set forth by law shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

2 No one shall be discriminated against by any public authority on any ground such as those mentioned in paragraph 1.

(5.1.1.4) Article 21 EU Charter on Fundamental Rights – Non-discrimination

1. Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.

2. Within the scope of application of the Treaties and without prejudice to any of their specific provisions, any discrimination on grounds of nationality shall be prohibited.

(5.1.2) Specialised treaties

(5.1.2.1) International Convention on the Elimination of All Forms of Racial Discrimination

Article 1(1)

In this Convention, the term "racial discrimination" shall mean any distinction, exclusion, restriction or preference based on race, colour, descent, or national or ethnic origin which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise, on an equal footing, of human rights and fundamental freedoms in the political, economic, social, cultural or any other field of public life

Article 2

1. States Parties condemn racial discrimination and undertake to pursue by all appropriate means and without delay a policy of eliminating racial discrimination in all its forms and promoting understanding among all races, and, to this end:

(a) Each State Party undertakes to engage in no act or practice of racial discrimination against persons, groups

of persons or institutions and to en sure that all public authorities and public institutions, national and local, shall act in conformity with this obligation;

(b) Each State Party undertakes not to sponsor, defend or support racial discrimination by any persons or organizations;

(c) Each State Party shall take effective measures to review governmental, national and local policies, and to amend, rescind or nullify any laws and regulations which have the effect of creating or perpetuating racial discrimination wherever it exists;

(d) Each State Party shall prohibit and bring to an end, by all appropriate means, including legislation as required by circumstances, racial discrimination by any persons, group or organization;

(e) Each State Party undertakes to encourage, where appropriate, integrationist multiracial organizations and movements and other means of eliminating barriers between races, and to discourage anything which tends to strengthen racial division.

(5.1.2.2) International Convention on the Elimination of All Forms of Discrimination Against Women

Article 2

States Parties condemn discrimination against women in all its forms, agree to pursue by all appropriate means and without delay a policy of eliminating discrimination against women and, to this end, undertake:

(a) To embody the principle of the equality of men and women in their national constitutions or other appropriate legislation if not yet incorporated therein and to ensure, through law and other appropriate means, the practical realization of this principle;

(b) To adopt appropriate legislative and other measures, including sanctions where appropriate, prohibiting all discrimination against women;

(c) To establish legal protection of the rights of women on an equal basis with men and to ensure through competent national tribunals and other public institutions the effective protection of women against any act of discrimination;

(d) To refrain from engaging in any act or practice of discrimination against women and to ensure that public authorities and institutions shall act in conformity with this obligation;

(e) To take all appropriate measures to eliminate discrimination against women by any person, organization or enterprise;

(f) To take all appropriate measures, including legislation, to modify or abolish existing laws, regulations, customs and practices which constitute discrimination against women;

(g) To repeal all national penal provisions which constitute discrimination against women.

(5.1.2.3) Article 10 Framework Convention on AI, Human Rights, Democracy and the Rule of Law – Equality and non-discrimination

1. Each Party shall adopt or maintain measures with a view to ensuring that activities within the lifecycle of artificial intelligence systems respect equality, including gender equality, and the prohibition of discrimination, as provided under applicable international and domestic law.

2. Each Party undertakes to adopt or maintain measures aimed at overcoming inequalities to achieve fair,

just and equitable outcomes, in line with its applicable domestic and international human rights obligations, in relation to activities within the lifecycle of artificial intelligence systems.

(5.2) Protective Scope of the Right to be Free from Discrimination

(5.2.1) A distinction does not constitute discrimination, if there are reasonable and objective reasons

Discrimination in law is a difference in treatment based on the ground of a protected characteristic (e.g., race, colour, sex, language) as long as it is not justified by reasonable and objective reasons.

UN Human Rights Committee, General Comment No 18: Non-discrimination, UN Doc HRI/GEN/1/Rev.1 10 November 1989

> 7. [...] the term "discrimination" as used in the Covenant should be understood to imply any distinction, exclusion, restriction or preference which is based on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status, and which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise by all persons, on an equal footing, of all rights and freedoms.
>
> [...]
>
> 13. [....] not every differentiation of treatment will constitute discrimination, if the criteria for such differentiation are reasonable and objective and if the aim is to achieve a purpose which is legitimate under the Covenant.

(5.2.2) Applying the definition of discrimination

ECtHR, Schalk and Kopf v Austria, App no 30141/04, 24 June 2010

> 96. The Court has established in its case-law that in order for an issue to arise under Article 14 there must be a difference in treatment of persons in relevantly similar situations. Such a difference of treatment is discriminatory if it has no objective and reasonable justification; in other words, if it does not pursue a legitimate aim or if there is not a reasonable relationship of proportionality between the means employed and the aim sought to be realised. The Contracting States enjoy a margin of appreciation in assessing whether and to what extent differences in otherwise similar situations justify a difference in treatment [...].
>
> 97. On the one hand, the Court has held repeatedly that, just like differences based on sex, differences based on sexual orientation require particularly serious reasons by way of justification [...]. On the other hand, a wide margin of appreciation is usually allowed to the State under the Convention when it comes to general measures of economic or social strategy [....].
>
> 98. The scope of the margin of appreciation will vary according to the circumstances, the subject matter and

its background; in this respect, one of the relevant factors may be the existence or non-existence of common ground between the laws of the Contracting States [...].

(5.2.3) Difference between direct and indirect discrimination

ECtHR, D.H. and Others v. the Czech Republic, app no. 57325/00, 13 November 2007 (Grand Chamber)

175. [...] discrimination means treating differently, without an objective and reasonable justification, persons in relevantly similar situations [...] The Court has also accepted that a general policy or measure that has disproportionately prejudicial effects on a particular group may be considered discriminatory notwithstanding that it is not specifically aimed at that group [...], and that discrimination potentially contrary to the Convention may result from a de facto situation [...]

(5.2.4) The special function of Article 14 ECHR: not a self-standing provision

ECtHR, Schalk and Kopf v Austria, App no 30141/04, 24 June 2010

89. As the Court has consistently held, Article 14 complements the other substantive provisions of the Convention and its Protocols. It has no independent existence since it has effect solely in relation to "the enjoyment of the rights and freedoms" safeguarded by those provisions. Although the application of Article 14 does not presuppose a breach of those provisions – and to this extent it is autonomous –, there can be no room for its application unless the facts at issue fall within the ambit of one or more of the latter [...].

[...]

However, Article 1 of Additional Protocol 12 to the ECHR creates a general prohibition of discrimination that functions independently of the applicability of other ECHR rights. Therefore, individuals may claim a violation of Article 1 of Additional Protocol 12 to the ECHR as a self-standing provision. This concerns only States that have signed and ratified Additional Protocol 12 (for details on those states see here).

(5.2.5) Who proves what and how? Burden of proof and evidentiary means in cases of discrimination

ECtHR, D.H. and Others v. the Czech Republic, app no. 57325/00, 13 November 2007 (Grand Chamber)

177. As to the burden of proof [in cases of alleged discrimination], the Court has established that once the applicant has shown a difference in treatment, it is for the Government to show that it was justified [...]

178. As regards the question of what constitutes prima facie evidence capable of shifting the burden of proof on to the respondent State, the Court stated in Nachova and Others [...] that in proceedings before it there are no procedural barriers to the admissibility of evidence or pre-determined formulae for its assessment. The Court adopts the conclusions that are, in its view, supported by the free evaluation of all evidence, including such inferences as may flow from the facts and the parties' submissions. According to its established case-law, proof may follow from the coexistence of sufficiently strong, clear and concordant inferences or of similar unrebutted presumptions of fact. Moreover, the level of persuasion necessary for reaching a particular conclusion and, in

this connection, the distribution of the burden of proof are intrinsically linked to the specificity of the facts, the nature of the allegation made and the Convention right at stake.

179. The Court has also recognised that Convention proceedings do not in all cases lend themselves to a rigorous application of the principle affirmanti incumbit probatio [he who alleges something must prove that allegation] [...]. In certain circumstances, where the events in issue lie wholly, or in large part, within the exclusive knowledge of the authorities, the burden of proof may be regarded as resting on the authorities to provide a satisfactory and convincing explanation [...]. In Nachova and Others, the Court did not rule out requiring a respondent Government to disprove an arguable allegation of discrimination in certain cases, even though it considered that it would be difficult to do so in that particular case, in which the allegation was that an act of violence had been motivated by racial prejudice. It noted in that connection that in the legal systems of many countries proof of the discriminatory effect of a policy, decision or practice would dispense with the need to prove intent in respect of alleged discrimination in employment or in the provision of services.

180. As to whether statistics can constitute evidence, the Court has in the past stated that statistics could not in themselves disclose a practice which could be classified as discriminatory [...]. However, in more recent cases on the question of discrimination in which the applicants alleged a difference in the effect of a general measure or de facto situation [...], the Court relied extensively on statistics produced by the parties to establish a difference in treatment between two groups (men and women) in similar situations.

(5.2.6) Horizontal application of EU Directives and Article 21 EU Charter on Fundamental Rights

Xenidis, 'Article 21. An Exploration, or the Right to Algorithmic Non-Discrimination', in Alexandra Giannopoulou (ed), Digital Rights Are Charter Rights: Essay Series (Digital Freedom Fund & DitiRISE, 2023) 22, 23

[...] Due to the scope of the [EU Charter on Fundamental Rights], as expressed in Article 51(1), the prohibition of discriminations applies to 'the institutions [and] bodies [...] of the Union' as well as 'the Member States only when they are implementing Union law'. Hence, the EU has a comprehensive obligation to refrain from any form of discrimination based on all grounds listed in Article 21. For instance, this implies that Frontex, an EU agency, cannot utilize border control software that discriminates against individuals based on factors like skin colour, ethnic origin or language.

The obligations for member States, however, is more limited: the non-discrimination clause contained in Article 21 only applies when there is a 'direct link' with EU law. Within the material scope of the EU's four anti-discrimination directives (Directives 2000/43/EC, 2000/78/EC, 20004/113/EC and 2006/54/EC), EU secondary law provisions prohibit discrimination on grounds of sex or gender, race or ethnic origin, sexual orientation, disability, religion or belief and age. Article 21 of the Charter, embodying the general principle of equal treatment, applies within the specific framework defined by these Directives. Yet, where the Directives cannot, in principle, apply directly to private parties, the Court of Justice of the European Union has recognised horizontal direct effects to Article 21 of the Charter. [...]

In scenarios where the situation falls outside the scope of EU secondary law but maintains a direct link with EU law, Article 21 operates in a subsidiary manner.

(5.3) Discrimination Concerns in AI Systems

Watch the video on How AI is defining our bodies, by Access Now

One or more interactive elements has been excluded from this version of the text. You can view them online here: https://opentextbooks.rug.nl/dataprotectionanddigitalhumanrights/?p=38#oembed-1

General Recommendation No. 36 (2020) of the Committee on the Elimination of Racial Discrimination on preventing and combating racial profiling by law enforcement officials, UN Doc CERD/C/GC/36, 17 December 2020

> 33. Particular risks emerge when algorithmic profiling is used for determining the likelihood of criminal activity either in certain localities, or by certain groups or even individuals. Predictive policing that relies on historical data for predicting possible future events can easily produce discriminatory outcomes, in particular when the datasets used suffer from one or more of the flaws described above. For example, historical arrest data about a neighbourhood may reflect racially biased policing practices. If fed into a predictive policing model, use of these data poses a risk of steering future predictions in the same, biased direction, leading to overpolicing of the same neighbourhood, which in turn may lead to more arrests in that neighbourhood, creating a dangerous feedback loop.
>
> 34. Similar mechanisms have been reported to be present in judicial systems. When applying a sanction, or deciding whether someone should be sent to prison, be released on bail or receive another punishment, States are increasingly resorting to the use of algorithmic profiling, in order to foresee the possibilities that an individual may commit one or several crimes in the future. Authorities gather information regarding the criminal history of the individual, their family and their friends and their social conditions, including their work and academic history, in order to assess the degree of "danger" posed by the person from a score provided by the algorithm, which usually remains secret. [...]

(5.3.1) Bias in AI systems

(5.3.1.1) How does bias enter AI systems?

Centre for Data Ethics and Innovation, Review into bias in algorithmic decision-making, November 2020, 26

> Bias can enter algorithmic decision-making systems in a number of ways, including:

- **Historical bias**: The data that the model is built, tested and operated on could introduce bias. This may be because of previously biased human decision-making or due to societal or historical inequalities. For example, if [...] your criminal record is in part a result of how likely you are to be arrested (as compared to someone else with the same history of behaviour, but not arrests), an algorithm constructed to assess risk of reoffending is at risk of not reflecting the true likelihood of reoffending, but instead reflects the more biased likelihood of being caught reoffending.
- **Data selection bias**: How the data is collected and selected could mean it is not representative. [...] This has been the main cause of some of the widely reported problems with accuracy of some facial recognition algorithms across different ethnic groups, with attempts to address this focusing on ensuring a better balance in training data.
- **Algorithmic design bias**: It may also be that the design of the algorithm leads to introduction of bias. [...]
- **Human oversight** is widely considered to be a good thing when algorithms are making decisions, and mitigates the risk that purely algorithmic processes cannot apply human judgement to deal with unfamiliar situations. However depending on how humans interpret or use the outputs of an algorithm, there is also a risk that bias re-enters the process as the human applies their own conscious or unconscious biases to the final decision

There is also risk that bias can be amplified over time by feedback loops, as models are incrementally re-trained on new data generated, either fully or partly, via use of earlier versions of the model in decision-making. For example, if a model predicting crime rates based on historical arrest data is used to prioritise police resources, then arrests in high risk areas could increase further, reinforcing the imbalance. [...]

(5.3.1.2) Does discrimination in law capture unfair bias in AI systems?

Centre for Data Ethics and Innovation, Review into bias in algorithmic decision-making, November 2020, 28

Discrimination is a narrower concept than bias. Protected characteristics have been included in law due to historical evidence of systematic unfair treatment, but individuals can also experience unfair treatment on the basis of other characteristics that are not protected.

[...]

Algorithmic decision-making can also go beyond amplifying existing biases, to creating new biases that may be unfair, though difficult to address through discrimination law. This is because machine learning algorithms find new statistical relationships, without necessarily considering whether the basis for those relationships is fair, and then apply this systematically in large numbers of individual decisions.

Examples of non-protected characteristics

Individuals and/or groups may be discriminated based on characteristics not protected in law (e.g., socio-economic status). Moreover, data may encompass proxy information (e.g., postal

codes) indirectly indicating race or ethnic origin. Many times, the use of AI systems results in discriminatory practices not by using a prohibited category as a variable but through proxies and correlations established in the content of data and this very difficult, if not impossible, to trace back or review. A characteristic example of how training data sets and input data can lead to discrimination against individuals and groups comes from predictive policing. Predictive policing consists of AI systems pulling from multiple sources of data, such as criminal records, crime statistics and the demographics of neighbourhoods, for determining the likelihood of criminal activity. Reliance upon historical arrest data about a neighbourhood may reflect racially biased policing practices and, therefore, reproduce and reinforce biases and aggravate or lead to discrimination. In practice, this may result in over-policing of the same neighbourhood, which in turn leads to more arrests creating a dangerous feedback loop.

Example of new types of discriminatory harms

AI systems also create novel group discriminatory harms. For instance, when clustering algorithms profile and categorise individuals, they tend to discriminate against groups of individuals who display similar behavioural patterns. Group harms also relate to groups of people with shared backgrounds (e.g., income, residence, race, gender, nationality). In these instances, both individuals and groups have great difficulty to be identified as victims, not to mention that they may not be aware of the harms involved.

(5.3.2) Algorithmic opacity as a barrier to detecting and contesting discriminatory outcomes

Algorithmic opacity creates many challenges for detecting discriminatory and human rights harms and substantiating respective claims. Algorithmic opacity can be unintentional or intentional.

(5.3.2.1) Unintentional algorithmic opacity

Unintentional algorithmic opacity concerns the complexity of technological systems and the different ways in which bias can be ingrained into these systems. It was explained earlier how bias creeps in various – many times invisible – ways into AI systems. The so-called "black box"- namely the complexity of AI systems and our limited ability to understand how and why they reach certain outcomes – merits some explanation.

Explaining the black box of deep learning

Watch AI detectives are cracking open the black box of deep learning, by Science Magazine



One or more interactive elements has been excluded from this version of the text. You can view them online here: https://opentextbooks.rug.nl/dataprotectionanddigitalhumanrights/?p=38#oembed-2

(5.3.2.2) Intentional algorithmic opacity

Algorithmic opacity may be intentional too. It is common for AI systems that are developed by the private sector and deployed in the private or public sector to be shielded from scrutiny. This is due to restrictions imposed by contracts, intellectual property laws or technical measures.

(5.3.2.2.1) Intentional algorithmic opacity and IP interests

In *State* v. *Loomis* the Supreme Court of Wisconsin ruled for the first time on the constitutionality of the use of AI in sentencing. The case concerned the use of a risk assessment tool – COMPAS – to predict an individual's risk of recidivism. Loomis argued that the circuit court's use of a COMPAS risk assessment violated a defendant's right to due process for three reasons: (1) it violated a defendant's right to be sentenced based upon accurate information, in part because the proprietary nature of COMPAS prevents him from assessing its accuracy; (2) it violated a defendant's right to an individualised sentence; and (3) it improperly used gendered assessments in sentencing. The Supreme Court dismissed his arguments holding that the accuracy of the tools and the capacity of the judges to understand possible malfunctioning were adequate.

USA, Supreme Court of Wisconsin, State v. Loomis, 881, N.W.2d 749, 7532 (Wis, 2016)

> 35. Although we ultimately conclude that a COMPAS risk assessment can be used at sentencing, we do so by circumscribing its use. Importantly, we address how it can be used and what limitations and cautions a circuit court must observe in order to avoid potential due process violations.
>
> [...]
>
> 42. In response to a call to reduce recidivism by employing evidence-based practices, several states have passed legislation requiring that judges be provided with risk assessments and recidivism data at sentencing. Other states permit, but do not mandate, the use of risk assessment tools at sentencing.
>
> 43. But other voices are challenging the efficacy of evidence-based sentencing and raise concern about overselling the results. They urge that judges be made aware of the limitations of risk assessment tools, lest they be misused: "In the main, [supporters] have been reticent to acknowledge the paucity of reliable evidence

that now exists, and the limits of the interventions about which we do possess evidence. Unless criminal justice system actors are made fully aware of the limits of the tools they are being asked to implement, they are likely to misuse them"; Cecelia Klingele, The Promises and Perils of Evidence-Based Corrections, 91 Notre Dame L. Rev. 537, 576 (2015).

44. We heed this admonition. The DOC already recognizes limitations on the PSI, instructing that "[i]t is very important to remember that risk scores are not intended to determine the severity of the sentence or whether an offender is incarcerated." We are in accord with these limitations. Further, we set forth the corollary limitation that risk scores may not be considered as the determinative factor in deciding whether the offender can be supervised safely and effectively in the community.

[...]

62. [...] there is concern that risk assessment tools may disproportionately classify minority offenders as higher risk, often due to factors that may be outside their control, such as familial background and education. Other state studies indicate that COMPAS is more predictive of recidivism among white offenders than black offenders.

64. Additional concerns are raised about the need to closely monitor risk assessment tools for accuracy [...]

65. Focusing exclusively on its use at sentencing and considering the expressed due process arguments regarding accuracy, we determine that use of a COMPAS risk assessment must be subject to certain cautions in addition to the limitations set forth herein.

66. Specifically, any [Presentence Investigation Report] containing a COMPAS risk assessment must inform the sentencing court about the following cautions regarding a COMPAS risk assessment's accuracy: (1) the proprietary nature of COMPAS has been invoked to prevent disclosure of information relating to how factors are weighed or how risk scores are to be determined; (2) risk assessment compares defendants to a national sample, but no cross-validation study for a Wisconsin population has yet been completed; (3) some studies of COMPAS risk assessment scores have raised questions about whether they disproportionately classify minority offenders as having a higher risk of recidivism; and (4) risk assessment tools must be constantly monitored and re-normed for accuracy due to changing populations and subpopulations. Providing information to sentencing courts on the limitation and cautions attendant with the use of COMPAS risk assessment will enable courts to better assess the accuracy of the assessment and the appropriate weight to be given to the risk score.

Question:

Do you find the court's reasoning and outcome convincing? Do you think that the court's cautions (para 66) address the concerns raised by Loomis?

(5.3.2.2.2) Intentional algorithmic opacity and "gaming the system"

States may also refuse to reveal details about AI systems used in the public sector invoking, or under the

pretext, that individuals will "game the system". This was the case in *SyRI*: The Netherlands refused to reveal before the court more details on how the AI system functioned.

In the *SyRI* case, the applicants challenged the Dutch government's use of System Risk Indication (SyRI)—an algorithm designed to predict social welfare fraud. The applicants argued that SyRI's use was in violation of the right to privacy, data protection and the principle of non-discrimination.

District Court of The Hague, NCJM et al. and FNV v The State of the Netherlands, 6 March 2020

> 6.49 The court finds that it is unable to assess the correctness of the position of the State of the precise nature of SyRI because the State has not disclosed the risk model and the indicators of which the risk model is composed or may be composed. In these proceedings the State has also not provided the court with objectively verifiable information to enable the court to assess the viewpoint of the State on the nature of SyRI. The reason the State gives for this is that citizens could then adjust their conduct accordingly. This is a deliberate choice of the State. That choice also coincides with the starting point of the legislator regarding the provision of information on SyRI. The SyRI legislation does not show how the decision model of SyRI functions and which indicators are or can be used in a SyRI project [...], i.e. which factual data make or can make the presence of a certain situation plausible.

(5.3.2.2.3) The need for transparency and scrutiny

Netherlands Institute for Human Rights, Transparent Use of Algorithms by the Government, 29 June 2023, 9-10

> Objections to the obligation of transparency
>
> [...]
>
> Objection 2: Secrecy required in risk selection
>
> Administrative bodies in charge of enforcement and detecting fraud or the abuse of schemes benefit from a degree of secrecy. For example, the Tax and Customs Administration has to choose from nearly 10 million income tax returns each year with regard to its inspections. In such circumstances, is a government entitled to keep selection criteria used by its algorithm secret, in order to prevent calculating citizens from anticipating these criteria in order to avoid an inspection?
>
> The phenomenon of citizens tailoring their behaviour to known or public detection criteria is referred to as the problem of 'gaming the system'. [...]
>
> First of all, it is useful to mention that in practice, transparency need not be completely ignored for detection methods and fraud detection. By not naming the exact values of criteria used in calculations, but explaining in comprehensible language how they came to a suspicion of fraud, partial transparency can often be achieved without objection.
>
> At the same time, the need for the secrecy of detection methods – in the broad sense – is understandable. However, the Institute sees a dilemma here. Fraud detection algorithms in particular are susceptible to highly damaging and far-reaching stigmatising forms of discrimination. Although risk selection algorithms only involve further inspection and not a sanction at that point, selective controls for suspicious characteristics such as a migration background have a highly stigmatising effect.
>
> That effect is self-reinforcing, as an algorithm that selectively searches more intensively than average on the basis of bias will also find more cases of fraud [...]. Therefore, when Dutch administrative bodies choose to

exempt detection algorithms (in part) from an obligation of transparency, the related monitoring will have to be organised through other, thorough and prudent methods.

In such cases, the Institute considers it necessary to carry out mandatory and independent verification beforehand. Algorithms for which the confidentiality of (some) test and selection elements is desired should be submitted to a body qualified to handle this matter. Until authorisation has been given, detection algorithms with secret elements must not be put into use.

Since the choice of these types of elements in algorithms can be dynamic, the possibility of subjecting these algorithms to periodic retesting should also be implemented.

(5.3.3) Evidence and burden of proof: detecting and contesting discriminatory harms

(5.3.3.1) Evidence and burden of proof in absence of sufficient information on AI systems: State obligation to put safeguards in place to neutralise the risk of discriminatory effects

District Court of The Hague, NCJM et al. and FNV v The State of the Netherlands, 6 March 2020

6.92 NJCM et al., in these proceedings also supported by FNV and the UN Special Rapporteur on extreme poverty and human rights, has explained extensively that it believes that the use of SyRI has a discriminatory and stigmatising effect. NJCM et al. notes that SyRI is used to further investigate neighbourhoods that are known as problem areas. This increases the chances of discovering irregularities in such areas as compared to other neighbourhoods, which in turn confirms the image of a neighbourhood as a problem area, contributes to stereotyping and reinforces a negative image of the occupants of such neighbourhoods, even if no risk reports have been generated about them.

6.93 It is correct that to date SyRI has only been applied to so-labelled 'problem districts', as confirmed by the State at the hearing. This in and of itself need not imply that such use is disproportionate or otherwise contrary to Article 8 paragraph 2 ECHR in all cases. However, given the large amounts of data that qualify for processing in SyRI, including special personal data, and the circumstance that risk profiles are used, there is in fact a risk that SyRI inadvertently creates links based on bias, such as a lower socio-economic status or an immigration background, as NJCM et al. argue.

6.94 Based on the SyRI legislation, it cannot be assessed whether this risk is sufficiently neutralised due to the absence of a verifiable insight into the risk indicators and the risk model as well as the functioning of the risk model, including the analysis method applied by the Social Affairs and Employment Inspectorate. The circumstance that the process of data processing consists of two phases and that the analysis unit of the Social Affairs and Employment Inspectorate, following a link of the files by the IB, assesses the decrypted data on their worthiness of investigation, which includes a human check for false positives and false negatives, is deemed insufficient by the court. After all, the manner in which the definitive risk selection takes place is not public. Nor are the data subjects informed about how the definitive risk selection is effectuated or about the associated conclusion whether or not a risk report is submitted, while the SyRI legislation only provides for a general monitoring by the AP afterwards.

6.95 In view of the foregoing, the court is of the opinion that the SyRI legislation contains insufficient safeguards to protect the right to respect for private life in relation to the risk indicators and the risk model which can be used in a concrete SyRI project. [...]

(5.3.3.2) Burden of proof lies with the State to dispel suspicion of discriminatory effects?

Brief by the United Nations Special Rapporteur on extreme poverty and human rights as Amicus Curiae in the case of NJCM c.s./De Staat der Nederlanden (SyRI) before the District Court of The Hague

> 37. In the context of an appropriately demanding proportionality assessment, the Special Rapporteur believes the burden of proof lies with the government to provide evidence that dispels the suspicion that the singular focus of SyRI on poor and marginalised groups in Dutch society is justified in light of available government statistics. An important test in this regard would be whether similar levels of intrusiveness that are evident in the context of the SyRI system would also be considered acceptable if well-off areas and groups were involved instead of poor ones. These considerations affect the proportionality assessment in this case, but are also relevant in light of an assessment of whether SyRI discriminates on prohibited grounds, including on the basis of race, colour, national or social origin, property or birth status.

(5.4) States' Obligations Ensuring that AI Systems Comply with the Prohibition of Discrimination

(5.4.1) Racial profiling

General Recommendation No. 36 (2020) of the Committee on the Elimination of Racial Discrimination on preventing and combating racial profiling by law enforcement officials, UN Doc CERD/C/GC/36, 17 December 2020

> 58. States should ensure that algorithmic profiling systems used for the purposes of law enforcement are in full compliance with international human rights law. To that effect, before procuring or deploying such systems States should adopt appropriate legislative, administrative and other measures to determine the purpose of their use and to regulate as accurately as possible the parameters and guarantees that prevent breaches of human rights. Such measures should, in particular, be aimed at ensuring that the deployment of algorithmic profiling systems does not undermine the right not to be discriminated against, the right to equality before the law, the right to liberty and security of person, the right to the presumption of innocence, the right to life, the right to privacy, freedom of movement, freedom of peaceful assembly and association, protections against arbitrary arrest and other interventions, and the right to an effective remedy.
>
> 59. States should carefully assess the potential human rights impact prior to employing facial recognition technology, which can lead to misidentification owing to a lack of representation in data collection [...]
>
> 60. States should ensure that algorithmic profiling systems deployed for law enforcement purposes are designed for transparency, and should allow researchers and civil society to access the code and subject it to scrutiny. There should be continual assessment and monitoring of the human rights impact of those systems throughout their life cycle, and States should take appropriate mitigation measures if risks or harms to human rights are identified. [...] Such processes should include community impact assessments. Groups that are potentially or actually affected and relevant experts should be included in the assessment and mitigation processes.
>
> 61. States should take all appropriate measures to ensure transparency in the use of algorithmic profiling systems. This includes public disclosure of the use of such systems and meaningful explanations of the ways

in which the systems work, the data sets that are being used, and the measures in place to prevent or mitigate human rights harms. States should adopt measures to ensure that independent oversight bodies have a mandate to monitor the use of artificial intelligence tools by the public sector, and to assess them against criteria developed in conformity with the [CERD] to ensure they are not entrenching inequalities or producing discriminatory results [...]

(5.4.2) Public authorities have the positive duty to do all that they reasonably can to ensure that an AI system does not have an inbuilt racial or gender bias

R (on the application of Edward Bridges) v. Chief Constable of S. Wales Police [2020] EWCA Civ 1058 (Ed Bridges)

1. This appeal concerns the lawfulness of the use of live automated facial recognition technology ("AFR") by the South Wales Police Force [...] in an ongoing trial using a system called AFR Locate. AFR Locate involves the deployment of surveillance cameras to capture digital images of members of the public, which are then processed and compared with digital images of persons on a watchlist compiled by the South Wales Police Force for the purpose of the deployment. On the facts of the present case, AFR Locate has been used in an overt manner. [...]

2. [...] The grounds of challenge were that AFR is not compatible with the right to respect for private life under Article 8 of the European Convention on Human Rights ("the Convention"), which is one of the Convention rights set out in Sch.1 to the Human Rights Act 1998 ("HRA"); data protection legislation; and the Public Sector Equality Duty [...] in section 149 of the Equality Act 2010.

[...]

Ground 5: Public Sector Equality Duty

181. We acknowledge that what is required by the Public Sector Equality Duty is dependent on the context and does not require the impossible. It requires the taking of reasonable steps to make enquiries about what may not yet be known to a public authority about the potential impact of a proposed decision or policy on people with the relevant characteristics, in particular for present purposes race and sex.

182. We also acknowledge that, as the Divisional Court found, there was no evidence before it that there is any reason to think that the particular AFR technology used in this case did have any bias on racial or gender grounds. That, however, it seems to us, was to put the cart before the horse. The whole purpose of the positive duty (as opposed to the negative duties in the Equality Act 2010) is to ensure that a public authority does not inadvertently overlook information which it should take into account.

[...]

191. In our view, this does not constitute a sufficient answer to the challenge based on the Public Sector Equality Duty. As Mr Squires submitted, Mr Edgell was dealing with a different set of statistics. He did not know, for obvious reasons, the racial or gender profiles of the total number of people who were captured by the AFR technology but whose data was then almost immediately deleted. In order to check the racial or gender bias in the technology, that information would have to be known. We accept Mr Beer's submission that it is impossible to have that information, precisely because a safeguard in the present arrangements is that that data is deleted in the vast majority of cases. That does not mean, however, that the software may not have an inbuilt bias, which needs to be tested. In any event, with respect to Mr Edgell, he is not an expert who can deal with the technical aspects of the software in this context.

[...]

200. Finally, we would note that the Divisional Court placed emphasis on the fact that the South Wales Police

> Force continue to review events against the section 149(1) criteria. It said that this is the approach required by the Public Sector Equality Duty in the context of a trial process. With respect, we do not regard that proposition to be correct in law. The Public Sector Equality Duty does not differ according to whether something is a trial process or not. If anything, it could be said that, before or during the course of a trial, it is all the more important for a public authority to acquire relevant information in order to conform to the Public Sector Equality Duty and, in particular, to avoid indirect discrimination on racial or gender grounds.
>
> 201. In all the circumstances, therefore, we have reached the conclusion that the South Wales Police Force have not done all that they reasonably could to fulfil the Public Sector Equality Duty. We would hope that, as AFR is a novel and controversial technology, all police forces that intend to use it in the future would wish to satisfy themselves that everything reasonable which could be done had been done in order to make sure that the software used does not have a racial or gender bias.

(5.4.3) States' obligations in connection to corporations' activities

Report of the Special Rapporteur, E. Tendayi Achiume, on contemporary forms of racism, racial discrimination, xenophobia, and related intolerance, Racial discrimination and emerging digital technologies: a human rights analysis UN Doc A/HRC/44/57, 18 June 2020

> 59. Although international human rights law is only directly legally binding on States, in order to discharge their legal obligations in this regard, States are required to ensure effective remedies for racial discrimination attributable to private actors, including corporations. Under the International Convention on the Elimination of All Forms of Racial Discrimination, States must enact special measures to achieve and protect racial equality throughout the public and private spheres. This should include close regulatory oversight of companies involved in emerging digital technologies.
>
> 60. States must ensure that human rights ethical frameworks for corporations involved in emerging digital technologies are linked with and informed by binding international human rights law obligations, including on equality and non-discrimination. There is a genuine risk that corporations will reference human rights liberally for the public relations benefits of being seen to be ethical, even in the absence of meaningful interventions to operationalize human rights principles. Although references to human rights, and even to equality and non-discrimination, proliferate in corporate governance documents, these references alone do not ensure accountability. Similarly, implementation of the framework of Guiding Principles on Business and Human Rights, including through initiatives such as the B-Tech Project, must incorporate legally binding obligations to prohibit – and provide effective remedies for – racial discrimination.

(5.5) Corporations' Duties Ensuring that AI Systems Comply with the Prohibition of Discrimination

(5.5.1) Racial profiling

General Recommendation No. 36 (2020) of the Committee on the Elimination of Racial Discrimination on preventing and combating racial profiling by law enforcement officials, UN Doc CERD/C/GC/36, 17 December 2020

64. [...] private business enterprises [...], in the process of developing, learning, marketing and using algorithms: (a) comply with the principle of equality and non-discrimination, and respect human rights in general, in line with the Guiding Principles on Business and Human Rights (in particular guiding principles 1–3, 11 and 24); (b) respect the precautionary principle and any administrative or legislative measure enacted to ensure transparency; (c) disclose publicly whether law enforcement has access to private data on individuals; and (d) avoid causing disparate or disproportionate impact on the social groups protected by the [CERD].

[...]

66. [...] companies that are developing, selling or operating algorithmic profiling systems for law enforcement purposes have a responsibility to involve individuals from multiple disciplines, such as sociology, political science, computer science and law, to define the risks to, and ensure respect for, human rights [...]

67. In the process of identifying, assessing, preventing and mitigating adverse human rights impacts, companies should pay particular attention to the data-related factors [...]. Training data should be selected, and models designed, so as to prevent discriminatory outcomes and other adverse impacts on human rights. Moreover, companies should pursue diversity, equity and other means of inclusion in the teams developing algorithmic profiling systems. Companies should also be open to independent third-party audits of their algorithmic profiling systems. Where the risk of discrimination or other human rights violations has been assessed to be too high or impossible to mitigate, including because of the nature of a planned or foreseeable use by a State, private sector actors should not sell or deploy an algorithmic profiling system.

Questions

1. Why discrimination in law does not capture unfair bias in AI systems?
2. Can you think of arguments and solutions for mitigating intentional algorithmic opacity?
3. According to Recommendation No 36(2020) by the UN CERD Committee, the processes of identifying, assessing, monitoring and mitigating human rights impacts of AI systems throughout their life cycle should include community impact assessments. What are community impact assessments and why they are important?

Exercise: States should ensure that AI systems are designed for transparency and subject to

external scrutiny. What specific measures need to be taken and what stakeholders should be involved?

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://opentextbooks.rug.nl/dataprotectionanddigitalhumanrights/?p=38#h5p-17



(5.5.2) Case study: Intersectionality and gender identity

(5.5.2.1) How does automated gender classification contribute to gender identity?

Theilen, 'Article 20. Digital Inequalities and the Promise of Equality before the Law', in Giannopoulou (ed), Digital Rights Are Charter Rights: Essay Series (Digital Freedom Fund & DitiRISE, 2023) 18, 20

> While legal doctrine sees [intersectionality analysis] as subsidiary to more specific non-discrimination clauses, the promise of equality for 'everyone' in Article 20 of the Charter [of Fundamental Rights] should serve as a reminder that discrimination cannot be siloed into separate grounds of discrimination but must be considered holistically.
>
> [...]
>
> Automated gender classification contributes to normalising the idea that gender identity is readable from physical appearance and stands opposed to a self-determined gender identity – which many trans persons resists the technology as such, rather than focusing on reform to make it more inclusive.

(5.5.2.2) Disproportionate effects of content moderation and platform governance on the expressive rights of women and LGBTQI+ users

(5.5.2.2.1) Adult Nudity and Sexual Activity Community Standard, Meta Community Standards

> Do not post:
>
> Imagery of real nude adults, if it depicts:
>
> [...]
>
> Uncovered female nipples except in the context of breastfeeding, birth giving and after-birth moments, medical or health context (for example, post-mastectomy, breast cancer awareness or gender confirmation surgery) or an act of protest.

(5.5.2.2.2) META Oversight Board, Gender identity and nudity cases, 2022-009-IG-UA and 2022-010-IG-UA, 17 January 2023

> Case summary
>
> The Oversight Board has overturned Meta's original decisions to remove two Instagram posts depicting transgender and non-binary people with bare chests. It also recommends that Meta change its Adult Nudity and Sexual Activity Community Standard so that it is governed by clear criteria that respect international human rights standards.
>
> *About the case*
>
> In this decision, the Oversight Board considers two cases together for the first time. Two separate pieces of content were posted by the same Instagram account, one in 2021, the other in 2022. The account is maintained by a US-based couple who identify as transgender and non-binary.
>
> Both posts feature images of the couple bare-chested with the nipples covered. The image captions discuss transgender healthcare and say that one member of the couple will soon undergo top surgery (gender-affirming surgery to create a flatter chest), which the couple are fundraising to pay for.
>
> Following a series of alerts by Meta's automated systems and reports from users, the posts were reviewed multiple times for potential violations of various Community Standards. Meta ultimately removed both posts

for violating the Sexual Solicitation Community Standard, seemingly because they contain breasts and a link to a fundraising page.

The users appealed to Meta and then to the Board. After the Board accepted the cases, Meta found it had removed the posts in error and restored them.

Key findings

The Oversight Board finds that removing these posts is not in line with Meta's Community Standards, values or human rights responsibilities. These cases also highlight fundamental issues with Meta's policies.

Meta's internal guidance to moderators on when to remove content under the Sexual Solicitation policy is far broader than the stated rationale for the policy, or the publicly available guidance. This creates confusion for users and moderators and, as Meta has recognized, leads to content being wrongly removed.

In at least one of the cases, the post was sent for human review by an automated system trained to enforce the Adult Nudity and Sexual Activity Community Standard. This Standard prohibits images containing female nipples other than in specified circumstances, such as breastfeeding and gender confirmation surgery.

This policy is based on a binary view of gender and a distinction between male and female bodies. Such an approach makes it unclear how the rules apply to intersex, non-binary and transgender people, and requires reviewers to make rapid and subjective assessments of sex and gender, which is not practical when moderating content at scale.

The restrictions and exceptions to the rules on female nipples are extensive and confusing, particularly as they apply to transgender and non-binary people. Exceptions to the policy range from protests to scenes of childbirth, and medical and health contexts, including top surgery and breast cancer awareness. These exceptions are often convoluted and poorly defined. In some contexts, for example, moderators must assess the extent and nature of visible scarring to determine whether certain exceptions apply. The lack of clarity inherent in this policy creates uncertainty for users and reviewers, and makes it unworkable in practice.

The Board has consistently said Meta must be sensitive to how its policies impact people subject to discrimination [...]. Here, the Board finds that Meta's policies on adult nudity result in greater barriers to expression for women, trans, and gender non-binary people on its platforms. For example, they have a severe impact in contexts where women may traditionally go bare-chested, and people who identify as LGBTQI+ can be disproportionately affected, as these cases show. Meta's automated systems identified the content multiple times, despite it not violating Meta's policies.

Meta should seek to develop and implement policies that address all these concerns. It should change its approach to managing nudity on its platforms by defining clear criteria to govern the Adult Nudity and Sexual Activity policy, which ensure all users are treated in a manner consistent with human rights standards. It should also examine whether the Adult Nudity and Sexual Activity policy protects against non-consensual image sharing, and whether other policies need to be strengthened in this regard.

The Oversight Board's decision

The Oversight Board overturns Meta's original decision to remove the posts.

The Board also recommends that Meta:

- Define clear, objective, rights-respecting criteria to govern its Adult Nudity and Sexual Activity Community Standard, so that all people are treated in a manner consistent with international human rights standards, without discrimination on the basis of sex or gender. Meta should first conduct a comprehensive human rights impact assessment on such a change, engaging diverse stakeholders, and create a plan to address any harms identified.

- Provide more detail in its public-facing Sexual Solicitation Community Standard on the criteria that lead to content being removed.
- Revise its guidance for moderators on the Sexual Solicitation Community Standard so that it more accurately reflects the public rules on the policy. This would help to reduce enforcement errors on Meta's part.

Recommended reading: for those interested in reading the whole decision, please check here.

Further readings

- Lu, 'Regulating Algorithmic Harms', Florida Law Review (2025 forthcoming)
- Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics' (2017) 30 Philosophy & Technology 478
- Taylor, Floridi, van der Sloot (eds), Group Privacy: New Challenges of Data Technologies (Springer 2017)
- S Lilian Gössl, 'Recommender Systems and Discrimination', in S Genovesi, K Kaesling and S Robbins (eds), Recommender Systems: Legal and Ethical Issues (Springer 2023) 13

6. RIGHT TO A FAIR TRIAL

Outline of this chapter

This chapter examines the challenges of the nature of encrypted electronic data and its handling in criminal proceedings in light of the safeguards of the right to a fair trial. It also points to the ongoing question of criminalising one's refusal to disclose to the police the security code to unlock their mobile phone and whether this id in accordance with the right to remain silent and not to incriminate oneself. More specifically, this chapter highlights:

- the Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence (section 6.1.2)
- questions of evidence and quality of encrypted electronic data (section 6.2.2)
- the ability to verify the reliability and integrity of encrypted electronic evidence and challenge it in criminal proceedings in light of the principles of equality of arms and adversarial proceedings (section 6.2.3)
- the right to have adequate time and facilities for the preparation of one's defence (section 6.2.4)
- whether the rights to remain silent and not to incriminate oneself allow authorities to force suspects to unlock their electronic devices (section 6.3)

(6.1) Relevant law

(6.1.1) Article 6 ECHR – Right to a fair trial

1. In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all

or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.

1. Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.

3. Everyone charged with a criminal offence has the following minimum rights:

a) to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him;

b) to have adequate time and facilities for the preparation of his defence;

[...]

(6.1.2) States responding to novel challenges: enhanced co-operation and disclosure of electronic evidence

Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence (CETS No. 224)

Considering the proliferation of cybercrime and the increasing complexity of obtaining electronic evidence that may be stored in foreign, multiple, shifting or unknown jurisdictions, the powers of law enforcement are limited by territorial boundaries. As a result, only a very small share of cybercrime that is reported to criminal justice authorities is leading to court decisions.

The Second Additional Protocol to the Convention on Cybercrime (ETS No. 185) responds to these challenges and provides a series of tools for enhanced co-operation and disclosure of electronic evidence, such as:

- direct requests to registrars in other jurisdictions to obtain domain name registration information
- direct co-operation with service providers in other jurisdictions to obtain subscriber information
- more effective means to obtain subscriber information and traffic data through government-to-government co-operation
- expeditious co-operation in emergency situations
- joint investigation teams and joint investigations
- video conferencing
- a strong system of human rights and rule of law safeguards, including for the protection of personal data

Status of new protocol

- The protocol was opened for signature on 12 May 2022. The total number of ratifications

required for the protocol to enter into force is 5.
- Although 48 States have signed the treaty, only 2 States (Serbia and Japan) have ratified it (at the time of writing)

For an updated status on ratifications check here.

(6.2) The nature of encrypted electronic data and its handling in criminal proceedings

(6.2.1) General principles regarding the nature of encrypted electronic data and its handling

ECtHR, Yüksel Yalçınkaya v. Türkiye, App no 15669/20, 26 September 2023 (Grand Chamber)

This is the first case in which the ECtHR addressed the challenges of the nature of encrypted electronic data stored at the server of an Internet-based communication application (ByLock application).

The ECtHR set out certain general principles regarding the nature of such evidence, the special technologies required for its collection, securing, processing and analysis as well as the distinct reliability issues raised (e.g., destruction, damage, alteration or manipulation).

> 311. [...] the Court wishes to clarify whether the specific nature of the evidence at issue, that is encrypted electronic data stored at the server of an Internet-based communication application, requires it to adapt the application of the relevant guarantees under Article 6 § 1 in any way.
>
> 312. The Court [...] notes that electronic evidence differs in many respects from traditional forms of evidence, including as regards its nature and the special technologies required for its collection, securing, processing and analysis. Most significantly, it raises distinct reliability issues as it is inherently more prone to destruction, damage, alteration or manipulation. The Court also reiterates that the use of untested electronic evidence in criminal proceedings may involve particular difficulties for the judiciary as the nature of the procedure and technology applied to the collection of such evidence is complex and may therefore diminish the ability of national judges to establish its authenticity, accuracy and integrity. Moreover, the handling of electronic evidence, particularly where it concerns data that are encrypted and/or vast in volume or scope, may present the law enforcement and judicial authorities with serious practical and procedural challenges at both the investigation and trial stages.
>
> [...]

(6.2.2) Evidence and quality of encrypted electronic data

ECtHR, Yüksel Yalçınkaya v. Türkiye, App no 15669/20, 26 September 2023 (Grand Chamber)

The ECtHR examined the applicant's claim that the data regarding his use of the ByLock application, which had been the decisive evidence to secure his conviction, had been obtained unlawfully and should, therefore, have been inadmissible.

> 309. The essence of the applicant's complaint under the present head is that despite their inadmissibility as evidence on account of their unlawful procurement by the [Turkish Intelligence service], the data regarding his alleged use of ByLock were relied on as the decisive element to secure his conviction by the domestic courts, without duly addressing his concerns regarding their integrity and evidential value and in disregard of the principles of equality of arms and adversarial proceedings.
>
> 310. The Court considers at the outset that, having regard to its limited role in determining the admissibility of a piece of evidence or reviewing its assessment by national courts, it is not necessary, for the purposes of its present examination under Article 6, to determine whether the contested evidence was actually obtained lawfully in terms of domestic law and was admissible, or whether the domestic courts made any substantive errors in their assessment of the relevant evidence. Its task under Article 6 § 1 is rather to assess the fairness of the proceedings as a whole [...]. The Court notes in this regard that there is a distinction between the admissibility of evidence – that is to say the question of which elements of proof may be submitted to the relevant court for its consideration – and the rights of the defence in respect of evidence which in fact has been submitted to the court [...]
>
> 311. Turning to the facts of the present case, [...] the applicant's conviction for membership of an armed terrorist organisation rested decisively on the finding that he had used the ByLock application, which finding was primarily based on the data obtained by the [Turkish Intelligence service], the remaining evidence serving only as a source of corroboration. In these circumstances, the quality of the evidence in question [...] [was] all the more important. [...]
>
> [...]
>
> 314. According to the applicant, the detailed requirements set out in Articles 134 and 135 of the [Code of Criminal Procedure] [...] regarding the collection of electronic data pursued the aim of protecting against abuse and ensuring the authenticity and integrity of such data. He claimed, on that basis, that the fact that the State intelligence service had obtained and processed the relevant ByLock data in total secrecy and without any judicial oversight or other procedural guarantees envisaged under the Code of Criminal Procedure had put into question the reliability of the data.
>
> 315. The Court notes that electronic or other data collected by intelligence services, whose activities in that regard may or may not be subject to the standard rules of procedure applicable to the collection of evidence, may be increasingly resorted to in criminal proceedings as direct or indirect evidence. [...]
>
> 316. It is not for the Court to pronounce on whether and in what circumstances and format intelligence information may be admitted in criminal proceedings as evidence. [...] [This] is a matter that primarily remains within the discretion of national courts and other competent authorities [...]. It acknowledges, however, that in cases where the collection or processing of such information is not subject to prior independent authorisation or supervision, or a post factum judicial review, or where it is not accompanied by other procedural safeguards or corroborated by other evidence, its reliability may be more likely to be called into question.
>
> 317. [...] [I]t transpires from the information in the case file that sections 4 (1) and 6 (1) of the Law on Intelligence Services, invoked by the domestic courts and the Government as the legal basis for the [Turkish Intelligence service's] conduct, do not envisage procedural safeguards akin to those set out under Article 134 of

the Code of Criminal Procedure with respect to the collection of electronic evidence, including independent authorisation or oversight. Moreover, nothing in the case file suggests that the Ankara Fourth Magistrate's Court's subsequent order for the examination of the ByLock data pursuant to Article 134 of the Code of Criminal Procedure entailed a post factum judicial review of the [Turkish Intelligence service's] data collection activity. [...]

318. The Court [...] considers that it is not in a position to assess whether those measures presented sufficient guarantees of integrity and reliability, given in particular that the domestic courts did not engage in such an assessment.

[...]

323. [...] [A]lthough [the Court] recognises that the circumstances in which the ByLock data was retrieved by the Turkish Intelligence service did prima facie raise doubts as to their "quality" in the absence of specific procedural safeguards geared to ensuring their integrity until the handover to the judicial authorities, the Court does not have sufficient elements to impugn the accuracy of those data – at least to the extent that they established the applicant's use of the ByLock application.

(6.2.3) Principles of equality of arms and adversarial proceedings: the ability to verify the reliability and integrity of encrypted electronic evidence and challenge it in criminal proceedings

ECtHR, Yüksel Yalçınkaya v. Türkiye, App no 15669/20, 26 September 2023 (Grand Chamber)

The Court discusses the following questions:

- Does an individual have a right to have access to raw, encrypted electronic data so as to verify their reliability and integrity and, thus, be able to contest the veracity of the arguments made against them?
- Is the disclosure of evidence an absolute right under the right to a fair trial?
- If it is not an absolute right, what are the obligations of national authorities/courts in order to comply with the guarantees of a fair trial?

[...]

306. [..] a fundamental aspect of the right to a fair trial is that criminal proceedings, including the elements of such proceedings which relate to procedure, should be adversarial and that there should be equality of arms between the prosecution and defence. The right to an adversarial trial means, in a criminal case, that both prosecution and defence must be given the opportunity to have knowledge of and comment on the observations filed and the evidence adduced by the other party. [....]

307. The right to an adversarial trial also requires, in a criminal case, that the prosecution authorities disclose to the defence all material evidence in their possession for or against the accused. [...]

308. However, the entitlement to disclosure of relevant evidence is not an absolute right. In any criminal proceedings there may be competing interests, such as national security or the need to keep secret police methods of investigation of crime, which must be weighed against the rights of the accused. [...] In some cases, it may be necessary to withhold certain evidence from the defence so as to preserve the fundamental rights of another individual or to safeguard an important public interest. That said, in principle, only such measures restricting the rights of the defence which are strictly necessary are permissible under Article 6 § 1. Moreover, in order to

ensure that the accused receives a fair trial, any difficulties caused to the defence by a limitation on its rights must be sufficiently counterbalanced by the procedures followed by the judicial authorities [...]

[...]

324. The Court reiterates that a review of the overall fairness of the proceedings must also incorporate an assessment as to whether the applicant was given the opportunity of challenging the evidence and of opposing its use in circumstances where the principles of adversarial proceedings and equality of arms between the prosecution and the defence were respected [...]. It is stressed that the question whether the applicant's challenges to the evidence were properly examined by the domestic courts, that is whether the applicant was truly "heard", and whether the courts supported their decisions with relevant and adequate reasoning, are also factors to be taken into account in conducting this assessment. [...]

325. The applicant [..] claimed that it was essential for him to have access to [the data collected by the Turkish Intelligence service from the ByLock server] so as to verify their reliability and integrity, as well as to access potentially exculpatory information, and to contest the veracity of the arguments [...] that were relied on by the domestic courts in support of his conviction [...]

326. The Court notes, as also pointed out by the Government, that the applicant had available to him all the ByLock reports relied on by the domestic courts in the criminal proceedings, and that the accuracy of the ByLock data pertaining to him had been verified on the basis of data obtained from other sources. The Court further notes that a technical report produced in 2020 explained that it was not possible to sort the raw data on a user ID basis without first processing them [...]

327. The Court reiterates in this connection that the requirement of disclosure to the defence of "all material evidence" for or against the accused, which is an aspect of the right to adversarial proceedings [...], cannot be construed narrowly [...]

328. [...] the ByLock data in question were critical in the applicant's case [...] It may, moreover, not be excluded that the ByLock material potentially contained elements which could have enabled the applicant to exonerate himself, or to challenge the admissibility, reliability, completeness or the evidential value of that material [...]

329. The Court must nevertheless emphasise that the entitlement to disclosure of evidence is not an absolute right. [...] [T]here may be a variety of reasons which may require the withholding of evidence from the defence, including concerns over national security [...]

330. That said, even in such circumstances, the Court must examine whether any prejudice sustained by the applicant on account of the non-disclosure of the relevant ByLock data was counterbalanced by adequate procedural safeguards and whether he was given a proper opportunity to prepare his defence, as required by Article 6 [...]

331. The Court notes firstly that according to the information in the case file, the reasons advanced by the Government before the Court [...] to justify the non-disclosure of the relevant data to the applicant were never actually adverted to in the domestic courts' judgments [...]; the applicant's request that the data be admitted to the case file simply went unanswered. The complementary analysis report submitted by the Government to the Court, which provided further insight into how the ByLock user lists had been drawn up and why the raw data pertaining to individual ByLock users could not be isolated and shared with the relevant users, was similarly not available to the applicant during the course of the criminal proceedings against him. [...] Accordingly [...] the Court [...] cannot but note that the applicant was given no explanation by the domestic courts as to why, and upon whose decision, the raw data – particularly to the extent that they concerned him specifically – were kept from him. He was therefore deprived of the opportunity to present any counter-arguments, such as to contest

the validity of those reasons or to dispute that all efforts had been made to strike a fair balance between the competing interests at play and to ensure the rights of the defence. [...]

332. Secondly, the applicant's request that the raw data be submitted to an independent examination for the verification of their content and integrity was also not entertained by the domestic courts. [...]

333. That said, given in particular the absence of any concrete information in the case file to suggest that the data in question had at any point been subjected to examination for verification of their integrity [...] the Court considers that the applicant had a legitimate interest in seeking their examination by independent experts and that the courts had the duty of properly responding to him. [...]

334. [...] The Court notes [...] that other than confirming the lawfulness of the data collection procedure [...] the domestic courts did not address the separate matter of how the integrity of the data obtained from the server had been ensured in all respects – that is, beyond the issue of the applicant's individual use [...]. Nor did they refer to any other judgments or procedures where this matter was addressed. [...]

335. [W]hile it may not have been possible to share the raw data with the applicant, the requirement of "fair balance" between the parties would have at least required the proceedings to be conducted in a manner that would enable the applicant to comment on the full extent of the decrypted material concerning him, including, in particular, the nature and content of his activity over that application. [...]

341. The Court considers, in the light of the foregoing, that there were not enough safeguards in place to ensure that the applicant had a genuine opportunity to challenge the evidence against him and conduct his defence in an effective manner and on an equal footing with the prosecution [...]. Moreover, the domestic courts' failure to respond to the applicant's specific and pertinent requests and objections raised a legitimate doubt that they were impervious to the defence arguments and that the applicant was not truly "heard". In view of the importance of duly reasoned decisions for the proper administration of justice, the domestic courts' silence on vital matters that went to the heart of the case also raised well-founded concerns on the applicant's part regarding their findings and the conduct of the criminal proceedings "as a matter of form" only [...].

[...]

346. In the Court's view, the foregoing considerations are sufficient to lead to the conclusion that the criminal proceedings against the applicant fell short of the requirements of a fair trial in breach of Article 6 § 1 of the Convention.

(6.2.4) Right to have adequate time and facilities for the preparation of one's defence (Art 6(3)(b) ECHR)

ECtHR, Rook v. Germany, App no 1586/15, 25 July 2019

One of the relevant questions in this case was whether the State should bear the cost for the expensive special forensic-data-analysis programme which was used by authorities to encrypt the applicant's data.

3. The applicant alleged that, during the criminal proceedings against him, he and his counsel had not been provided with sufficient and adequate access to audio files, text messages and electronic files (specifically emails and other text documents) which the investigating authorities had seized throughout the investigation. He relied on Article 6 § 1 and 3 (b) of the Convention.

8. During searches of the applicant's home and of other premises between 13 July 2011 and 1 February 2012, some 14 million electronic files (for example emails and other text documents), stored on a range of data devices, for example hard discs, were seized. The files of each device were copied as a single "image file", the devices were returned to the rightful holders, including the applicant, afterwards. Each image file was a full digital clone

of each data device, readable with a program available free of charge online. However, the image files were subsequently entered into a special forensic-data-analysis program, after which their content could be retrieved only using that special program, available for 4,031.72 euros (EUR). After the data had been entered into that program, in order to be able to read the data with a program available free of charge online, the data had to be exported from the special forensic-data-analysis program and converted back into an image format. The above-described processing of the data, in particular feeding them into the special forensic-data-analysis program, was finished by the end of February 2012; they were stored at the Bavarian Office of Criminal Investigation in Munich.

9. The data were analysed by the police; around 1,100 of these electronic files were considered as relevant to the case and were printed and subsequently included in the paper files.

[...]

Disclosure of the electronic files

70. The Court observes that the applicant's lawyer could have accessed – but never did – the entirety of the electronic files on the premises of the criminal police as of the end of February 2012, when he must also have been aware of the fact that electronic files – apart from his own – had been retrieved [...]. The Court furthermore observes that, after the applicant had only on 3 April 2012 [...] requested disclosure of the entirety of the electronic files, the authorities did not object in principle, but were ready to allow for examination. In this connection, the Court notes that on 22 May 2012 the authorities provided the applicant's lawyer with a copy of the entirety of the electronic files. This copy was, however, readable only with an expensive software which lawyers and private individuals appear to not usually have at their disposal [...]. Therefore, the events following the request of 3 April 2012, in particular the dispute concerning the question whether the state should bear the cost for the expensive special forensic-data-analysis program [...], disclose practical difficulties in view of the encryptment of an enormous amount of data. The Court moreover notes that only in July 2012, the defence asked to be provided with a copy in a format readable with freely available software, a request to which the authorities agreed on short notice [...]. The applicant's lawyer provided two hard discs at the end of July 2012, and the data was provided on 4 September 2012 [...]. Moreover, even if the Court does not consider it necessary for the applicant to explain his defence strategy, the Court observes that the applicant has, neither in the domestic proceedings nor before the Court, specified in what particular manner the invoked restrictions had interfered with his opportunity to defend himself.

[...]

(6.3) The rights to remain silent and not to incriminate oneself: forcing suspects to unlock their electronic devices

(6.3.1) Criteria for the lawful use of compulsory powers to obtain material from a suspect

ECtHR, Saunders v the United Kingdom, App no 19187/91, 17 December 1996 (Grand Chamber)

- According to the ECtHR, the right not to incriminate oneself is primarily concerned with respecting the will of an accused person to remain silent.
- However, this right does not extend to the use in criminal proceedings of material which may be

obtained from the accused through the use of compulsory powers that has an existence independent of the will of the suspect (e.g., documents, breath, blood and urine samples and bodily tissue acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue)

- The crucial question is to decide when an action is independent of the will of the suspect.

> 68. [...] although not specifically mentioned in Article 6 of the Convention, the right to silence and the right not to incriminate oneself are generally recognised international standards which lie at the heart of the notion of a fair procedure under Article 6. Their rationale lies, inter alia, in the protection of the accused against improper compulsion by the authorities thereby contributing to the avoidance of miscarriages of justice and to the fulfilment of the aims of Article 6 [...]. The right not to incriminate oneself, in particular, presupposes that the prosecution in a criminal case seek to prove their case against the accused without resort to evidence obtained through methods of coercion or oppression in defiance of the will of the accused. In this sense the right is closely linked to the presumption of innocence contained in Article 6 para. 2 of the Convention.
>
> 69. The right not to incriminate oneself is primarily concerned, however, with respecting the will of an accused person to remain silent. As commonly understood in the legal systems of the Contracting Parties to the Convention and elsewhere, it does not extend to the use in criminal proceedings of material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect such as, inter alia, documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing.

(6.3.2) Forcing the biometric unlocking of a smartphone?

Dutch Supreme Court, 9 February 2021, ECLI: SR:HR:2021:202 (in Dutch) (unofficial translation)

- The case concerned the forced biometric unlocking (by engaging suspect and placing his thumb on fingerprint scanner of the confiscated smartphone of the suspect) so as to gain access to content for investigative purposes.
- The Court found, in this case, that the material obtained existed independently of the will of the suspect and could be obtained under duress.
- The Court also distinguished this scenario (forcing biometric unlocking) from forcing a suspect to give the access code of his phone, which requires a statement and likely violates the right not to be self-incriminated.

In this context, the question arises whether placing the thumb of the suspect on the iPhone without his consent/co-operation is contrary to the nemo tenetur principle. This principle concerns the right of a suspect not to be forced (actively) to cooperate in his own conviction. It follows from the case-law of the European Court of Human Rights (the ECHR) that this mainly concerns the making of declarations under duress. The right of suspect not to [incriminate] himself is "primarily concerned with respecting the will of an accused person to [be] silent" [...]. A suspect is obliged to (passively) undergo and tolerate investigation measures.

Material that exists independently of the will of the suspect may be obtained under duress, such as blood and urine samples ([...] ECHR 17 December 1996, NJ 1997/699 (Saunders/United Kingdom)).

Unlike the situation in which the defendant is forced to give the access code of his phone, which requires a statement from a suspect, placing the thumb of the suspect on his iPhone in the opinion of the court does not infringe the nemo tenetur principle. This concerns the tolerance of an investigative measure that does not require the active cooperation of the suspect. In addition, the fingerprint is obtained with a very small degree of coercion. The fact that with the placing of the suspect's thumb on the iPhone access to possible will-dependent and incriminating data does not make this any other in the opinion of the court.

Read: A Pivaty, Suspects' privilege against self-incrimination not violated when made to unlock smartphone with fingerprint, Dutch Supreme Court rules, Fair Trials, 19 February 2021

(6.3.3) Forcing the disclosure of the security code to unlock a mobile phone?

ECtHR, Minteh v France, App no 23624/20 (pending case)

> Communicated under Article 6(1) and Article 8 ECHR
>
> This case concerns the criminal conviction of the applicant for refusing to disclose to the police the security code to unlock his mobile phone while he was in police custody.
>
> It is an offence under the French criminal code "for an individual having knowledge of the decryption procedure for access to an encrypted device that could have been used to prepare, facilitate or commit a serious offence, to refuse to disclose that procedure to the judicial authorities or to use it when so directed by the authorities ..." (Article 434-15-2).
>
> Having been convicted on the basis of that provision for refusing to disclose to the police the code to unlock his mobile phone while he was in police custody, the applicant complains of a breach of his right to remain silent and not to incriminate himself, together with a breach of his right to respect for his private life and for his correspondence.

Questions:

- Do you think that French legislation is in accordance with the right to remain silent and not to incriminate oneself?
- How do you think that the ECtHR will decide this case?



Further readings

- Y Gökce, 'The Bylock fallacy: An In-depth Analysis of the Bylock Investigations in Turkey'(2018) 26 Digital Investigation 81-91
- Y Gökce, 'Systemic Problems Unveiled: The Yalcinkaya Case and the Demise of the Bylock Digital Evidence' ECHR Blog, 25 October 2023
- H Partouche, and C Berthélémy, Mass hacking and fundamental rights: a missed opportunity for the CJEU?, EU Law Analysis, EU law analysis blog, 11 July 2024

- R Stoykova, 'Encrochat: The hacker with a warrant and fair trials?' (2023) 46 Forensic Science International: Digital Investigation 301602

7. RIGHTS TO POLITICAL PARTICIPATION AND FREE ELECTIONS

Outline of this chapter

This chapter explains how the effective exercise of the rights to political participation and free elections is being undermined by the functioning of AI systems and AI decision-making processes on large online platforms (e.g., social media). More specifically, this chapter addresses:

- the relevant law concerning the right to political participation and the right to free elections (section 7.2)
- the protective scope of the rights and the respective States' obligations (section 7.3)
- what the new protected interests introduced by recent regulation are and their relationship to human rights law (section 7.4)
- how the concepts of 'integrity of democratic processes' and 'individual's fair access to and participation in public debate' under the Framework AI Convention purport to capture some of the new challenges (section 7.5)
- the role of the negative effects on 'civic discourse' and 'electoral processes' under the DSA to mitigating systemic risks and large-scale societal harms (section 7.6)

(7.1) What's at Stake? Setting the Scene

> Commission opens formal proceedings against TikTok on election risks under the Digital Services Act, 17 December 2024
>
> > Today, the Commission has opened formal proceedings against TikTok for a suspected breach of the DSA in relation to TikTok's obligation to properly assess and mitigate systemic risks linked to election integrity, notably in the context of the recent Romanian presidential elections on 24 November.
> >
> > [...]
> >
> > The proceedings will focus on management of risks to elections or civic discourse, linked to the following areas:
> >
> > - TikTok's recommender systems, notably the risks linked to the coordinated inauthentic manipulation or automated exploitation of the service.
> > - TikTok's policies on political advertisements and paid-for political content.

Big Tech companies are increasingly under scrutiny for their influence on elections and, more generally, on political/civic space. The Cambridge Analytica scandal revealed that the data analytics firm that worked with Donald Trump's election team and the winning Brexit campaign harvested millions of Facebook profiles of US voters and used them to build a software programme to predict and influence choices at the ballot box. It is also documented that TikTok, X and Instagram's algorithms recommended right-leaning content more than twice as much as left-leaning content to politically interested yet non-partisan users in the 2025 federal elections in Germany.

There are serious concerns on how AI systems of online platforms:

- undue influence voters and their political behaviour, including casting their vote
- compromise individuals' ability to freely form opinions
- erode the overall environment which gives rise to the formation of political views and political participation

(7.2) Relevant Law

(7.2.1) Right to political participation

Article 25 International Civil and Political Rights

> Every citizen shall have the right and the opportunity, without any of the distinctions mentioned in article 2 and without unreasonable restrictions:
>
> 1. To take part in the conduct of public affairs, directly or through freely chosen representatives;
> 2. To vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors;
>
> [...]

(7.2.2) Right to free elections

Article 3, Protocol 1 to the ECHR

> The High Contracting Parties undertake to hold free elections at reasonable intervals by secret ballot, under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature.

(7.3) Protective Scope of the Right

The scope of the right to political participation (under the ICCPR) and of the right to free elections (under the ECHR) include the guarantee of the conditions which ensure the free expression of the opinion of the people. This guarantee is explicit in the letter of the provisions quoted earlier. However, fleshing out what these conditions are and what the respective States' obligations are is not challenge-free given the fact that States enjoy a considerable margin of appreciation in this area. The novel risks in the context of AI systems and business practices embedded in very large online platforms and search engines bring to the table societal harms of a large scale and/or with long-term effects in society (e.g., undue influence/manipulation and distortion of the civic space) that are difficult to be identified and isolated under human rights law given the latter's individualistic character.

For present purposes, the material and discussion focus on the existing "tools" that we have in the human rights law "toolbox" to guarantee the conditions which ensure the free expression of the opinion of the people and aspects of political participation.

(7.3.1) Elections and media pluralism

Human rights bodies emphasise the interrelation between free elections and freedom of expression. Free

communication of information and ideas about political issues and a free press able to inform public opinion without censorship or restraint are essential guarantees. States parties to the ECHR have the positive obligation to intervene in order to open up the media to different viewpoints and a diversity of political outlook. However, States enjoy a wide margin of appreciation in the field of electoral legislation.

(7.3.1.1) UN Human Rights Committee, General Comment No 34, Article 19: Freedoms of opinion and expression, UN Doc CCPR/C/GC/34, 12 September 2011

> 20. The Committee, in general comment No. 25 on participation in public affairs and the right to vote, elaborated on the importance of freedom of expression for the conduct of public affairs and the effective exercise of the right to vote. The free communication of information and ideas about public and political issues between citizens, candidates and elected representatives is essential. This implies a free press and other media able to comment on public issues and to inform public opinion without censorship or restraint. [...]

(7.3.1.2) ECtHR, Manole and Others v. Moldova, App no 13936/02, 17 September 2009

> 100. [...] a duty on the State to ensure that the public has access to impartial and accurate information and a range of opinion and comment, reflecting inter alia the diversity of political outlook within the country [...]

(7.3.1.3) ECtHR, Communist Party of Russia and Others v. Russia, App no 29400/05, 19 June 2012

> 107. [...] The interrelation between free elections and freedom of expression was also emphasised in Bowman v. the United Kingdom [...], where the Court held that "it is particularly important in the period preceding an election that opinions and information of all kinds are permitted to circulate freely". Lastly, in Yumak and Sadak v. Turkey [GC], the Court held that the State was under an obligation to adopt positive measures to organise elections "under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature".
>
> [...]
>
> 123. [...] The next question is whether the State was under any positive obligation under Article 3 of Protocol No. 1 to ensure that media coverage by the State-controlled mass-media was balanced and compatible with the spirit of "free elections" [...] In examining this question the Court will bear in mind that "States enjoy a wide margin of appreciation in the field of electoral legislation" [...]
>
> [...]
>
> 125. [...] The Court reiterates that there can be no democracy without pluralism [...] In the context of elections the duty of the State to adopt some positive measures to secure pluralism of views has also been recognised by the Court. [...]
>
> 126. The Court notes that the State was under an obligation to intervene in order to open up the media to different viewpoints. That being said, it is clear that the time and technical facilities available for political broadcast were not unlimited. [...]

(7.3.2) Elections and manipulation of the media

ECtHR, Communist Party of Russia and Others v. Russia, App no 29400/05, 19 June 2012

In a rather uncommon case before the ECtHR, the applicants alleged that the media coverage on the TV channels had been predominantly hostile to the opposition parties and candidates due to political manipulation. They further submitted that the biased media coverage had affected public opinion to a critical extent and had made the elections not "free". The ECtHR found that the applicants' claims on political manipulation were not substantiated and proved. Interestingly, the Court added that, even if propaganda by a political party takes place, it is very difficult, if not impossible, to determine a causal link between "excessive" political publicity and the election result.

> 111. In most of the previous cases under Article 3 of Protocol No. 1 the Court has had to consider a specific legislative provision or a known administrative measure which has somehow limited the electoral rights of a group of the population or of a specific candidate. In those cases the measure complained of lay within the legal field, and, therefore, could be easily identified and analysed [...]
>
> 112. The situation in the present case is different. The applicants did not deny that Russian law guaranteed neutrality of the broadcasting companies, making no distinction between pro-governmental and opposition parties, and proclaimed the principle of editorial independence of the broadcasting companies. They claimed, however, that the law was not complied with in practice, and that de jure neutrality of the five nationwide channels did not exist de facto.
>
> 113. The applicant's position in the present case can be narrowed down to three main factual assertions. First, the applicants alleged that media coverage on the five TV channels had been predominantly hostile to the opposition parties and candidates. Secondly, they asserted that it was a result of a political manipulation, that the executive authorities and/or United Russia had used their influence to impose a policy on the TV companies which had helped to promote United Russia. Thirdly, the applicants claimed that biased media coverage on TV had affected public opinion to a critical extent, and had made the elections not "free".
>
> 114. As to the first point, the Court observes that the Supreme Court in its judgment of 16 December 2004 did not find that the media coverage had been equal in all respects. [...] The Supreme Court's conclusion was formulated more carefully and in a qualified manner: it noted that the tenor of media coverage on TV during the elections had not been so "egregious" to make the ascertaining of the genuine will of the voters impossible.
>
> 115. The answer given by the Supreme Court to the applicant's first point was somewhat elusive. Conversely, on the other two propositions of the applicants the Supreme Court was more explicit. It found in essence that no proof of political manipulation had been adduced, and that no causal link between media coverage and the results of the elections had been shown.
>
> 116. The applicants argued that the findings of the Supreme Court in these respects were arbitrary and should not be relied upon. [...] The first question is thus whether the Supreme Court's findings were arbitrary or manifestly unreasonable.
>
> [...]
>
> 118. The Supreme Court found that the applicants had failed to show a causal link between the media coverage and the results of the elections. That finding is debatable; it is clear that the media coverage must have at least some effect on the voting preferences. What is true, however, is that the effect of media coverage is often very difficult to quantify. The Court recalls its own finding in the case of Partija Jaunie Demokrāti and Partija Mūsu Zeme v. Latvia where it held that "however important [the propaganda by a political party] may be, [it] is not the only factor which affects the choice of potential voters. Their choice is also affected by other factors

[...], so it is very difficult, if not impossible, to determine a causal link between "excessive" political publicity and the number of votes obtained by a party or a candidate at issue". [...] the SPS political party which obtained generally positive media coverage did not even pass the minimal electoral threshold. The Rodina political block, by contrast, obtained a much better score at the elections despite poor media coverage. Therefore, the Supreme Court's arguments in this part did not appear "arbitrary or manifestly unreasonable".

119. Furthermore, and most importantly, the Supreme Court's findings did not support the applicants' allegation of a manipulation of the media by the government, which was their central proposition. The Supreme Court found that the journalists covering elections or political events had been independent in choosing the events and persons to report on, that it had been their right to inform the public about events involving political figures, and that they had not had the intent of campaigning in favour of the ruling party [...]

120. The Court notes that, indeed, the applicants did not adduce any direct proof of abuse by the Government of their dominant position in the capital or management of the TV companies concerned. [...] [T]he TV journalists in the present case did not complain of undue pressure by the Government or their superiors during the elections. The Court reiterates that the weight to be given to an item of information "is a matter to be assessed, in principle, by the responsible journalists" [...], and that the journalists and news editors enjoyed, under Article 10 of the Convention, a wide discretion on how to comment on political matters. The applicants did not sufficiently explain how it was possible, on the basis of the evidence and information available and in the absence of complaints of undue pressure by the journalists themselves, to distinguish between Government-induced propaganda and genuine political journalism and/or routine reporting on the activities of State officials [...]

[...]

Alleged failure by the State to comply with its positive obligations

[...]

126. [...] As the case shows, the applicants did obtain some measure of access to the nation-wide TV channels; thus, they were provided with free and paid airtime, with no distinction made between the different political forces. The amount of airtime allocated to the opposition candidates was not insignificant. The applicants did not claim that the procedure of distribution of airtime was unfair in any way. Similar provisions regulated access of parties and candidates to regional TV channels and other mass media. In addition, the opposition parties and candidates were able to convey their political message to the electorate through the media they controlled. In this connection, the Court also notes that it follows from the report of the OSCE/ODIHR, which generally found that the main country-wide state sponsored broadcasters that were monitored, openly promoted United Russia, that voters who actively sought information could obtain it from various sources [...] The Court considers that the arrangements which existed during the 2003 elections guaranteed the opposition parties and candidates at least minimum visibility on TV.

127. Lastly, the Court turns to the applicants' allegation that the State should have ensured neutrality of the audio-visual media. [...] The question is what sort of interference with journalistic freedom would be appropriate in the circumstances in order to protect the applicants' rights under Article 3 of Protocol No. 1. [...] Having regard to the materials at its possession, including the Supreme Court's findings [...], the Court considers that the applicants' claims in this respect have not been sufficiently substantiated.

(7.4) New Protected Interests Introduced by Recent

Regulation

- **What are these new protected interests?**

Certain algorithmic harms are not necessarily effectively addressed by human rights law (or other areas of law either). The large scale and systemic nature of said harms cannot be fully captured by human rights law considering the latter's individualistic character.

Recent pieces of legislation introduce and protect new regulatory categories/interests, including 'democratic processes' and 'individuals' fair access to and participation in public debate', under the Framework AI Convention (7.4.1); or 'electoral processes' and 'civic discourse', under the DSA (7.4.2). Potential manipulation or exploitation of human vulnerabilities can also be relevant under Article 5(1)(a), (b) EU AI Act (7.4.3) (for prohibited AI practices see discussion in 4.4))

- **Distinguishing the recent regulatory developments from human rights law**

These interests may seem to be "human rights-like" but they need to be understood in their own context. As far as the Framework AI Convention is concerned, it needs to be reminded that it does not create new rights for individuals or new obligations for States. The Framework AI Convention certainly advances our understanding of the harms at hand and highlights the interconnectedness of interests/rights but it is up to State parties how they will implement the Convention. Turning to the DSA, it does not create rights for individuals; rather, its added value lies in introducing obligations for very large online platforms and search engines on identifying, assessing and mitigating systemic risks. The AI Act does not create rights for individuals either but imposes due diligence and transparency obligations on private and public actors when they develop and/or deploy certain AI systems. Consequently, these new pieces of legislation are underpinned by protecting the at-scale impacts on human rights (among other interests) but strictly speaking they do not qualify as human rights law since they **a)** do not create rights; **b)** do not specifically focus on the protection of the individual; and **c)** do not provide for remedies.

(7.5) 'Integrity of democratic processes' and 'individual's fair access to and participation in public debate' under the Framework Convention on AI, Human Rights, Democracy and the Rule of Law

The added value of the Framework AI Convention lies in protecting not only human rights (Article 4) but also democratic processes (Article 5). The Convention stresses:

- state parties' obligation to adopt measures so that AI systems are not used to undermine the integrity of democratic processes (Article 5(1))
- state parties' obligation to ensure individuals' fair access to and participation in public debate (Article 5(2))
- the link between an individual's ability to freely form opinions and democratic processes (Article 5(2)). Notwithstanding that Article 7 covers states' obligation to respect individual autonomy, the rationale of Article 5(2) is twofold: first, it pinpoints at the formation of political opinions, as an aspect of individual autonomy; and, second, it stresses the implications of manipulating and altering political opinions on a large scale.

Nonetheless, the Framework AI Convention does not give any further guidance on what these positive obligations of states may be.

(7.5.1) Article 5 – Integrity of democratic processes and respect for the rule of law

> 1. Each Party shall adopt or maintain measures that seek to ensure that artificial intelligence systems are not used to undermine the integrity, independence and effectiveness of democratic institutions and processes, including the principle of the separation of powers, respect for judicial independence and access to justice.
>
> 2. Each Party shall adopt or maintain measures that seek to protect its democratic processes in the context of activities within the lifecycle of artificial intelligence systems, including individuals' fair access to and participation in public debate, as well as their ability to freely form opinions.

(7.5.2) Explanatory Report to Council of Europe Framework Convention on artificial intelligence human rights, democracy and the rule of law

> 42. Artificial intelligence technologies possess significant potential to enhance democratic values, institutions, and processes. Potential impacts include the development of a deeper comprehension of politics among citizens, enabling increased participation in democratic debate or improving the integrity of information in online civic space. [...]
>
> [...]

> 47. Furthermore, the integrity of democracy and its processes is based on two important assumptions referred to in Article 7, namely that individuals have agency (capacity to form an opinion and act on it) as well as influence (capacity to affect decisions made on their behalf). Artificial intelligence technologies can strengthen these abilities but, conversely, can also threaten or undermine them. It is for this reason that paragraph 2 of the provision refers to the need to adopt or maintain measures that seek to protect "the ability [of individuals] to freely form opinions". With respect to public sector uses of artificial intelligence, this could refer to, for example, general cybersecurity measures against malicious foreign interference in the electoral process or measures to address the spreading of misinformation and disinformation

(7.6) Negative Effects on Civic Discourse and Electoral Processes as Systemic Risks under the DSA

Actual or foreseeable negative effects on electoral processes and civic discourse qualify as systemic risks under Article 34(1)(c) DSA. Providers of very large online platforms and search engines have the obligation to carry out risk assessments and undertake mitigation measures (7.6.1).

As far as **electoral processes** are concerned, the Commission has published Guidelines with best practices and mitigation measures to be undertaken by providers before, during, and after electoral events (7.6.2). By way of example, the discussion indicates the challenges surrounding real-time election-monitoring tools (7.6.3).

'Civic discourse' is a broader notion to 'electoral processes' linking elections and political participation. It brings to the foreground the overall environment giving rise to the formation of political views. Curation and moderation practices, the functioning of recommender systems and the visibility of political content are crucial components (7.6.4).

(7.6.1) Risk assessment – Article 34(1)(c) DSA

> Providers of very large online platforms and of very large online search engines shall diligently identify, analyse and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services.
>
> They shall carry out the risk assessments by the date of application referred to in Article 33(6), second subparagraph, and at least once every year thereafter, and in any event prior to deploying functionalities that are likely to have a critical impact on the risks identified pursuant to this Article. This risk assessment shall be specific to their services and proportionate to the systemic risks, taking into consideration their severity and probability, and shall include the following systemic risks:
>
> [...]

any actual or foreseeable negative effects on civic discourse and electoral processes [...]

(7.6.2) Mitigation measures to be undertaken before, during, and after electoral events

Commission Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065, March 2024

22. To reinforce internal processes and resources in a particular electoral context, providers of VLOPs and VLOSEs should consider setting up a dedicated, clearly identifiable internal team prior to each individual electoral period [...]. The resource allocation for that team should be proportionate to the risks identified for the election in question, including being staffed by persons with Member State specific expertise, such as local, contextual and language knowledge. The team should cover all relevant expertise including in areas such as content moderation, fact-checking, threat disruption, hybrid threats, cybersecurity, disinformation and FIMI, fundamental rights and public participation and cooperate with relevant external experts [...]

27. Specifically, mitigation measures aimed at addressing systemic risks to electoral processes should include measures in the following areas:

[...]

d) **Recommender systems** can play a significant role in shaping the information landscape and public opinion, as recognised in recitals 70, 84, 88, and 94, as well as Article 34(2) of Regulation (EU) 2022/2065. To mitigate the risk that such systems may pose in relation to electoral processes, providers of VLOPs and VLOSEs should consider:

(i) Ensuring that recommender systems are designed and adjusted in a way that gives users meaningful choices and controls over their feeds, with due regard to media diversity and pluralism;

(ii) Establishing measures to reduce the prominence of disinformation in the context of elections based on clear and transparent methods, e.g. regarding deceptive content that has been fact-checked as false or coming from accounts that have been repeatedly found to spread disinformation;

(iii) Establishing measures to limit the amplification of deceptive, false or misleading content generated by AI in the context of elections through their recommender systems;

(iv) Regularly assessing the performance and impact of recommender systems and addressing any emerging risks or issues related to electoral processes, including by updating and refining policies, practices, and algorithms;

(v) Establishing measures to provide transparency around the design and functioning of recommender systems, in particular in relation to the data and information used in designing systems that foster media pluralism and diversity of content, to facilitate third party scrutiny and research;

(vi) Engaging with external parties to conduct adversarial testing and red team exercises on these systems to identify potential risks such as risks stemming from biases, susceptibility to manipulation, or amplification of misinformation, disinformation, FIMI or other harmful content.

[...]

Fundamental rights

33. Risk mitigation measures, taken in line with Article 35 of Regulation (EU) 2022/2065, should be taken with due regard for the protection of fundamental rights enshrined in the Charter of Fundamental Rights of the European Union, in particular the right to freedom of expression and of information, including media freedom and pluralism. [...]

34. When mitigating systemic risks for electoral integrity, the Commission recommends that due regard is also given to the impact of measures to tackle illegal content such as public incitement to violence and hatred to the extent that such illegal content may inhibit or silence voices in the democratic debate, in particular those representing vulnerable groups or minorities. For example, forms of racism, or gendered disinformation and gender-based violence online including in the context of violent extremist or terrorist ideology or FIMI targeting the LGBTIQ+ community can undermine open, democratic dialogue and debate, and further increase social division and polarization. [...]

(7.6.3) Case study: Real-time election-monitoring tools

(7.6.3.1) Commission opens formal proceedings against Facebook and Instagram under the Digital Services Act, 30 April 2024

> The current proceedings will focus on the following areas:
>
> [...]
>
> The non-availability of an effective third-party real-time civic discourse and election-monitoring tool ahead of the upcoming elections to the European Parliament and other elections in various Member States. Meta is in the process of deprecating "CrowdTangle", a public insights tool that enables real-time election-monitoring by researchers, journalists and civil society, including through live visual dashboards, without an adequate replacement. However, as reflected in the Commission's recent Guidelines for providers of Very Large Online Platforms on systemic risks for electoral processes, in times of elections, access to such tools should instead be expanded. The Commission therefore suspects that, taking into account Meta's deprecation and planned discontinuation of CrowdTangle, Meta has failed to diligently assess and adequately mitigate risks related to Facebook's and Instagram's effects on civic discourse and electoral processes and other systemic risks.

(7.6.3.2) Criticism to Meta's EU election monitoring dashboard

Marsh, 'Meta's elections dashboard: A very disappointing sign', 6 June 2024, AlgorithmWatch

> On 3 June, Meta released an EU election monitoring dashboard, responding to investigations by the EU Commission under the Digital Services Act. It is riddled with basic errors, raising severe concerns about Meta's engagement with risks of electoral interference.
>
> Building election monitoring tools can be complicated. Nonetheless there are basic markers of quality. I used to lead team building dashboards for potential crisis situations in Number 10 Downing Street in the UK. If my team had come up with the product Meta has published, I would have asked them to

redo it – because of the issues and missing basic quality standards. It is unclear if Meta would redo their product.

(7.6.4) Case study: Visibility of political content and civic discourse under the DSA

In early 2025, META adopted a new policy regarding its 'political content approach', allegedly in an effort to reduce disinformation. The new policy changes how the recommender systems of Instagram and Facebook curate content and, therefore its visibility to users. There is evidence to suggest that the new policy excludes many actors and topics from civic discourse, such as reproductive rights.

(7.6.4.1) META, Our Approach to Political Content, updated 7 January 2025

> We want you to have a valuable experience when you use Facebook, Instagram and Threads, which is why we use AI systems to personalise the content you see based on the choices you make. People have told us that they want to see less political content, so we have spent the last few years refining our approach on Facebook to reduce the amount of political content – including from politicians' accounts – that you see in Feed, Reels, Watch, Groups you should join and Pages you may like. We've recently extended this approach in Reels, Explore and in-feed recommendations on Instagram and Threads too.
>
> As part of this, we aim to avoid making recommendations that could be about politics or political issues, in line with our approach of not recommending certain types of content to those who don't wish to see it.
>
> [....]

(7.6.4.2) Commission opens formal proceedings against Facebook and Instagram under the Digital Services Act, 30 April 2024

> Visibility of political content. The Commission suspects that Meta's policy linked to the 'political content approach', that demotes political content in the recommender systems of Instagram and Facebook, including their feeds, is not compliant with DSA obligations. The investigation will focus on

the compatibility of this policy with the transparency and user redress obligations, as well as the requirements to assess and mitigate risks to civic discourse and electoral processes.

(7.7) Prohibition of Manipulation and Exploitation of Human Vulnerabilities under the AI Act

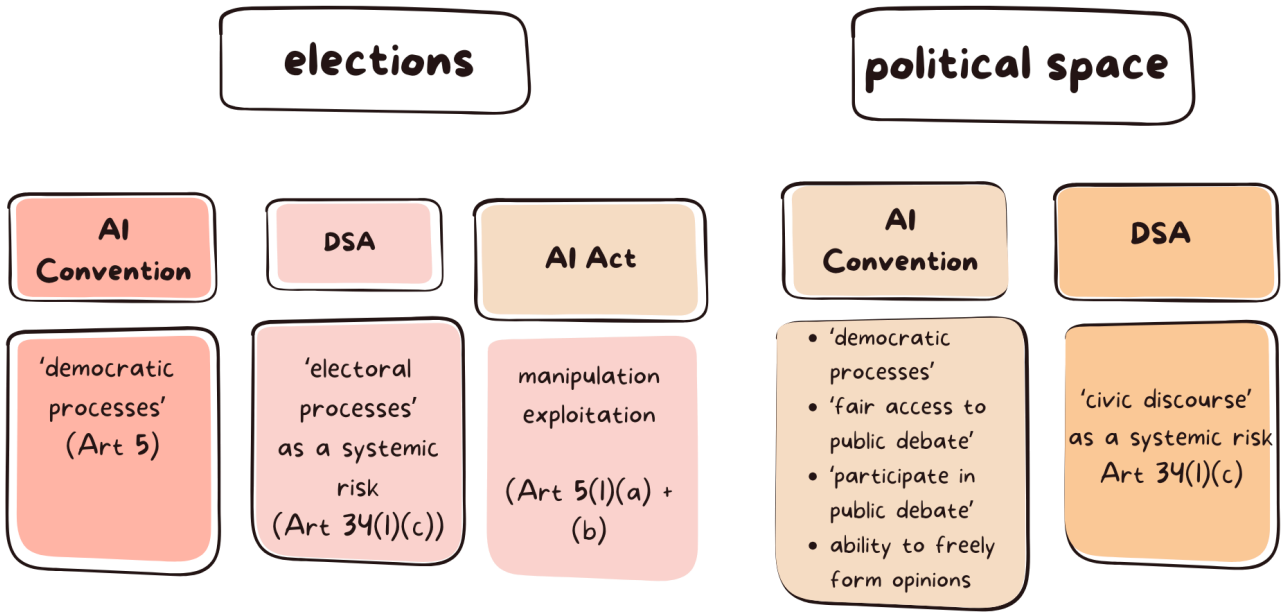
Article 5(1)(a) and (b) EU AI Act – Prohibited AI Practices

The following AI practices shall be prohibited:

(a) the placing on the market, the putting into service or the use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm;

(b) the placing on the market, the putting into service or the use of an AI system that exploits any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm;

For further discussion see section **(4.4)**



Further readings/resources

- A Rachovitsa, How AI Systems Threaten to Erode the Rule of Law, Jurist, 13 March 2025
- M Ingram, Threads: You can have political content but you will have to work for it, Columbia Journalism Review, 15 February 2024
- Marsh, 'Meta's elections dashboard: A very disappointing sign', 6 June 2024, AlgorithmWatch
- P Iyer, Report Finds Meta's Approach to Political Content Reduces Reach for Activist Accounts, Tech Policy Press, 13 August 2024
- S Bradshaw, H Bailey & PN Howard, Report: Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation, Programme on Democracy & Technology, 2021
- J Williams, 'Ethical Dimensions of Persuasive Technology', in C Véliz (ed), The Oxford Handbook of Digital Ethics (OUP 2022) 1

On political advertisement:

- Pooja Chaudhuri and Melissa Zhu, 'What Meta's Ad Library Shows About Harris and Trump's Campaigns on Facebook and Instagram', 4 November 2024 (Bellingcat investigation)
- EU Regulation 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising

8. RIGHT TO THE FREEDOM OF ASSEMBLY

Outline of this chapter

This chapter explains the applicability and scope of protection of the right to assembly. It then unpacks how new technologies impact the exercise of the right to assembly.

More specifically, this chapter addresses:

- the relevant law concerning the right to assembly (section 8.1)
- the protective scope of the right to assembly (section 8.2)
- restrictions imposed to the right to assembly (section 8.3)
- how new technologies impact the exercise of the right to assembly with a special focus on implications of technology-enabled surveillance, including the chilling effect (section 8.4)

Case study: Navigate360

E Gaumond and C Régis, Assessing Impacts of AI on Human Rights: It's Not Solely About Privacy and Nondiscrimination**, Lawfare, 27 January 2023**

Navigate360 (formerly known as Sentinel) is another striking example of the potential impact of AI on freedom of assembly. It's an AI system that scans social media and geolocation data to produce reports on topics such as potential threats of violence or suicide to help U.S. colleges keep their campuses safe. Although Navigate360 denies it, an investigation conducted by the Pulitzer Center's AI Accountability Network revealed that the company boasted in promotional materials and emails that its technology is used by several university administrations to "forestall potential volatile protests/demonstrations."

The Harvard Crimson, Social Sentinel and the Creeping Surveillance University, 18 October 2022

At least 37 universities [in the US] have been confirmed as clients of Social Sentinel (also known by its new, rebrand-attempting name, Navigate 360), a technology monitoring company that tracks students' social media behavior with the stated intention of identifying risks of self-harm or violence on campuses and alerting administrators.

The purported goal is admirable. Yet the chosen method — invasive, sweeping surveillance — is entirely inappropriate for the problem at hand. Worse still, the institutions using the service do not seem exclusively concerned with improving mental health. Sentinel's services have, in fact, reportedly been deployed in far more nefarious contexts, following buzzwords like "protest" on social media and even scavenging one student's social media posts after she alleged that administrators at North Carolina A&T mishandled her rape allegation.

Universities seem to be using Social Sentinel whenever surveillance might make their lives easier, even if doing so makes students' lives worse. Meanwhile, many affected students aren't even aware that such surveillance is occurring.

(8.1) Relevant law

(8.1.1) Article 21 International Covenant on Civil and Political Rights

The right of peaceful assembly shall be recognized. No restrictions may be placed on the exercise of this right other than those imposed in conformity with the law and which are necessary in a democratic society in the interests of national security or public safety, public order (ordre public), the protection of public health or morals or the protection of the rights and freedoms of others.

(8.1.2) Article 11 ECHR – Freedom of assembly and association

1. Everyone has the right to freedom of peaceful assembly and to freedom of association with others, including the right to form and to join trade unions for the protection of his interests.

2. No restrictions shall be placed on the exercise of these rights other than such as are prescribed by law and are necessary in a democratic society in the interests of national security or public safety, for the prevention

of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others. This Article shall not prevent the imposition of lawful restrictions on the exercise of these rights by members of the armed forces, of the police or of the administration of the State.

(8.2) The Protective Scope of the Right to Freedom of Assembly

UN Human Rights Committee, General comment No. 37 (2020) on the right of peaceful assembly (article 21), 17 September 2020, UN Doc CCPR/C/GC/37

1. The fundamental human right of peaceful assembly enables individuals to express themselves collectively and to participate in shaping their societies. The right of peaceful assembly is important in its own right, as it protects the ability of people to exercise individual autonomy in solidarity with others. Together with other related rights, it also constitutes the very foundation of a system of participatory governance based on democracy, human rights, the rule of law and pluralism. Peaceful assemblies can play a critical role in allowing participants to advance ideas and aspirational goals in the public domain and to establish the extent of support for or opposition to those ideas and goals. Where they are used to air grievances, peaceful assemblies may create opportunities for the inclusive, participatory and peaceful resolution of differences

[...]

4. The right of peaceful assembly protects the non-violent gathering by persons for specific purposes, principally expressive ones. It constitutes an individual right that is exercised collectively. [...]

[...]

6. Article 21 of the Covenant protects peaceful assemblies wherever they take place: outdoors, indoors and online; in public and private spaces; or a combination thereof. Such assemblies may take many forms, including demonstrations, protests, meetings, processions, rallies, sit-ins, candlelit vigils and flash mobs. They are protected under article 21 whether they are stationary, such as pickets, or mobile, such as processions or marches.

(8.3) Restrictions to the Right of Freedom of Assembly

UN Human Rights Committee, General comment No. 37 (2020) on the right of peaceful assembly (article 21), 17 September 2020, UN Doc CCPR/C/GC/37

36. While the right of peaceful assembly may in certain cases be limited, the onus is on the authorities to justify any restrictions. Authorities must be able to show that any restrictions meet the requirement of legality, and are

also both necessary for and proportionate to at least one of the permissible grounds for restrictions enumerated in article 21 [...]. Where this onus is not met, article 21 is violated. The imposition of any restrictions should be guided by the objective of facilitating the right, rather than seeking unnecessary and disproportionate limitations on it. Restrictions must not be discriminatory, impair the essence of the right, or be aimed at discouraging participation in assemblies or causing a chilling effect.

[...]

38. [...] Blanket restrictions on peaceful assemblies are presumptively disproportionate

[...]

40. Article 21 provides that any restrictions must be "necessary in a democratic society". Restrictions must therefore be necessary and proportionate in the context of a society based on democracy, the rule of law, political pluralism and human rights, as opposed to being merely reasonable or expedient. Such restrictions must be appropriate responses to a pressing social need, relating to one of the permissible grounds listed in article 21. They must also be the least intrusive among the measures that might serve the relevant protective function. Moreover, they must be proportionate, which requires a value assessment, weighing the nature and detrimental impact of the interference on the exercise of the right against the resultant benefit to one of the grounds for interfering. If the detriment outweighs the benefit, the restriction is disproportionate and thus not permissible.

41. The last part of the second sentence of article 21 sets out the legitimate grounds on which the right of peaceful assembly may be restricted. This is an exhaustive list, consisting of the following grounds: the interests of national security; public safety; public order (ordre public); the protection of public health or morals; or the protection of the rights and freedoms of others.

[...]

(8.4) New Technologies and the Right to Assembly

(8.4.1) Potential of and challenges by new technologies

Report of the United Nations High Commissioner for Human Rights, Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests, 24 June 2020, UN Doc A/HRC/44/24

7. New technologies, in particular ICT, have a positive, transformative potential. These technologies enable people to exercise the right of peaceful assembly and related rights through their use: in mobilizing for and organizing peaceful protests; in forming networks and coalitions; and in becoming better informed about assemblies and the reasons behind them, thus driving social change. New technologies may also be useful in increasing transparency and accountability for violations and abuses that may occur during protests.

[...]

17. Interference with access to and the availability and use of new technologies in the context of peaceful protests poses multiple human rights challenges. Such interference includes the filtering of content related to protests, the blocking of websites or certain platforms used to mobilize protesters, the closure of accounts belonging to activists or organizers, or the shutdown of the Internet and communications networks

(8.4.2) Technology-enabled surveillance and facial recognition

Technology-enabled surveillance has serious ramifications on the effective exercise of the right to peaceful assembly. The discussion also brings to surface aspects of the interdependence of the effective exercise of different rights (e.g., freedom of expression and freedom of assembly, right to privacy and freedom of assembly). For a more detailed account of issues concerning biometric/facial recognition see (3.5).

(8.4.2.1) Report of the United Nations High Commissioner for Human Rights, Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests, 24 June 2020, UN Doc A/HRC/44/24

> 24. [...] Technology-enabled surveillance poses significant risks to the enjoyment of human rights in peaceful assemblies and is an important contributor to the shrinking of civic space in many countries. [...]
>
> [...]
>
> 26. The Special Rapporteur on the rights to freedom of peaceful assembly and of association has called for the prohibition of indiscriminate and untargeted surveillance of those exercising their right of peaceful assembly, in both physical and digital spaces. He underscored that surveillance of protesters should only be conducted on a targeted basis, and only when there is reasonable suspicion that they are engaging in or planning to engage in serious criminal offences, based on principles of necessity and proportionality and with judicial supervision. [...]
>
> 33. The use of facial recognition technology to identify persons in the context of assemblies has considerable adverse effects on the rights to privacy, freedom of expression and peaceful assembly, if effective safeguards are not in place. A person's image constitutes one of the key attributes of her or his personality as it reveals unique characteristics distinguishing her or him from other persons. Recording, analysing and retaining someone's facial images without her or his consent constitute interferences with a person's right to privacy. By deploying facial recognition technology at assemblies, these interferences occur on a mass and indiscriminate scale, as this requires the collection and processing of facial images of all persons captured by the camera equipped with or connected to a facial recognition technology system.

(8.4.2.2) UN Human Rights Committee, General comment No. 37 (2020) on the right of peaceful assembly (article 21), 17 September 2020, UN Doc CCPR/C/GC/37

> 61. While the collection of relevant information and data by authorities may under certain circumstances assist the facilitation of assemblies, it must not result in suppressing rights or creating a chilling effect. Any information gathering, whether by public or private entities, including through surveillance or the interception of communications, and the way in which data are collected, shared, retained and accessed, must strictly conform to applicable international standards, including on the right to privacy, and may never be aimed at intimidating or harassing participants or would-be participants in assemblies. Such practices should be regulated by appropriate and publicly accessible domestic legal frameworks that are compatible with international standards and subject to scrutiny by the courts.

(8.4.2.3) Facial recognition technology and the interrelation of the right to assembly with the right to privacy

UN Human Rights Committee, General comment No. 37 (2020) on the right of peaceful assembly (article 21), 17 September 2020, UN Doc CCPR/C/GC/37

> 62. The mere fact that a particular assembly takes place in public does not mean that participants' privacy cannot be violated. The right to privacy may be infringed, for example, by facial recognition and other technologies that can identify individual participants in a crowd. The same applies to the monitoring of social media to glean information about participation in peaceful assemblies. Independent and transparent scrutiny and oversight must be exercised over the decision to collect the personal information and data of those engaged in peaceful assemblies and over its sharing or retention, with a view to ensuring the compatibility of such actions with the Covenant.

(8.4.2.3) Facial recognition technology and the interrelation of the right to assembly with the right to freedom of expression

ECtHR, Glukhin v. Russia, App no 11519/20, 4 July 2023

> 88. [...] The Court [...] considers that the use of highly intrusive facial recognition technology to identify and arrest participants in peaceful protest actions could have a chilling effect in relation to the rights to freedom of expression and assembly.
>
> [...]
>
> 90. [...] the use of highly intrusive facial recognition technology in the context of the applicant's exercising his Convention right to freedom of expression is incompatible with the ideals and values of a democratic society governed by the rule of law, which the Convention was designed to maintain and promote.

(8.4.3) What is the chilling effect?

UK Parliament, Justice and Home Affairs Committee, Inquiry on new technologies and the application of the law, written evidence, submitted by Dr Joe Purshouse et al

> 10. [Facial Recognition Technology (FRT)] may have a 'chilling effect' on public assemblies, freedom of expression, and the general use of public space by certain communities and demographics. Overt surveillance can damage legitimate political mobilisations in public space by undermining the perceived legitimacy of protest groups and limiting their access to resources. Furthermore, the perception of being controlled in the public space breaks down the trust in police and other state institutions. In the United Kingdom, football fans have responded to the use of live FRT at a number of matches by wearing face coverings or holding up signage to protest its use. When South Wales Police used live facial recognition at a football match between Cardiff City and Swansea City in January 2020, this prompted condemnation from football supporters' groups and civil liberties campaigners who argued that its use on football fans was unduly stigmatising.

(8.4.3.1) Accounting for, and incorporating, the chilling effect in data protection impact assessments?

Information Commissioner's Opinion, The use of live facial recognition technology in public places, 18 June 2021

Identifying and assessing the risks and potential impacts of [Live Recognition Technology (LRT)] is a highly context-specific process. The controller should pay close attention to the specific circumstances of their processing. The focus is on the potential for the deployment of LFR to cause any type of direct or indirect impact, and material or non-material damage.

Where LFR is used for the automatic collection of biometric data in public places, controllers should consider at least any potential:

- inability to exercise any legal rights;
- inability to exercise any specific data protection rights, including the right to be informed, the right of access and the right to object;
- inability to opt-out of the processing;
- loss of control over the use of personal data;
- inability to access services or opportunities; and
- direct or indirect impact on individuals' ability to exercise their rights and freedoms in this public setting, such as freedom of expression, assembly and association, including any potential inhibiting effect.

Further readings/resources

- M Hamilton, 'The Meaning and Scope of "Assembly" in International Human Rights Law' (2020) 69 ICLQ 521
- I Siatitsa, 'Freedom of Assembly under Attack: General and Indiscriminate Surveillance and Interference with Internet Communications' (2020) 913 International Review of the Red Cross
- Have a look at the work of the UN Special Rapporteur on freedom of peaceful assembly and of association, including the annual thematic reports.
- For a **gendered perspective on peaceful assembly**, read the report Celebrating women in activism and civil society: the enjoyment of the rights to freedom of peaceful assembly and of association by women and girls by the UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, UN Doc A/75/184, 20 July 2020
- For the exercise of the rights to freedom of peaceful assembly and of association as essential to advancing **climate justice**, read the report by the UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, UN Doc A/76/222, 23 July 2021

PART II: DATA PROTECTION AND THE GDPR

9. DATA PROTECTION AS A FUNDAMENTAL RIGHT

Outline of this chapter

In this chapter we will focus on the development of the right to data protection in the European Union. The protection of personal data emerged as a fundamental right which is closely linked to but distinct from the right to privacy. Where the right to privacy encompasses a broad range of protections in the realm of personal autonomy and freedom from intrusive measures, data protection under EU law has a rather specialised role. The right to data protection focuses on the control, processing and security of personal information, and by extension – the natural persons to whom this information refers.

We will first focus our attention on similarities and differences between human rights and fundamental rights. Such analysis will be useful to better understand the nature of data protection and privacy, as well as the emerging challenges within the scope of these rights.

The main goal of this chapter is to give the reader insight into the growing importance of data protection – not only as an independent right, but also as an instrument for upholding other fundamental rights. Maintaining stability and balance in the digital world is challenging, and it begins with a clear recognition of the core principles of the right to data protection.

The topics covered are:

- Human Rights and Fundamental Rights (9.1)
- Some historical highlights (9.2)
- Right to Privacy v. Right to Data Protection (9.3)
- Lawful limitation of the right to data protection (9.4)

9.1 Human Rights and Fundamental Rights

As already discussed in the first part of this book, human rights can be found in international law and are considered inherent to all human beings. They should be universally applied irrespective of nationality, race, ethnicity, religion, gender, sexual orientation, etc. Often human rights are enshrined in international treaties – such as, for example, the UDHR, the ICCPR, the ICESCR and the ECHR. Human rights can also be found in customary international law and general principles of international law.

Fundamental rights are those used in constitutional context. They could be specific to a domestic legal order and therefore be subject to varying approaches and protections depending on the State's law. Often when a State ratifies an international treaty and becomes party to it, it will transpose international law human rights into domestic law fundamental rights. In this sense, fundamental rights are not universal, but they are applicable to individuals belonging to a national/regional legal framework. The European Union has chosen to use the term "fundamental rights" to describe the obligations of Member States toward persons residing in the Union.

9.2 Some historical highlights

After World War II, human rights frameworks were established without considering data protection. The emphasis was placed on the right to privacy. An example of this development is the European Convention on Human Rights (ECHR), adopted in 1950 by the Council of Europe. Art. 8 ECHR was adopted as a classic negative right, meant to protect citizens from arbitrary interference into their personal "sphere". Due to the dynamic nature of the ECHR, the personal sphere is capable of encompassing multiple aspects – private and family life, home and correspondence. Nowadays, the aspects of privacy that might be interfered by surveillance as well as the separation of subcategories have increased due to the development of technology. For example, one could think of: (i) privacy of the person concerned with the privacy of an individual's body; (ii) privacy of personal behaviour; (iii) privacy of personal communication; (iv) privacy of personal data; (v) privacy of location and space; (vi) privacy of association; and (vii) privacy of thoughts and feelings. Chile, is the first country in the world to have included the protection of neurorights in their Constitution.

However, the right to privacy emerged well before the rise of the information society. The latter subsequently introduced new risks to privacy, particularly in the realm of "informational privacy". This necessitated a development of specific and proactive rules governing the collection and use of personal information. It is also in this context that the right to data protection emerged as an independent such.

9.3 Right to Privacy v. Right to Data Protection

The right to privacy is a widely recognised human right – one that has received recognition at the international level and is included in multiple international human rights treaties. As already mentioned, the right to privacy is contained in art. 8 ECHR and art. 7 EU CFR. The right is also present in art. 7 of the American Convention on Human Rights. Interestingly, an explicit right to privacy is not mentioned in the African Charter on Human and People's Rights. However, it can be argued that such a right can be read into the text of the African Charter through the right to respect for life and integrity of the person (art. 4). Nonetheless, the right to privacy has also been deemed a standard of public international law, as one of the modern pillars of democracy, safeguarding autonomy and dignity.

Alongside the right to privacy, a more considerably recent right is the one to data protection. The right to data protection is not internationally recognised as a human right. It is rather a fundamental right established within *inter alia* the EU legal framework, art. 8 EU CFR. This means that the right to data protection is not a universal right – it is only applicable as a separate right insofar as countries have introduced it in their domestic legal systems. In order to understand the historical development of the right, it is worth mentioning that some jurisdictions had introduced legal frameworks on data protection even before the Council of Europe or the EU established its own recognition of the right. Notable examples are the *1970 Data Protection Statute* introduced by the State of Hesse (at the time in the Western part of Germany) and the *1973 Data Protection Act* introduced in Sweden (information in English available here).

At an international level the protection of personal data was first introduced in 1981 in the Council of Europe Convention 108. The Convention introduced various principles for the processing of personal data. It only entered into force in 2004 and until this day, it is the only legally binding international instrument in the field of personal data protection ratified by 44 countries (including 8 countries that are not members of the Council of Europe).

Presently, fundamental rights, included in the EU Charter of Fundamental Rights, as for example: the right to life, prohibition of torture, the right to private life, etc. are not directly reflected in the EU Treaties and secondary laws. The right to protection of personal data makes an exception. The right is reflected in the Treaty on the Functioning of the European Union (art. 16) and in secondary legislation (eg. GDPR, LED, etc.). This is linked historically with the nature of the European Union as an economic organisation, not a strictly speaking an organisation created for safeguarding human rights or fundamental rights. Thus, because personal data have intrensic eonomic value in the data economy, the right to data protection is viewed as naturally belonging to the field of competencies of the EU and has obtained more attention in the EU than other fundamental rights in the Charter.

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://opentextbooks.rug.nl/dataprotectionanddigitalhumanrights/?p=44#h5p-3

The current data protection secondary law in the Europen Union, was adopted in 2016 and became applicable and enforcable as of 25 May 2018. It includes, among other laws, the 'General Data Protection Regulation' (GDPR) and the 'Law Enforcement Directive' (LED) for the police and criminal justice sector. The data protection laws were adopted as an essential step to strengthening citizens' fundamental rights in the digital age and to facilitate business by simplifying rules for companies in the Digital Single Market. At the time of writing, a reform of the GDPR has been initiated by the European Commission. The reform will touch upon two aspects of the GDPR: (i) procedural rules relating to the enforcement of the GDPR; (ii) changes to record-keeping obligations.

As a result of all these legislative developments, the right to data protection has been separated from the right to privacy in the EU. This can be noted also in the wording of the law itself. While the pre-decesor of the GDPR, the Data Protection Directive (1995) made a direct link between the right to privacy and data protection in its art. 1, the GDPR does not mention the right to privacy in any of the articles. The right to privacy is only mentioned once in the Preamble of the GDPR (recital 4), together with other fundamental rights listed in the EU CFR.

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://opentextbooks.rug.nl/dataprotectionanddigitalhumanrights/?p=44#h5p-4

GDPR, Recital 4: The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. *This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the*

> *respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.*

Being a fundamental right, data protection does not just protect personal data. It protects individuals – the natural leaving persons, to whom the personal data belong. As such, it *results* in a broader protection of values such as dignity, personality, non discrimination and democracy and it serves as an "essential prerequisite" for the exercise of other human or fundamental rights. In today's data driven world, protecting personal data increasingly determines to what extent other rights can be protected and enjoyed by individuals.



An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://opentextbooks.rug.nl/dataprotectionanddigitalhumanrights/?p=44#h5p-5

9.4 Lawful limitation of the right to data protection

The right to data protection within the EU is enshrined in art. 8 EU CFR and in art. 16 TFEU. Both of these instruments are primary law of the European Union codifying the existence of the right to data protection. The EU Charter, is the legal instrument which establishes the protection of fundamental rights across the Union and prescribes also the conditions for lawful interference with these rights. Most fundamental rights are, indeed, not absolute and subject to limitation. Such limitation, however, cannot be arbitrary and has to abide by art. 52(1) EU CFR.

> **1.** *Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the*

principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

2. Rights recognised by this Charter for which provision is made in the Treaties shall be exercised under the conditions and within the limits defined by those Treaties.

3. In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.

4. In so far as this Charter recognises fundamental rights as they result from the constitutional traditions common to the Member States, those rights shall be interpreted in harmony with those traditions.

5. The provisions of this Charter which contain principles may be implemented by legislative and executive acts taken by institutions, bodies, offices and agencies of the Union, and by acts of Member States when they are implementing Union law, in the exercise of their respective powers. They shall be judicially cognisable only in the interpretation of such acts and in the ruling on their legality.

6. Full account shall be taken of national laws and practices as specified in this Charter.

7. The explanations drawn up as a way of providing guidance in the interpretation of this Charter shall be given due regard by the courts of the Union and of the Member States.

Art. 52 EU CFR generally deals with the limitation and interpretation of the rights contained in the EU Charter. In its first paragraph, the article codifies established jurisprudential practice – namely, that fundamental rights can, under specific circumstances, be interfered with.[1] The article's unique position within the Charter serves as a general limitation clause and is thus applicable to art. 8 – the right to data protection. So long as a limitation complies with art. 52(1) EU CFR and its requirements, it is to be considered lawful.

1. Case C-292/97 *Kjell Karlsson and Others* [2000] ECLI:EU:C:2000:202, para 45.

Should the EU CFR be applicable in accordance with art. 51(1) CFR, violations and complaints for these violations must **A)** fall within the scope of a right (*ratione personae, materiae, and tempore*); **B)** prove an interference has occurred; **C)** analyse whether the interference can be justified in the meaning of art. 52(1) CFR.

The test for lawful limitation in art. 52(1) CFR contains the following cumulative conditions:

1. The limitation must be provided for by law;
2. The limitation must respect the essence of the right;
3. The limitation must be proportionate;
4. The limitation must have the objective of a general interest recognized by the Union or the protection of the rights and freedoms of others (and genuinely meet this objective).

Condition 1: provided for by law

This condition is an essential feature of the rule of law and is similar to the "prescribed by law" requirement contained in provisions of the ECHR. Within the Union legal framework, the concept of "law" can be interpreted broadly, encompassing primary and secondary EU legislation, national legislation – written and unwritten, so long as these legal rules are *adequately accessible,* formulated with *sufficient precision* and *foreseeable*. The law serving as basis for interference must be in force and legal in itself.[2]

Condition 2: respect for the essence of the right

This criteria is undoubtedly the most difficult to define and thus apply. While it is clear from the wording of art. 52(1) CFR that affecting the essence of a right is unlawful, not much more is provided in terms of defining the concept of "essence". Essence is the inalienable core of a right, but what forms the core? It is subject to

2. Tobias Lock, 'Article 52 CFR', in Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (online edn, OUP 2019) 2249-2250 <https://doi-org.proxy-ub.rug.nl/10.1093/oso/9780198759393.003.577>accessed 23 March 2025.

scholarly debate whether the notion carries independent absolute weight or whether it should/could also be subjected to a balancing exercise with, e.g., other fundamental rights.[3]

The CJEU has also not been too clear about what defines and constitutes "essence" of a fundamental right. In joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Others*, the CJEU ruled that Directive 2006/24/EC on data retention violated fundamental rights under the EU CFR. The Directive required telecommunications providers to retain metadata (e.g., call logs, location data) for up to 24 months, which the Court found to be a *disproportionate* and *generalized interference* with privacy and data protection rights (arts. 7 and 8 EU CFR). The concept of "essence" was mentioned and considered, however it was decided that it was not infringed, eventhough the Directive was declared invalid.

Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* EU:C:2014:238

Relevant paragraphs:

- **[38]** *Article 52(1) of the Charter provides that any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.*
- **[39]** *So far as concerns the essence of the fundamental right to privacy and the other rights laid down in Article 7 of the Charter, it must be held that, even though the retention of data required by Directive 2006/24 constitutes a particularly serious interference with those rights, it is not such as to adversely affect the essence of those rights given that, as follows from Article 1(2) of the directive, the directive does not permit the acquisition of knowledge of the content of the electronic co munications as such.*
- **[40]** *Nor is that retention of data such as to adversely affect the essence of the*

3. Lock (n 2), 2251; Maja Brkan, 'The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core' (2018) 14(2) European Constitutional Law Review 332, 335-338 <https://doi.org/10.1017/S1574019618000159> accessed 23 March 2025.

fundamental right to the protection of personal data enshrined in Article 8 of the Charter, because Article 7 of Directive 2006/24 provides, in relation to data protection and data security, that, without prejudice to the provisions adopted pursuant to Directives 95/46 and 2002/58, certain principles of data protection and data security must be respected by providers of publicly available electronic communications services or of public communications networks. According to those principles, Member States are to ensure that appropriate technical and organisational mesures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data.

- **[59]** *Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.*
- **[60]** *Secondly, not only is there a general absence of limits in Directive 2006/24 but Directive 2006/24 also fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law.*
- **[61]** *Furthermore, Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use (...)*
- **[62]** *In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued (...)*
- **[63]** *Thirdly, so far as concerns the data retention period, Article 6 of Directive*

2006/24 requires that those data be retained for a period of at least six months, without any distinction being made between the categories of data set out in Artcle 5 of that directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned.

- **[65]** *It follows from the above that Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.*
- **[66]** *Moreover, as far as concerns the rules relating to the security and protection of data retained by providers of publicly available electronic communications services or of public communications networks, it must be held that Directive 2006/24 does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. In the first place, Article 7 of Directive 2006/24 does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality. Furthermore, a specific obligation on Member States to establish such rules has also not been laid down.*
- **[69]** *Having regard to all the foregoing considerations, it must be held that, by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter.*
- **[73]** *... Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC is invalid.*

In another judgement, *Schrems I*, the CJEU ruled on the violation of the condition of 'essence of the right'. A comparison of the CJEU reasoning in both cases shows that the Court links the essence of the right to the

existence or the lack thereof of the possibility for an individual to pursue legal remedies for the protection of the right.

Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* EU:C:2015:650

- **[94]** *In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter* (see, to this effect, judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 39).
- **[95]***Likewise, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. The first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law* (see, to this effect, judgments in *Les Verts* v *Parliament*, 294/83, EU:C:1986:166, paragraph 23; *Johnston*, 222/84, EU:C:1986:206, paragraphs 18 and 19; *Heylens and Others*, 222/86, EU:C:1987:442, paragraph 14; and *UGT-Rioja and Others*, C-428/06 to C-434/06, EU:C:2008:488, paragraph 80).

Condition 3: Proportionality

The principle of proportionality is a general principle of EU law. An assessment of proportionality with reference to human rights often aims to achieve and rationalize legal discourse. Proportionality is assessed through its own set of steps.

Stage 1 ***Does the interferring measure follow a legitimate goal ?***

A measure interfering with a fundamental right can only be justified if it pursues a *legitimate goal*, an objective of a general interest recognized by EU law. Such objectives, broadly speaking, are contained in art. 3 TEU, art. 4(1) TEU, art. 35(3) TFEU, art. 36 TFEU, art. 346 TFEU. In the context of the right to data

protection, more details about objectives of general interest will be provided in Condition 4 below. Generally, so long as the measure is not arbitrarily applied, it usually passes the *legitimate purpose* stage.

Stage 2 ***Is the interferring measure appropriate and suitable for reaching the legitimate goal?***

Any measure restricting fundamental rights must be first of all appropriate or suitable to protect the interests that require protection. A measure is considered as *appropriate and suitable* for reaching a goal if there is a rational connection, a real contribution towards achieving the legitimate goal.

Stage 3 ***Is the interferring measure necessary for reaching the legitimate goal?***

The necessity requirement usually is twofold in itself. On the one hand, analysis by the CJEU will be conducted to establish *whether there were less intrusive measures* which could have been taken. The "intruder" of the fundamental right has to substantiate the choice of action. This threshold is much higher to achieve. On the other hand, necessity also encompasses proportionality *stricto sensu*, which requires a balancing exercise of competing interests. This balancing is especially complex as it supposes that a comparison must be made between, e.g., two fundamental rights. How does one weigh one fundamental right against another?

It needs to be kept in mind though, that the CJEU does not always distinguish between the second and the third step of the test. Sutability and necessity are often discussed together within the umbrella of proportionality.

Condition 4: Objectives of general interest & rights of others

Restrictions to the right of data protection are further specified in art. 23 GDPR. The article serves as a *lex specialis* by providing specific grounds under which Union or Member State law may restrict certain data protection rights and obligations to safeguard important objectives of general public interest.

Article 23 GDPR

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

a. national security;

b. defence;

c. public security;

d. the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

e. other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;

f. the protection of judicial independence and judicial proceedings;

g. the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

h. a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

i. the protection of the data subject or the rights and freedoms of others;

j. the enforcement of civil law claims.

9.5 Conclusion

The right to data protection in Union law, enshrined in art. 8 of the EU CFR and art. 16 TFEU, is a distinct fundamental right that ensures that natural living persons have control over their personal data and the way the data is processed. While closely related to the right to privacy under art. EU 7 CFR and art. 8 ECHR, the right to data protection in the EU has a number of characteristics that make it distinguished. The right focuses primarly on the lawful processing of personal data, the transparency of such processing as well as on the accountability of controllers rather than just providing the conditions for non interference. Unlike privacy, which protects against unjustified intrusions, data protection establishes proactive safeguards and positive obligations when handling personal data. Similarly to the right to privacy, data protection is not an absolute right – it can be lawfully restricted provided that any interference is in comliance with the conditions provided by the law. The importance of the right extends beyond individual autonomy, playing a crucial role in democratic governance, digital economy regulation and fundamental rights protection in an era of mass data collection and AI-driven decision-making.

Brainstorming Exercise

- Can you think of potential situations where there is an interference with the right to privacy or with the right to data protection but not an interference with both rights at the same time?
- Do you think the distinction between the right to privacy and the right to data protection in the EU has any merits, or it is just a legal complication?

Extra readings

Milaj, J. (2020). Safeguarding Privacy by Regulating the Processing of Personal Data – An EU Illusion? *European Journal of Law and Technology*, 11(2).

Brkan, M. (2018) The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its C ore *European Constitutional Law Review,* 14(2).

Lock, T. (2019) Article 52 CFR, in Kellerbauer, Klamert and Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary*

10. GDPR - SCOPE AND OBJECTIVES

Outline of this chapter

In this chapter we will take a closer look into the scope of application of the GDPR. The GDPR is a pioneering and comprehensive legal instrument in the field of data protection, building upon the 1995 Data Protection Directive. While it is not the first legislative initiative in the field of data protection, it marks a significant evolution by establishing enforceable, directly applicable rules with (potentially) global reach. Thus, to truly understand its inner workings, the focus of this chapter shall be the foundations of the Regulation.

Firstly, we will outline the application of the GDPR, beginning with its subject matter and objectives. We will understand the meaning of personal data as well as special categories of data. Further information will discuss its temporal, material, and territorial scope. While this information may seem elementary and thus relatively straightforward, we will see that this is not always the case.

The topics covered are:

- GDPR: Subject matter and objectives (10.1)
- GDPR: Temporal, material and territorial scope (10.2)

10(1) GDPR: Subject Matter and Objectives

The GDPR is a EU regulation which build upon its predecessor – the 1995 Data Protection Directive. At the time the Directive was adopted, there was no specific legal bases in the EU treaties that would allow for the adoption of legislation in the field of data protection. Thus, the Directive was adopted on the bases of the general legal basis that can be now found in Article 114(1) TFEU for the purpose of maintaining and safeguarding the proper functioning of the internal market. With the adoption of the Lisbon treaty in 2009, Article 16 TFEU introduced a specific legal bases for legislating in the field of data protection within the

Union. Article 16 TFEU serves as a legal basis to the GDPR shifting the focus and purpose of the lega; instrument from internal market regulation to the protection of fundamental rights.

The adoption of a regulation instead of a directive is also of importance – as a regulation, the GDPR is directly applicable in a uniform manner across the Member States. Thus, a better harmonisation between laws and practices in the Member States is achieved. This harmonisation benefits controllers of personal data that operate in cross-border situations. Now there is one set of identical rules that they need to follow within the Union and thus there is legal certainty.

A Starting Point: Article 1 GDPR

The first article of the GDPR lays down the general purpose and rationale of the legal instrument. The rules within it relate to the protection of personal data of natural persons when being processed as well as it free movement (Article 1(1)). The recognition of data protection as a separate right from the one to privacy is clearly established in this article. While the 1995 Directive explicitly referred to the right to privacy in article 1(1) referring to data protection as a way for protecting privacy (Art 1(1) Data Protection Directive – *In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their* ***right to privacy with respect to the processing of personal data***), the GDPR only mentions the right to privacy in recital 4, among other fundamental rights that can be effected.

Article 1 GDPR – Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

The third paragraph of the Article refers to the free movement of data within the Union. This provision demonstrates that the internal market aspect still remains relevant for the Regulation, but as a separate and additional objective within it rather than being a leading goal in itself. Collectively, all three subparagraphs of Article 1 summarize the core subject matter of the GDPR.

Intuitively, to gain a comprehensive understanding of these goals one would need to understand the terminology contained in the provisions. Therefore, we turn to Article 4 of the GDPR which provides definitions for purposes of the GDPR.



An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://opentextbooks.rug.nl/dataprotectionanddigitalhumanrights/?p=46#h5p-6

Despite the definition of personal data in the law seems to be quite extensive and clear, the question '*What is personal data?*' has been brought before the Court of Justice of the EU (CJEU) in various situations. This is why the CJEU's interpretation of the GDPR is of crucial importance. Below we will focus on a couple of examples where the nature of data was not so clear at first glance. Moreover, we will turn to the Court's reasoning to better understand the interpretations provided by it.

Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen* EU:C:2010:662

Relevant facts

In *Volker und Markus Schecke and Eifert*, the CJEU considered the legality of EU rules requiring Member States to publish the names, locations, and subsidy amounts received by beneficiaries of agricultural funds. The case arose after two recipients – an agricultural partnership and a full-time farmer – challenged the publication of their data, arguing it infringed their right to data protection.

Legal question(s)

Crucially, the case raised a fundamental question: *Does information relating to professional or economic activity, such as publicly funded business operations, still qualify as personal data subject to protection?*

Court's interpretation

- **[49]** *Article 8(2) of the Charter thus authorises the processing of personal data if certain conditions are satisfied. It provides that personal data 'must be processed fairly for specified*

purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'.

- **[50]** *Moreover, Article 52(1) of the Charter accepts that limitations may be imposed on the exercise of rights such as those set forth in Articles 7 and 8 of the Charter, as long as the limitations are provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.*

- **[51]** *Finally, according to Article 52(3) of the Charter, in so far as it contains rights which correspond to rights guaranteed by the Convention, the meaning and scope of those rights are to be the same as those laid down by the Convention. Article 53 of the Charter further states that nothing in the Charter is to be interpreted as restricting or adversely affecting the rights recognised inter alia by the Convention.*

- **[52]***In those circumstances, it must be considered that the right to respect for private life with regard to the processing of personal data, recognised by Articles 7 and 8 of the Charter, concerns any information relating to an identified or identifiable individual (see, in particular, European Court of Human Rights, Amann v. Switzerland [GC], no. 27798/95, § 65, ECHR 2000-II, and Rotaru v. Romania [GC], no. 28341/95, § 43, ECHR 2000-V) and the limitations which may lawfully be imposed on the right to the protection of personal data correspond to those tolerated in relation to Article 8 of the Convention.*

Remark(s)

Data concerning professional activities is personal data within the meaning of (now) art. 4(1) GDPR.

Case C-434/16 *Peter Nowak v Data Protection Commissioner* EU:C:2017:994

Relevant facts

Peter Nowak, a trainee accountant, failed an exam and requested all personal data held about him from the Institute of Chartered Accountants of Ireland. The Institute refused to provide his exam script, claiming it wasn't personal data. Nowak challenged this with the Data Protection Commissioner, who also rejected his complaint. After the lower courts dismissed his case, the Supreme Court allowed his appeal and referred the issue to the CJEU.

Legal question(s)

The main question was: *Can exam scripts be considered personal data under EU data protection law?*

Court's interpretation

- **[33]** *As the Court has held previously, the scope of Directive 95/46 is very wide and the personal data covered by that directive is varied...*
- **[34]** *The use of the expression 'any information' in the definition of the concept of 'personal data', within Article 2(a) of Directive 95/46, reflects the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject.*

....

- **[37]** *First, the content of those answers reflects the extent of the candidate's knowledge and competence in a given field and, in some cases, his intellect, thought processes, and judgment. In the case of a handwritten script, the answers contain, in addition, information as to his handwriting.*

....

- **[40]** *It is, moreover, equally true that the written answers submitted by a candidate at a professional examination constitute information that relates to that candidate by reason of its content, purpose or effect, where the examination is, as in this case, an open book examination.*
- **[41]** *As is stated by the Advocate General in point 24 of her Opinion, the aim of any examination is to determine and establish the individual performance of a specific person, namely the candidate, and not, unlike, for example, a representative survey,*

to obtain information that is independent of that person.

....

- **[49]** *Accordingly, if information relating to a candidate, contained in his or her answers submitted at a professional examination and in the comments made by the examiner with respect to those answers, were not to be classified as 'personal data', that would have the effect of entirely excluding that information from the obligation to comply not only with the principles and safeguards that must be observed in the area of personal data protection, and, in particular, the principles relating to the quality of such data and the criteria for making data processing legitimate, established in Articles 6 and 7 of Directive 95/46, but also with the rights of access, rectification and objection of the data subject, provided for in Articles 12 and 14 of that directive, and with the supervision exercised by the supervisory authority under Article 28 of that directive.*

....

- **[62]** *In the light of all the foregoing, the answer to the questions referred is that Article 2(a) of Directive 95/46 must be interpreted as meaning that, in circumstances such as those of the main proceedings, the written answers submitted by a candidate at a professional examination and any comments made by an examiner with respect to those answers constitute personal data, within the meaning of that provision.*

Remark(s)

Answers to an exam can fall within the meaning of personal data in (now) art. 4(1) GDPR.

Joined Cases C-141/12 and C-372/12 *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S* EU:C:2014:2081

Relevant facts

The case focused on whether the legal analysis contained in a draft decision (or "minute") in Dutch asylum procedures constituted personal data under Article 2(a) of Directive 95/46. These internal documents included both factual information about the applicant (such as name, date of birth, and ethnicity) and a legal assessment of their application.

Legal question(s)

One of the key questions referred to the CJEU was: *whether such legal analysis, when linked to an identifiable individual, qualifies as personal data under the Directive.*

Court's interpretation

- **[37]** *In this respect, it should be noted that Article 2(a) of Directive 95/46 defines personal data as 'any information relating to an identified or identifiable natural person'.*
- **[38]** *There is no doubt that the data relating to the applicant for a residence permit and contained in a minute, such as the applicant's name, date of birth, nationality, gender, ethnicity, religion and language, are information relating to that natural person, who is identified in that minute in particular by his name, and must consequently be considered to be 'personal data'...*
- **[39]** *As regards, on the other hand, the legal analysis in a minute, it must be stated that, although it may contain personal data, it does not in itself constitute such data within the meaning of Article 2(a) of Directive 95/46.*

Remark(s)

The information contained within the minutes (for example, name, date of birth, nationality, ethnicity, religion, etc.) is personal data within the meaning of (now) art. 4(1) GDPR. However, the legal analysis in a minute, while containing personal data, does not constitute personal data in and of itself.

Case C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* EU:C:2011:771

Relevant facts

In this case, SABAM, a Belgian copyright management organization, sought to compel the internet service provider Scarlet to prevent its users from illegally sharing copyrighted works via peer-to-peer networks. After an initial court ruling confirmed copyright infringement, a later judgment ordered Scarlet to implement a filtering system to block such activities. Scarlet appealed, arguing that installing such a system would require general surveillance of all user communications and the processing of IP addresses. It claimed this would breach EU privacy and data protection laws, as IP addresses are personal data under Directive 95/46 when they can identify individuals.

Legal question(s)

The Belgian court referred the matter to the CJEU and *inter alia*, posed the question *whether IP addresses constitute personal data*.

Court's interpretation

- **[26]** *Lastly, Scarlet considered that the installation of a filtering system would be in breach of the provisions of European Union law on the protection of personal data and the secrecy of communications, since such filtering involves the processing of IP addresses, which are personal data.*

....

- **[50]** *Moreover, the effects of that injunction would not be limited to the ISP concerned, as the contested filtering system may also infringe the fundamental rights of that ISP's customers, namely their right to protection of their personal data and their freedom to receive or impart information, which are rights safeguarded by Articles 8 and 11 of the Charter respectively.*
- **[51]** *It is common ground, first, that the injunction requiring installation of the contested filtering system would involve a systematic analysis of all content and the collection and identification of users' IP addresses from which unlawful content on the network is sent. Those addresses are protected personal data because they allow those users to be precisely identified.*
- **[52]** *Secondly, that injunction could potentially undermine freedom of information since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications. Indeed, it is not contested that the reply to the question whether a transmission is lawful also depends on the application of statutory*

exceptions to copyright which vary from one Member State to another. Moreover, in some Member States certain works fall within the public domain or can be posted online free of charge by the authors concerned.

- **[53]** *Consequently, it must be held that, in adopting the injunction requiring the ISP to install the contested filtering system, the national court concerned would not be respecting the requirement that a fair balance be struck between the right to intellectual property, on the one hand, and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information, on the other.*
- **[54]** *In the light of the foregoing, the answer to the questions submitted is that Directives 2000/31, 2001/29, 2004/48, 95/46 and 2002/58, read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights, must be interpreted as precluding an injunction made against an ISP which requires it to install the contested filtering system.*

Remark(s)

IP addresses are capable of precisely identifying users on the Internet and thus fall within the concept of personal data under (now) art. 4(1) GDPR.

Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* EU:C:2016:779

Relevant facts

Mr. Breyer accessed publicly available websites operated by German federal institutions, which stored user data – including dynamic IP addresses – for security reasons. He challenged this practice, arguing that it violated his data protection rights, and sought an injunction to prevent the storage of his access information. While the first court rejected his claim, the appellate court partially upheld it, ruling that a dynamic IP address, when combined with other data that could identify the user, could constitute personal data if the user had revealed their identity during the

session. However, it held that if only the internet service provider could link the IP to an identity, the IP address alone was not personal data. Both parties appealed, and the German Federal Court referred the matter to the CJEU.

Legal question(s)

The German Federal Court posed the question *whether dynamic IP addresses should be considered personal data under Directive 95/46*.

Court's interpetation

- **[32]** *According to that provision, 'personal data' 'mean any information relating to an identified or identifiable natural person ("data subject")'. Pursuant to that provision, an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.*
- **[33]** *As a preliminary point, it must be noted that, in paragraph 51 of the judgment of 24 November 2011, Scarlet Extended (C-70/10, EU:C:2011:771), which concerned inter alia the interpretation of the same directive, the Court held essentially that the IP addresses of internet users were protected personal data because they allow users to be precisely identified.*
- **[34]** *However, that finding by the Court related to the situation in which the collection and identification of the IP addresses of internet users is carried out by internet service providers.*
- **[35]** *In the present case, the first question concerns the situation in which it is the online media services provider, namely the Federal Republic of Germany, which registers IP addresses of the users of a website that it makes accessible to the public, without having the additional data necessary in order to identify those users.*

....

- **[38]** *In that connection, it must be noted, first of all, that it is common ground that a dynamic IP address does not constitute information relating to an 'identified natural person', since such an address does not directly reveal the identity of the natural person who owns the computer from which a website was accessed, or that of another person who might use that computer.*

....

- **[41]** *The use by the EU legislature of the word 'indirectly' suggests that, in order to treat information as personal data, it is not necessary that that information alone allows the data subject to be identified.*

....

- **[44]** *The fact that the additional data necessary to identify the user of a website are held not by the online media services provider, but by that user's internet service provider does not appear to be such as to exclude that dynamic IP addresses registered by the online media services provider constitute personal data within the meaning of Article 2(a) of Directive 95/46.*

....

- **[47]** *Although the referring court states in its order for reference that German law does not allow the internet service provider to transmit directly to the online media services provider the additional data necessary for the identification of the data subject, it seems however, subject to verifications to be made in that regard by the referring court that, in particular, in the event of cyber attacks legal channels exist so that the online media services provider is able to contact the competent authority, so that the latter can take the steps necessary to obtain that information from the internet service provider and to bring criminal proceedings.*
- **[48]** *Thus, it appears that the online media services provider has the means which may likely reasonably be used in order to identify the data subject, with the assistance of other persons, namely the competent authority and the internet service provider, on the basis of the IP addresses stored.*
- **[49]** *Having regard to all the foregoing considerations, the answer to the first question is that Article 2(a) of Directive 95/46 must be interpreted as meaning that a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person.*

Remark(s)

Dynamic IP addresses do constitute personal data within the meaning of (now) art. 4(1) GDPR where additional data can be provided by legal means and enables the identification of the person.

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://opentextbooks.rug.nl/dataprotectionanddigitalhumanrights/?p=46#h5p-7

Special Categories of Personal Data

The processing of special categories of personal data, often referred to as sensitive data, is governed by Article 9 GDPR. Special categories of data are those capable of revealing a data subject's "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership" as well as "genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation". The proceesing of such data is prohibited in Article 9(1). Recital 51 further explains the reasons for such prohibition. The processing od special categories of data could pose a significant risk to the enjoyment of many of the fundamental rights and freedoms of a person. However, as any rule, art 9 GDPR provides also a list of exceptions. It is possible to process special categories of data if one of the conditions listed in the second paragraph of the article is fulfilled.

GDPR – Recital 51

Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. **The processing**

of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing.
Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

Article 9 GDPR: *Processing of special categories of personal data*

1. Processing of personal data revealing **racial** or **ethnic origin**, **political opinions**, **religious** or **philosophical beliefs**, or **trade union membership**, and the processing of **genetic data**, **biometric data** for the purpose of uniquely identifying a natural person, **data concerning health** or **data concerning a natural person's sex life** or **sexual orientation** shall be **prohibited.**
2. Paragraph 1 shall not apply if one of the following applies:

a) the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

b) processing is **necessary for the purposes of carrying out the obligations and exercising**

specific rights of the controller or of the data subject in the **field of employment and social security and social protection law** in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

c) processing is **necessary to protect the vital interests** of the **data subject** or of **another natural person** where the **data subject is physically or legally incapable of giving consent**;

d) processing is carried out in the course of its **legitimate activities with appropriate safeguards** by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that **the processing relates solely to the members or to former members of the body** or to persons who have regular contact with it in connection with its purposes and that **the personal data are not disclosed outside that body without the consent of the data subjects**;

e) processing relates to personal data which are **manifestly made public by the data subject**;

f) processing is **necessary for the establishment, exercise or defence of legal claims** or whenever courts are acting in their judicial capacity;

g) processing is **necessary for reasons of substantial public interest**, on the basis of Union or Member State law which shall be **proportionate to the aim pursued**, **respect the essence of the right** to data protection and **provide for suitable and specific measures to safeguard** the fundamental rights and the interests of the data subject;

h) processing is **necessary for the purposes of preventive or occupational medicine**, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

i) processing is **necessary for reasons of public interest in the area of public health**, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for **suitable and specific measures to safeguard** the rights and freedoms of the data subject, in particular **professional secrecy**;

j) processing is **necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes** in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for **suitable and specific measures to safeguard** the fundamental rights and the interests of the data subject.

The derogation expressed in Article 9(2) GDPR is further elaborated on in Recitals 52-56. Apparent from the phrasing of Article 9(2) is that the exceptions are to be applied in a strict manner which at all times adheres to the data subject's choices, rights and interests. Special categories of data require a higher standard of security. For example, the concept of "consent" (Article 9(2)(a) GDPR) is described as "explicit consent" – meaning that a data controller/processor must prove that the data subject gave his/her consent in a free, fully informed and capable manner, under no duress or other forms of pressure for one or more specified purposes. In the other cases, where processing of special categories of data is described as "necessary", there still is a firm repetition of the required safeguards one must provide in order to process such data.

The existence of one of the derogations listed under the second paragraph of article 9, does not make the rest of the GDPR requirements obsolete. For example, the fact that a data subject has made sensitive information manifestly public (art 9(2)(e) GDPR), allows for the processing of such data only in compliane with the purpose for which the data was made originally public.

CJEU C-446/21 *Schrems v Meta Platforms Ireland* EU:C:2024:834

Relevant facts

Meta Platforms Ireland (formally known as Facebook) has collected data relating to users' activities outside Facebook, through the use of cookies, social plug-ins, pixels and comparable technologies integrated into third-party websites. Meta processed the collected data to identify users' interests in sensitive topics, such as sexual orientation, and to direct targeted advertising at the users.

Maximilian Schrems was a Facebook user. He never consented to the processing by Meta of his personal data concerning activities outside Facebook. Nonetheless, he received advertisements which, among others, targeted homosexual persons (which was based on Meta's analysis of the interests of Schrems and his friends). Schrems did not disclose his sexual orientation on his Facebook profile, although he had once made it public during a panel discussion that was open to the public.

Relevant question before the CJEU

Question 4 – Is Article 5(1)(b) of the GDPR, read in conjunction with Article 9(2)(e) thereof, to be interpreted as meaning that a statement made by a person about his or her own sexual orientation for the purposes of a panel discussion permits the processing of other data concerning sexual orientation with a view to aggregating and analysing the data for the purposes of personalised advertising?

CJEU's interpretation

[77] *It follows that, for the purposes of the application of the exception laid down in Article 9(2)(e) of the GDPR, it is important to ascertain whether the data subject had intended, explicitly and by a clear affirmative action, to make the personal data in question accessible to the general public (judgment of 4 July 2023, Meta Platforms and Others (General terms of use of a social network), C-252/21, EU:C:2023:537, paragraph 77).*

[78] *In the present case, it is apparent from the order for reference that the panel discussion organised in Vienna on 12 February 2019, in the context of which Mr Schrems made a statement about his sexual orientation, was accessible to the public, who could obtain a ticket to attend the event, subject to seating availability, and that it was streamed. Moreover, a recording of the round table was subsequently published as a podcast, as well as on the Commission's YouTube channel.*

[79] *In those circumstances, and subject to verifications which it is for the referring court to carry out, the possibility cannot be ruled out that that statement, although forming part of a broader discussion and made solely for the purpose of criticising the processing of personal data by Facebook, constitutes an act by which the person concerned in any event manifestly made his sexual orientation public within the meaning of Article 9(2)(e) of the GDPR.*

[80] *In the second place, if the consequence of the fact that the data subject has manifestly made public data concerning his or her sexual orientation is that those data may be processed, by way of derogation from the prohibition laid down in Article 9(1) of the GDPR and in accordance with the requirements deriving from the other provisions of that regulation (see, to that effect, judgment of 24 September 2019, GC and Others (De-referencing of sensitive data), C-136/17, EU:C:2019:773, paragraph 64), that fact alone does not, contrary to the contentions of Meta Platforms Ireland, authorise the processing of other personal data relating to that data subject's sexual orientation.*

[81] *Thus, it would be contrary to the restrictive interpretation that should be made of Article 9(2)(e) of the GDPR to find that all data relating to the sexual orientation of a person fall outside the scope of protection under Article 9(1) thereof solely because the data subject has manifestly made public personal data relating to his or her sexual orientation.*

[82] *Moreover, the fact that a person has manifestly made public information concerning his or her sexual orientation does not mean that that person has given his or her consent within the meaning of Article 9(2)(a) of the GDPR to processing of other data relating to his or her sexual orientation by the operator of an online social network platform.*

[83] *In the light of the foregoing, the answer to the fourth question is that Article 9(2)(e) of the GDPR must be interpreted as meaning that the fact that a person has made a statement about his or her sexual orientation on the occasion of a panel discussion open to the public does not*

authorise the operator of an online social network platform to process other data relating to that person's sexual orientation, obtained, as the case may be, outside that platform using partner third-party websites and apps, with a view to aggregating and analysing those data, in order to offer that person personalised advertising.

It is important to notice that the wording of Article 9(1) GDPR refers to data that reveal sensitive information. The CJEU has interpreted this wording extensively to include not only data that reveal such information directly, but also data that indirectly might reveal information that would fall under one of the listed special categories of data. Furthermore, the strict interpretation of the conditions for making the data public needs to be followed also when the processing of the data is considered as necessary by the law itself (Article 9(2)(g) GDPR).

Case C-184/20 *OT v Vyriausioji tarnybinės etikos komisija* EU:C:2022:601

Relevant facts

OT serves as the director of QP, an establishment governed by Lithuanian law in receipt of public funds. In accordance with national law, OT has an obligation to make public a declaration of private interests that will concern also the spouse. OT refuses to make such declaration public because, among other reasons, it would reveal the sexual orientation.

Relevant question before the CJEU

Question 2 – Must the prohibition of the processing of special categories of personal data established in Article 9(1) of the GDPR, regard being had to the conditions established in Article 9(2), including the condition established in point (g) thereof [..] be interpreted, also with regard to Articles 7 and 8 of the Charter, as meaning that national law may not require the disclosure of data relating to declarations of private interests which may disclose personal data, including data which make it possible to determine a person's political views, trade union membership, sexual orientation and other personal information, and their publication on the website of the controller, providing access to

those data to all individuals who have access to the internet?'

CJEU's interpretation

[122] *Article 8(1) of Directive 95/46 states that Member States are to prohibit the processing of personal data 'revealing' racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data 'concerning' health or sex life. Article 9(1) of the GDPR provides that, inter alia, processing of personal data 'revealing' racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of data 'concerning' health or data 'concerning' a natural person's sex life or sexual orientation, are to be prohibited.*

[123] *As the Advocate General has observed, in essence, in point 85 of his Opinion, whilst the use, in those provisions, of the verb 'reveal' is consistent with the taking into account of processing not only of inherently sensitive data, but also of data revealing information of that nature indirectly, following an intellectual operation involving deduction or cross-referencing, the preposition 'concerning' seems, on the other hand, to signify the existence of a more direct and immediate link between the processing and the data concerned, viewed inherently.*

[124] *Such an interpretation, which would result in a distinction being drawn according to the type of sensitive data at issue, would not, however, be consistent with a contextual analysis of those provisions, in particular with Article 4(15) of the GDPR, according to which 'data concerning health' are personal data related to the physical or mental health of a natural person, including the provision of health care services, which 'reveal' information about his or her health status, and with recital 35 of that regulation, which states that personal data concerning health should include all data pertaining to the health status of a data subject which 'reveal' information relating to the past, current or future physical or mental health status of the data subject.*

[125] *Furthermore, a wide interpretation of the terms 'special categories of personal data' and 'sensitive data' is confirmed by the objective of Directive 95/46 and the GDPR, noted in paragraph 61 of the present judgment, which is to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular of their private life, with respect to the processing of personal data concerning them (see, to that effect, judgment of 6 November 2003, Lindqvist, C-101/01, EU:C:2003:596, paragraph 50).*

[126] *The contrary interpretation would, moreover, run counter to the purpose of Article 8(1) of Directive 95/46 and Article 9(1) of the GDPR, namely to ensure enhanced protection as regards processing which, because of the particular sensitivity of the data processed, is liable to constitute, as follows from recital 33 of Directive 95/46 and recital 51 of the GDPR, a particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, guaranteed by Articles 7 and 8 of the Charter (see, to that effect, judgment of 24 September 2019, GC and Others (De-referencing of sensitive data), C-136/17, EU:C:2019:773, paragraph 44).*

[127] *Consequently, those provisions cannot be interpreted as meaning that the processing of personal data that are liable indirectly to reveal sensitive information concerning a natural person is excluded from the strengthened protection regime prescribed by those provisions, if the effectiveness of that regime and the protection of the fundamental rights and freedoms of natural persons that it is intended to ensure are not to be compromised.*

[128] *In the light of all the foregoing considerations, the answer to the second question is that Article 8(1) of Directive 95/46 and Article 9(1) of the GDPR must be interpreted as meaning that the publication, on the website of the public authority responsible for collecting and checking the content of declarations of private interests, of personal data that are liable to disclose indirectly the sexual orientation of a natural person constitutes processing of special categories of personal data, for the purpose of those provisions.*

Brainstorming Exercises

1. Financial data as well as the buying behaviour of data subjects are not listed as special categories of personal data under Article 9(1) GDPR. Can you think of situations when these type of data will fall under the prohibition of article 9?

2. Do photographs fall under the category of special categories of personal data?

10.2 GDPR: Temporal, Material and Territorial Scope

Temporal scope

The GDPR was adopted on 27 April 2016. As customary, it entered into force 20 days after the publication in the Official Journal, on 24 May 2016. However, as established in Article 99 GDPR, it started to apply only two years after, on 25 May 2018. The period of two years between the entry into force and the enforcement of the law allowed private and public entities to bring all their personal data processing operations in conformity with the new required standards.

Material scope

The material scope of the GDPR can be found in Article 2. Its first paragraph outlines: "*This Regulation **applies** to the processing of personal data **wholly** or **partly** by **automated means** and to the processing **other than by automated means** of personal data which **form part of a filing system** or are **intended to form** part of a filing system*".

The provision is broad and flexible, to encompas a very wide variety of situations. In order to provide better clarity, the second paragraph of the article excplicitly lists those cases which fall outside the scope of the Regulation.

Article 2(2) GDPR: *What falls outside the material scope of application?*

This Regulation does **not** apply to the processing of personal data:

a) in the course of an activity which falls **outside the scope of Union law**;

b) by the **Member States** when carrying out **activities** which fall within the scope of C**hapter 2 of Title V of the TEU**;

c) by a **natural person** in the course of a **purely personal** or **household activity**;

d) by **competent authorities** for the purposes of the **prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties**, including the **safeguarding against and the prevention of threats to public security.**

From the text of the provision it becomes apparent that there are certain categories of processing that will not be governed by the GDPR. The exceptions under points (a) and (b) are quite straight forward.

Point (a) is closely linked with the EU principle of conferral of powers. The EU is a regional international organisation that has recieved from its Member States competences to regulate upon specific areas. As stated in article 4(1) TEU: "*In accordance with Article 5, competences not conferred upon the Union in the Treaties remain with the Member States*." Thus, also the GDPR cannot extend its application in areas that fall outside the scope of application of the GDPR.

Point (b) closely follows the rational of the previous point. Title V Chapter II of TEU, is about the Common Foreign and Security policy where the Member States are on the driving seat. The EU has only special competences in the field and its institutions have limited decision making power.

Point (c) refers to processing by a natural person in the course of purely personal or household activities.

This explicit exclusion from the GDPR rules allows that activities involving the creation and use of, e.g., a personal agenda calendar, a phone book, or a birthay calendar, would be excluded from the scope of the law.

However, any purely personal or household activity must remain for truly private use in order to fall within the exception of Article 2(2)(c) GDPR. What happens when such data contained iniatially in a private manner becomes public is a matter that the Court of Justice of the European Union has addressed in various cases.

Case C-101/01 *Criminal proceedings against Bodil Lindqvist* EU:C:2003:596

Relevant facts

The case concerned Mrs. Lindqvist, a Swedish catechist who created personal webpages to assist parishioners preparing for confirmation. On these pages, she published personal information about herself and 18 colleagues – such as names, roles, hobbies, contact details, and even medical information about one person – without their knowledge or consent. She also linked the pages to the Swedish Church's official website. Swedish authorities prosecuted her for violating the Personal Data Act (PUL), alleging she had processed personal and sensitive data without prior notice to the data protection authority, consent from the individuals concerned, or authorization to transfer data to a third country.

Legal question(s)

Multiple questions were brought before the Court with three of them especially focusing on the consequences of making personal data available in a public (online) manner:

1. *Does entering personal data on a webpage and making it accessible online qualify as "processing of personal data by automatic means" under Directive 95/46?*
2. *Does the processing of personal data such as that described in the first question is covered by one of the exceptions in Article 3(2) of Directive 95/46?*
3. *Does the inclusion of sensitive personal data (such as health information) on a publicly accessible webpage fall under the special categories of data subject to enhanced protection under the Directive?*

Interpretation of the Court

First question (above)

- **[24]** *The term 'personal data' used in Article 3(1) of Directive 95/46 covers, according*

to the definition in Article 2(a) thereof, 'any information relating to an identified or identifiable natural person'. The term undoubtedly covers the name of a person in conjunction with his telephone coordinates or information about his working conditions or hobbies.

- **[25]** *According to the definition in Article 2(b) of Directive 95/46, the term 'processing' of such data used in Article 3(1) covers 'any operation or set of operations which is performed upon personal data, whether or not by automatic means'. That provision gives several examples of such operations, including disclosure by transmission, dissemination or otherwise making data available. It follows that the operation of loading personal data on an internet page must be considered to be such processing.*
- **[26]** *It remains to be determined whether such processing is 'wholly or partly by automatic means'. In that connection, placing information on an internet page entails, under current technical and computer procedures, the operation of loading that page onto a server and the operations necessary to make that page accessible to people who are connected to the internet. Such operations are performed, at least in part, automatically.*
- **[27]** *The answer to the first question must therefore be that the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes 'the processing of personal data wholly or partly by automatic means' within the meaning of Article 3(1) of Directive 95/46.*

Second question (above)

- **[46]** *As regards the exception provided for in the second indent of Article 3(2) of Directive 95/46, the 12th recital in the preamble to that directive, which concerns that exception, cites, as examples of the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, correspondence and the holding of records of addresses.*
- **[47]** *That exception must therefore be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people.*

- **[48]** *The answer to the third question must therefore be that processing of personal data such as that described in the reply to the first question is not covered by any of the exceptions in Article 3(2) of Directive 95/46.*

Third question (above)

- **[50]** *In the light of the purpose of the directive, the expression 'data concerning health' used in Article 8(1) thereof must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the health of an individual.*
- **[51]** *The answer to the fourth question must therefore be that reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health within the meaning of Article 8(1) of Directive 95/46.*

Remark(s)

The act of referring to individuals and identifying characteristics of said individuals on an internet page constitutes "processing of personal data" and due to its public nature does not benefit from the exception of the now Article 2(2)(c) GDPR. Furthemore, publication concerning the injury of an individual on that same internet page constitutes publication of "personal data" within the meaning of the GDPR and is, in fact, a special category of data that would now be governed by Article 9 GDPR.

Brainstorming Exercise

Would publishing of information on Social Media qualify for the exception of the purely personal and household activities as established under Article 2(2)(c) GDPR?

In contrast to the other 3 point, point (d) more than an exception is linked to the fact that to do with the fact that the use of data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and

the prevention of threats to public security requires a special regulation. The Law Enforcement Directive that focuses regulates the use of personal data by competent auuthorities for the purposes mentioned above was adopted in the same package with the GDPR but as a separate piece of lex specialis.

Territorial scope

In a global and digital economy, data travels easily accross borders. Data subjects in the EU benefit from online services offered all around the globe and international companies offer services and products within the EU. Article 3 GDPR focuses on the territorial scope of application of the GDPR.

Article 3 GDPR – Territorial scope

1. This Regulation applies to the processing of personal data in the context of **the activities of an establishment of a controller or a processor in the Union**, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to **the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union**, where the processing activities are related to:
    1. the **offering of goods or services**, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
    2. the **monitoring of their behaviour** as far as their behaviour takes place within the Union.
3. This Regulation applies to the processing of personal data by a controller **not established in the Union, but in a place where Member State law applies by virtue of public international law.**

11. GDPR - PRINCIPLES AND ACTORS

Outline of the chapter

The purpose of this chapter is to introduce the principles that one must follow when processing personal data as well as the legal bases that allow for processing of personal data. Adherence to the foundtional principles is mandatory and so is the choice of an appropriate legal basis in order to ensure that the processing of personal data is lawful. Following this discussion, this chapter will also introduce the main actors and their respective roles assigned to them in the GDPR.

The topics discussed are:

- Important definitions (11.1)
- Principles of data protection (11.2)
- Legal grounds for lawful processing of personal data (11.3)
- The main actors (11.4)

(11.1) Important definitions

To understand the terms and definitions used by the GDPR, one must turn the attention to Article 4 which provides, extensively so, definitions for key terms. Keeping in mind the meanings assigned by the Regulation is crucial in practice for the proper application of the rules subsequently provided.

Article 4 GDPR – Definitions

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

...

(5) 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

...

(7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

(8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

...

(11.2) Principles of data protection

The data protection principles are listed in Article 5 GDPR. These principles are cumulative. When engaging in any data processing activities, a controller and processor must follow all of these principles.

Article 5 GDPR – Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('***lawfulness, fairness and transparency***');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('***purpose limitation***');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('***data minimisation***');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('***accuracy***');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('***storage limitation***');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('***integrity and confidentiality***').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘***accountability***’).

A more detailed explanation of each of these principles, can be found in Recital 39, GDPR. Below, we are breaking the content of this recital to directly explain each of the principles. Furthermore, these principles have been given further elaboration with regards to the rights of data subjects and the obligations of controllers and procesors that will be discussed in the following chapter.

The principle of fairness, lawfulness and transparency – *Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.*

The principle of purpose limitation – *In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data.*

The principle of data minimisation – *The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed.*

The principle of storage limitation – *This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.*

The principle of accuracy – *Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted.*

The principle of integrity and confidentiality (security) – *Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.*

The application of the abovementioned principles is mandatory and cumulative – each must be applies simultaneously with the rest. These principles serve as the backbone of GDPR, ensuring that controllers handle personal data in a respectful, lawful and secure manner. Non-compliance can result in significant penalties and but also in reputational damage.

In Article 5(2) GDPR that prescribes the principle of accountability, it is clearly stated that the burden of proof, to show compliance with the principles of data processing stays with the controller – not with the data subject.

(11.3) Legal grounds for lawful processing of personal data

For the lawful processing of personal data, Article 6 GDPR lists (and thus exhausts) all the possible legal grounds.

Article 6 GDPR – Lawfulness of processing

1. Processing shall be *lawful only* if and to the extent that *at least one of the following applies*:

(a) the data subject has given ***consent*** to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the ***performance of a contract*** to which the data subject is

party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for ***compliance with a legal obligation*** to which the controller is subject;

(d) processing is necessary in order to ***protect the vital interests of the data subject*** *or* ***of another natural person***;

(e) processing is necessary for the ***performance of a task carried out in the public interest*** or in the ***exercise of official authority vested in the controller***;

(f) processing is necessary for the purposes of the ***legitimate interests pursued by the controller or by a third party***, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The lawful grounds for processing personal data are not cumulative. The controller needs to justify the processing of the data on the bases of one of these grounds.

Consent, is the first ground for processing personal data, but it is not the strongest one. According to the EDPB guidlines:

[...] consent can only be an appropriate lawful basis if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them
without detriment. When asking for consent, a controller has the duty to assess whether it will meet
all the requirements to obtain valid consent. If obtained in full compliance with the GDPR, consent is
a tool that gives data subjects control over whether or not personal data concerning them will be
processed. If not, the data subject's control becomes illusory and consent will be an invalid basis for
processing, rendering the processing activity unlawful. [...]

It is important to distinguish simple consent, requested under article 6 GDPR, from explicit consent, requested under article 9(2)(a) GDPR. For better understanding the meaning of simple consent in the framework of data processing activities, one needs to interpret together:

- the definition of 'consent' in article 4(11) GDPR

'**consent**' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

- the conditions for consent provided in article 7 GDPR as well as in article 8 when the data subject is a minor that benefits from information society services

Article 7 GDPR – Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Article 8 GDPR – Conditions applicable to child's consent in relation to information society services

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.
   Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.
2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.
3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

- and the case law of the CJEU

Case C-673/17 *Planet49* EU:C:2019:801

Relevant Facts and legal question

The case concerned a promotional lottery organised by Planet49 on a website. Internet

users wishing to take part in that lottery were required to enter their names and addresses on a web page with checkboxes. The checkbox authorising the installation of cookies contained a preselected tick.

The request for a preliminary ruling concerned the concept of consent.

Court's interpretation

[51] Article 2(h) of Directive 95/46 defines 'the data subject's consent' as being 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'.

....

[54] In particular, Article 7(a) of Directive 95/46 provides that the data subject's consent may make such processing lawful provided that the data subject has given his or her consent 'unambiguously'. Only active behaviour on the part of the data subject with a view to giving his or her consent may fulfil that requirement.

[55] In that regard, it would appear impossible in practice to ascertain objectively whether a website user had actually given his or her consent to the processing of his or her personal data by not deselecting a pre-ticked checkbox nor, in any event, whether that consent had been informed. It is not inconceivable that a user would not have read the information accompanying the preselected checkbox, or even would not have noticed that checkbox, before continuing with his or her activity on the website visited.

....

[62] Active consent is thus now expressly laid down in Regulation 2016/679. It should be noted in that regard that, according to recital 32 thereof, giving consent could include ticking a box when visiting an internet website. On the other hand, that recital expressly precludes 'silence, pre-ticked boxes or inactivity' from constituting consent.

Case C-61/19 *Orange România* EU:C:2020:901

Relevant facts and question before the court

Orange România had concluded contracts in writing for the provision of mobile telecommunications services with individuals and that copies of those persons' identity documents were annexed to those contracts. Orange România has not proven that the customers whose identity documents had been copied and annexed to their contracts had given their valid consent to the collection and storage of copies of their identity documents.

The CJEU was basically asked to clarify the concepts of specific, informed and freely given consent.

The Court's interpretation

[39] In that regard, the first sentence of Article 7(2) of that regulation states that if the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent is to be presented in a manner which is clearly distinguishable from the other matters. In particular, it is apparent from that provision, read in conjunction with recital 42 of that regulation, that such a declaration must be presented in an intelligible and easily accessible form, using clear and plain language, in particular where it concerns a declaration of consent which is to be pre-formulated by the controller of personal data.

[40] As regards the requirement arising from Article 2(h) of Directive 95/46 and Article 4(11) of Regulation 2016/679 that consent must be 'informed', that requirement implies, in accordance with Article 10 of that directive, read in the light of recital 38 thereof, and with Article 13 of that regulation, read in the light of recital 42 thereof, that the controller is to provide the data subject with information relating to all the circumstances surrounding the data processing, in an intelligible and easily accessible form, using clear and plain language, allowing the data subject to be aware of, inter alia, the type of data to be processed, the identity of the controller, the period and procedures for that processing and the purposes of the processing. Such information must enable the data subject to be able to determine easily the consequences of any consent he or she might give and ensure that the consent given is well informed.

....

[46] Since, according to the information in the request for a preliminary ruling, the customers concerned do not appear to have themselves ticked the box relating to that clause, the mere fact that that box was ticked is not such as to establish a positive indication of those customers' consent to a copy of their identity card being collected and stored. As the Advocate General observed in point 45 of his Opinion, the fact that those customers signed the contracts containing the ticked box does not, on its own, prove such consent, in the absence of any indications

confirming that that clause was actually read and digested. It is for the referring court to carry out the necessary investigations to that end.

....

[52] In the light of the foregoing considerations, the answer to the questions referred is that Article 2(h) and Article 7(a) of Directive 95/46 and Article 4(11) and Article 6(1)(a) of Regulation 2016/679 must be interpreted as meaning that it is for the data controller to demonstrate that the data subject has, by active behaviour, given his or her consent to the processing of his or her personal data and that he or she has obtained, beforehand, information relating to all the circumstances surrounding that processing, in an intelligible and easily accessible form, using clear and plain language, allowing that person easily to understand the consequences of that consent, so that it is given with full knowledge of the facts. A contract for the provision of telecommunications services which contains a clause stating that the data subject has been informed of, and has consented to, the collection and storage of a copy of his or her identity document for identification purposes is not such as to demonstrate that that person has validly given his or her consent, as provided for in those provisions, to that collection and storage, where

- the box referring to that clause has been ticked by the data controller before the contract was signed, or where
- the terms of that contract are capable of misleading the data subject as to the possibility of concluding the contract in question even if he or she refuses to consent to the processing of his or her data, or where
- the freedom to choose to object to that collection and storage is unduly affected by that controller in requiring that the data subject, in order to refuse consent, must complete an additional form setting out that refusal.

Case C-129/21 *Proximus* EU:C:2022:833

Relevant facts and legal question

Proximus, a Belgian provider of telephone directories, had received the address data of a data subject from another company, which in return had received the data from the data subject on the

basis of consent. The data subject's consent authorised the disclosure of the data to third parties such as Proximus.

The data subject had then contacted Proximus and requested that his address not be displayed in their directories as well as in the directories of Proximus' partners. However, after the data subject's request had been complied with, the data subject's address reappeared in the Proximus directory due to a "data update" by the company that had originally submitted the data subject's address to Proximus.

Upon a second request from the data subject, Proximus deleted the data again and informed the data subject that it had forwarded the request to all third parties who had received the data subject's data from Proximus.

One of the four legal questions asked on the obligation of a controller when a data subject withdraws consent or asks for the data to be erased based on the right to be forgoten.

Court's reasoning

[96] Accordingly, in circumstances such as those at issue in the main proceedings, it must be concluded that a controller such as Proximus is required, under Article 17(2) of the GDPR, to ensure that reasonable steps are taken to inform search engine providers of the request addressed to it by the subscriber of a telephone service operator for erasure of his or her personal data. However, as the Advocate General observed in point 76 of his Opinion, in order to assess the reasonableness of the steps taken by the provider of directories, Article 17(2) of the GDPR provides that the available technology and the cost of implementation must be taken into account, a task that falls primarily upon the authority competent for such matters, subject to judicial review.

....

[99] In the light of the foregoing considerations, the answer to the fourth question is that Article 17(2) of the GDPR must be interpreted as not precluding a national supervisory authority from ordering a provider of directories – which has been requested by the subscriber of a telephone service operator to cease disclosing personal data relating to him or her – to take 'reasonable steps', within the meaning of that provision, to inform search engine providers of that request for erasure of the data.

It is important not to confuse 'consent' with the lawful ground of article 6(1)(b): 'processing is necessary for the performance of a contract'. For the EDPB, a controller can rely on article 6(1)(b) to process personal data when it can establish both that: "*the processing takes place in the context of a valid contract with the data subject and that processing is necessary in order that the particular contract with the data subject can be performed. Where controllers cannot demonstrate that (a) a contract exists, (b) the contract is valid pursuant to applicable national*

contract laws, and (c) that the processing is objectively necessary for the performance of the contract, the controller should consider another legal basis for processing."

Case C-252/21 *Meta Platforms Inc and Others v Bundeskartellamt* EU:C:2023:537

Relevant facts

The business model of the social network Facebook, owned by Meta, is based on financing through online advertising, which is tailored to its individual users. That advertising is made possible in technical terms by the automated production of detailed profiles in respect of the network users and the users of the online services offered at the level of the Meta group. In order to be able to use that social network, when they register, users must accept the general terms drawn up by Meta Platforms, which refer to the data and cookies policies set by that company. Under those policies, in addition to the data which those users provide directly when they register, Meta Platforms also collects data about user activities on and off the social network and links the data with the Facebook accounts of the users concerned.

Relevant legal question

The referring court asks, in essence, whether and under what conditions point (b) of the first subparagraph of Article 6(1) of the GDPR must be interpreted as meaning that the processing of personal data by the operator of an online social network, may be considered to be necessary for the performance of a contract to which the data subjects are party.

Court's reasoning

[42] Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. … For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

[43] In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to

different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

....

[125] In the light of all the foregoing, the answer to Questions 3 and 4 is that point (b) of the first subparagraph of Article 6(1) of the GDPR must be interpreted as meaning that the processing of personal data by the operator of an online social network, which entails the collection of data of the users of such a network from other services of the group to which that operator belongs or from visits by those users to third-party websites or apps, the linking of those data with the social network account of those users and the use of those data, can be regarded as necessary for the performance of a contract to which the data subjects are party, within the meaning of that provision, only on condition that the processing is objectively indispensable for a purpose that is integral to the contractual obligation intended for those users, such that the main subject matter of the contract cannot be achieved if that processing does not occur.

When the lawful ground of Article 6(1)(f) GDPR is used for processing personal data, one must balance the legitimate interests pursued by the controller with the fundamental rights and freedoms of the data subject which necessitate the protection of his personal data. Such a balancing exercise can be expected to be complex and dynamic. While the EDPB has initially been strict in the interpretation, currently it seems to be more lenient, especially with regards of data scrapping for training AI technology.

Case C-708/18 *Asociaţia de Proprietari bloc M5A-ScaraA* EU:C:2019:1064

Relevant facts

TK lives in an apartment which he owns, located in the building M5A. At the request of certain co-owners of that building, the association of co-owners adopted, at a general assembly a decision approving the installation of video surveillance cameras in that building. TK objected to that video surveillance system being installed, on the ground that it constituted an infringement of the right to respect for private life. The association of co-owners stated that the decision to install a video

surveillance system had been taken in order to monitor as effectively as possible who enters and leaves the building, since the lift had been vandalised on many occasions and there had been burglaries and thefts in several apartments and the common parts. Other measures did not work out.

Courts's reasoning

[40] In that regard, Article 7(f) of Directive 95/46 lays down three cumulative conditions in order for the processing of personal data to be lawful, namely, first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; secondly, the need to process personal data for the purposes of the legitimate interests pursued; and thirdly, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence over the legitimate interest pursued.

[41] It must be stated that Article 7(f) of Directive 95/46 does not require the data subject's consent. Such consent, as a condition to which the processing of personal data is made subject, appears, however, only in Article 7(a) of that directive.

[42] In the present case, the objective which the controller essentially seeks to achieve when he or she installs a video surveillance system such as that at issue in the main proceedings, namely protecting the property, health and life of the co-owners of a building, is likely to be characterised as a 'legitimate interest', within the meaning of Article 7(f) of Directive 95/46. The first condition laid down in that provision appears, therefore, in principle, to be fulfilled.

Exercise

A small online bookstore uses customer purchase history to recommend similar books via email. Customers have not expressly consented to receive marketing emails, but the company believes that sending tailored recommendations improves customer satisfaction and supports its business model. The company includes an unsubscribe link in each email and ensures that data is not shared with third parties.

Can the company rely on Article 6(1)(f) (legitimate interests) as a legal basis for sending these

recommendation emails? What factors should be considered in the balancing test between the company's interest and the rights of the data subjects?

Exercise

A municipal housing office installs motion-activated CCTV cameras in the common areas of public housing buildings to deter vandalism and improve safety. The footage is retained for 30 days and accessed only if an incident is reported. The office does not request consent from tenants, and it does not rely on a specific legal obligation. Instead, it considers the surveillance to be in its legitimate interest, aiming to protect property and residents.

Can the housing office rely on Article 6(1)(f) (legitimate interests) as the legal basis for this processing? What legal or contextual factors might affect this assessment?

(11.4) The main actors

An effective data protection framework requires that there be clearly defined responsibilities for those involved in the processing of personal data. The GDPR establishes particular roles for key actors, most notably the data controller and the processor. Understanding their respective functions, duties and liabilities is essential for ensuring compliance. This section examines how the Regulation defines these roles and allocates responsibility within data processing activities, laying the groundwork for accountability and enforcement. How the breach of obligations affects the controller and processor will be discussed in Chapter 12.

(11.4.1) The role of the controller

The legal obligations of the controller when processing personal data can be found under Article 24 GDPR and they are as follows:

1. Taking into account the *nature*, *scope*, *context* and *purposes of processing* as well as the *risks* of varying likelihood and *severity* for the rights and freedoms of natural persons, the *controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.* Those measures shall be *reviewed* and *updated* where necessary.

2. *Where proportionate* in relation to processing activities, the *measures* referred to in paragraph 1 *shall include the implementation of appropriate data protection policies by the controller.*

3. Adherence to *approved codes of conduct* as referred to in Article 40 or *approved certification mechanisms* as referred to in Article 42 *may* be used as an *element by which to demonstrate compliance* with the obligations of the controller.

Recital 74 refers to the responsibility and liability of controllers in the context of the GDPR. It makes clear that the obligations of the data controller are not mere suggestions – they lead to liability for non-compliance. Furthermore, the data controller must not only show that appropriate measures have been implemented, but he must also be able to demonstrate that they are truly *effective*.

The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

The Regulation in its Article 25 suggests two types of data protection measures that a controller must implement – data protection by design and data protection by default.

Article 25 GDPR – Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, **implement appropriate technical and organisational measures**, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

The GDPR regulates also the possibility of more than one controller to work jointly together and thus, be jointly liable for any GDPR infringements.

Article 26 GDPR – Joint controllers

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. [3]The arrangement may

designate a contact point for data subjects.

2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.
3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

The CJEU has further clarified upon the concept of joint controllers.

Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein* EU:C:2018:388

Relevant facts:

Wirtschaftsakademie offers educational services by means of a fan page hosted on Facebook. Fan pages are user accounts that can be set up on Facebook by individuals or businesses. To do so, the author of the fan page, after registering with Facebook, can use the platform designed by Facebook to introduce himself to the users of that social network and to persons visiting the fan page, and to post any kind of communication in the media and opinion market. Administrators of fan pages can obtain anonymous statistical information on visitors to the fan pages via a function called 'Facebook Insights' which Facebook makes available to them free of charge under non-negotiable conditions of use. That information is collected by means of evidence files ('cookies'), each containing a unique user code, which are active for two years and are stored by Facebook on the hard disk of the computer or on other media of visitors to fan pages. The user code, which can be matched with the connection data of users registered on Facebook, is collected and processed when the fan pages are opened. According to the order for reference, neither Wirtschaftsakademie nor Facebook Ireland Ltd notified the storage and functioning of the cookie or the subsequent processing of the data, at least during the material period for the main proceedings.

Court's reasoning

[35] While the mere fact of making use of a social network such as Facebook does not make a Facebook user a controller jointly responsible for the processing of personal data by that network,

it must be stated, on the other hand, that the administrator of a fan page hosted on Facebook, by creating such a page, gives Facebook the opportunity to place cookies on the computer or other device of a person visiting its fan page, whether or not that person has a Facebook account.

[36] In this context, according to the submissions made to the Court, the creation of a fan page on Facebook involves the definition of parameters by the administrator, depending inter alia on the target audience and the objectives of managing and promoting its activities, which has an influence on the processing of personal data for the purpose of producing statistics based on visits to the fan page. The administrator may, with the help of filters made available by Facebook, define the criteria in accordance with which the statistics are to be drawn up and even designate the categories of persons whose personal data is to be made use of by Facebook. Consequently, the administrator of a fan page hosted on Facebook contributes to the processing of the personal data of visitors to its page.

[37] In particular, the administrator of the fan page can ask for — and thereby request the processing of — demographic data relating to its target audience, including trends in terms of age, sex, relationship and occupation, information on the lifestyles and centres of interest of the target audience and information on the purchases and online purchasing habits of visitors to its page, the categories of goods and services that appeal the most, and geographical data which tell the fan page administrator where to make special offers and where to organise events, and more generally enable it to target best the information it offers.

....

[39] In those circumstances, the administrator of a fan page hosted on Facebook, such as Wirtschaftsakademie, must be regarded as taking part, by its definition of parameters depending in particular on its target audience and the objectives of managing and promoting its activities, in the determination of the purposes and means of processing the personal data of the visitors to its fan page. The administrator must therefore be categorised, in the present case, as a controller responsible for that processing within the European Union, jointly with Facebook Ireland, within the meaning of Article 2(d) of Directive 95/46.

(11.4.2) The role of the processor

As already seen from the list of definitions in article 4 GDPR, the Regulation distinguishes between a controller (art 4(7) GDPR) and a processor (art 4(8) GDPR). While the controller (natural or legal person) is the one that determines the purposes and means of the processing of personal data, the processor is the one (natural or legal person) that processes the data on behalf of the controller. Undoubtedly, the roles are often overlaping and are covered by the same entity. Actually, other jurisdictions that have introduced their data

protection laws inspired by the GDPR, do not always make the distinction between these two actors but use umbrella definitions like 'data handlers' or 'entrusted parties'.

The distinction between the two actors in the GDPR framework is mirrored in the distinct responsibilities that they have when processing personal data.

Article 28 GDPR – Processor

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 32;

(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions [...]

Thus, according to the GDPR provisions, the processor operates under clear and strict guidance from the controller. If the processor decides by itself the purposes and means of processing, then it is considered a controller for that specific processing activity.

Article 28(10) GDPR – Processor

Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Article 29 GDPR – Processing under the authority of the controller or processor

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

The complicated relationship between controller and processor with regards to operators of search engines, was clarified by the CJEU in the Google Spain case. While Google originally claimed that serch engines qualify only as processors of information that other controllers have made available on internet, the CJEU reasoned that search engine qualify as processors and controllers at the same time. This is important since the GDPR places most of the responsibilities on controllers and not on processors.

Case C-131/12 *Google Spain* EU:C:2014:317

[22] According to Google Spain and Google Inc., the activity of search engines cannot be regarded as processing of the data which appear on third parties' web pages displayed in the list of search results, given that search engines process all the information available on the internet without effecting a selection between personal data and other information. Furthermore, even if that activity must be classified as 'data processing', the operator of a search engine cannot be regarded as a 'controller' in respect of that processing since it has no knowledge of those data and does not exercise control over the data.

[23] On the other hand, Mr Costeja González, the Spanish, Italian, Austrian and Polish Governments and the European Commission consider that that activity quite clearly involves 'data processing' within the meaning of Directive 95/46, which is distinct from the data processing by the publishers of websites and pursues different objectives from such processing. The operator of a search engine is the 'controller' in respect of the data processing carried out by it since it is the operator that determines the purposes and means of that processing [...]

....

[26] As regards in particular the internet, the Court has already had occasion to state that the operation of loading personal data on an internet page must be considered to be such 'processing' within the meaning of Article 2(b) of Directive 95/46 (see Case C-101/01 *Lindqvist* EU:C:2003:596, paragraph 25).

[27] So far as concerns the activity at issue in the main proceedings, it is not contested that the data found, indexed and stored by search engines and made available to their users include information relating to identified or identifiable natural persons and thus 'personal data' within the meaning of Article 2(a) of that directive.

[28] Therefore, it must be found that, in exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results. As those operations are referred to expressly and unconditionally in Article 2(b) of Directive 95/46, they must be classified as 'processing' within the meaning of that provision, regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data [...]

[33] It is the search engine operator which determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of that activity and which must, consequently, be regarded as the 'controller' in respect of that processing pursuant to Article 2(d).

[34] Furthermore, it would be contrary not only to the clear wording of that provision but also to its objective — which is to ensure, through a broad definition of the concept of 'controller', effective and complete protection of data subjects — to exclude the operator of a search engine from that definition on the ground that it does not exercise control over the personal data published on the web pages of third parties. [...]

....

[41] It follows from all the foregoing considerations that the answer to Question 2(a) and (b) is that Article 2(b) and (d) of Directive 95/46 are to be interpreted as meaning that, first, the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified

as ‘processing of personal data’ within the meaning of Article 2(b) when that information contains personal data and, second, the operator of the search engine must be regarded as the ‘controller’ in respect of that processing, within the meaning of Article 2(d).

Brainstorming exercise

Your social media account does not have any privacy filters. You often publish pictures that show your student life. In these pictures you are sometimes alone, and other times together with others. According to the GDPR, you qualify as:

a. controller

b. processor

c. data subject

d. none of the above

12. GDPR - RIGHTS AND OBLIGATIONS

Outline of the chapter

This chapter introduces the main rights that data subjects have with regards to the processing of personal data and the obligations established under the General Data Protection Regulation for controllers and processors.

The main topics discussed are:

- Individual rights of data subjects (12.2)
- Obligations for the lawful processing of data (12.3)

(12.1) Revision: Legal bases

The following questions are based on the knowledge that you acquired in the previous chapter.

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://opentextbooks.rug.nl/dataprotectionanddigitalhumanrights/?p=48#h5p-18

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://opentextbooks.rug.nl/dataprotectionanddigitalhumanrights/?p=48#h5p-19



An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://opentextbooks.rug.nl/dataprotectionanddigitalhumanrights/?p=48#h5p-20



An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://opentextbooks.rug.nl/dataprotectionanddigitalhumanrights/?p=48#h5p-21



An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://opentextbooks.rug.nl/dataprotectionanddigitalhumanrights/?p=48#h5p-22

(12.2) Individual rights of data subjects

In the previous chapter we learned about the principles that must be followed when processing personal data. We learned about the lawful grund for processing personal data as well as about the roles of controllers and processors. In order to ensure that the data protection principles are not mere ideals but mandatory rules which must be adhered to, the European legislator has introduced a set of rights for data subjects and obligations for controller and processor. The aim of these rights and obligations is to ensure that data processing is done in compliance with the legal rules.

The rights of the data subject are regulated in chapter III GDPR.

(12.2.1) Right to be informed

A pre-condition for exercising any rights is to be informed about the processing of personal data. Hence, the GDPR starts with the data subject right to be informed. The exercise of this right is clearly linked with the principle of lawfulness, fairness and transparency introduced in article 5(1)(a) GDPR.

In the information society, data can be directly collected from the data subject, or they can be acquired differently. The most obvious example of the later is the collection of data available online. To ensure fair and

transparent processing, the GDPR differentiates between these two different ways with regards to when the data subject should be informed.

On the one hand, Article 13 GDPR lays down the rules applicable when the information about the data subject has been collected from the data subject.

Article 13 GDPR – Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject *are collected from the data subject*, the controller shall, *at the time when personal data are obtained*, provide the data subject with all of the following information:

a) the *identity* and the *contact details of the controller* and, where applicable, of the controller's representative;

b) the *contact details of the data protection officer*, where applicable;

c) the *purposes of the processing* for which the personal data are intended *as well as the legal basis for the processing*;

d) where the processing is based on point (f) of Article 6(1), *the legitimate interests pursued* by the controller or by a third party;

e) the recipients or categories of recipients of the personal data, if any;

f) where applicable, the fact that the controller intends to *transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission*, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), *reference to the appropriate or suitable safeguards* and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing [...]

On the other hand, Article 14 GDPR regulates the situation in which information about the data subject has not been obtained from the data subject. Thus, via alternative routes and channels.

Article 14 GDPR – Information to be provided where personal data have not been obtained from the data subject

1. Where personal data *have not been obtained from the data subject*, the controller shall provide the data subject with the following information:

a) the *identity* and the *contact details of the controller* and, where applicable, of the controller's representative;

b) the *contact details of the data protection officer*, where applicable;

c) the *purposes of the processing* for which the personal data are intended *as well as the legal basis* for the processing;

d) the *categories of personal data* concerned;

e) the *recipients or categories of recipients* of the personal data, if any;

f) where applicable, that the controller intends to *transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission*, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), *reference to the appropriate or suitable safeguards* and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

e) the right to lodge a complaint with a supervisory authority;

f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

Articles 13 and 14 aim to ensure that processing is fair and transparent; that the data subject is at all times well-informed on 1) what data about him that is being processed, 2) what the purpose of the processing is and 3) what consequences could follow. Additionally, should the data be acquired directly from the data subject, he or she must be informed at that moment of time about all the relevant consequences. When the data are not collected directly from the data subject, a reasonable period of time is provided for following the provision of the 3rd paragraph of article 14 GDPR.

This regulation is clarified in Recital 61 as well:

> "The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case.

As any right of not-absolute nature, the right to information has also a number of exceptions. Paragraph 4 of art 13 and paragraph 5 of article 14 list a number of exceptions.

Article 13(4) GDPR

Paragraphs 1, 2 and 3 shall not apply where and insofar as the **data subject already has the information**.

Article 14(5) GDPR

Paragraphs 1 to 4 shall not apply where and insofar as:

a) the data subject **already has the information**;

b) the provision of such information proves **impossible** or would involve a **disproportionate effort**, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

c) obtaining or disclosure is **expressly laid down by Union or Member State law** to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

d) where the personal data must remain confidential subject to an **obligation of professional secrecy** regulated by Union or Member State law, including a statutory obligation of secrecy.

(12.2.2) Right of access

The second data subject right is the one to access the data that are being processed. The exercise of this right, gives the data subject the possibility to evaluate the lawfulness of the processing operations on the personal

data. The exercise of this right is clearly linked with the principle of lawfulness, fairness and transparency introduced in article 5(1)(a) GDPR, but it is also linked to other principles as for example: purpose limitation, data minimisation, storage limitation and accountability . Article 15 of the GDPR regulates the right of access:

Article 15 GDPR – Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

a) the purposes of the processing;

b) the categories of personal data concerned;

c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

f) the right to lodge a complaint with a supervisory authority;

g) where the personal data are not collected from the data subject, any available information as to their source;

e) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless

otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

In accordance with the right, the data subject is meant to not only have access to the data concerning him that are being processed, but the access itself must be easy and at reasonable intervals. However, such access is not without limitations, as for example when rights and freedoms of other data subjects are concerned or in case of potential disclosure of trade secrets and other intellectual property considerations. However, even in these cases, the data controller cannot fully refuse to provide the data subject with access. Case by case considerations will be made and taken into account.

(12.2.3) Right to rectification

The right to rectification of inaccurate information is contained in Article 16 of the Regulation. This short provision gives the possibility to data subjects to ask that inaccurate personal data are rectified and completed. The exercise of this right is clearly linked with the principle of accuracy in article 5(1)(d) GDPR.

Article 16 GDPR – Right to rectification

The data subject shall have the *right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.* Taking into account the purposes of the processing, the data subject shall have the *right to have incomplete personal data completed*, including by means of providing a supplementary statement.

(12.2.4) Right to erasure ("right to be forgotten")

The right to erasure is not an entirely new asset of the GDPR. It was regulated also in the Data Protection Directive, Article 12(b) as well as discussed in landmarking decisions of the CJEU, like in *Google Spain*, with regards to de-referencing from search engines and in *Google v CNIL* with regards to the territorial scope of de-

referencing. In the GDPR, the right is clearly demarcated from other rights, with broader and more accurate application as provided in Article 17 of the Regulation.

Article 17 GDPR – Right to erasure

1. The data subject shall have the *right* to obtain from the controller the *erasure of personal data concerning him or eher without undue delay* and the *controller shall have the obligation* to erase personal data without undue delay *where one of the following grounds applies*:

a) the *personal data are no longer necessary* in relation to the *purposes* for which they were collected or otherwise processed;

b) the *data subject withdraws consent on which the processing is based* according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

c) the data subject *objects to the processing pursuant to Article 21(1)* and there are *no overriding legitimate grounds* for the processing, or the data subject *objects to the processing pursuant to Article 21(2)*;

d) the personal data have been *unlawfully processed*;

e) the personal data have to be erased for *compliance with a legal obligation in Union or Member State law* to which the controller is subject;

f) the personal data *have been collected in relation t*o the offer of information society services referred to in *Article 8(1)*.

2. Where the *controller has made the personal data public* and is obliged pursuant to paragraph 1 to erase the personal data, the controller, *taking account of available technology and the cost of implementation*, shall take *reasonable steps*, including technical measures, to *inform controllers which are processing the personal data* that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall *not* apply to the extent that *processing is necessary*:

a) for exercising the *right of freedom of expression and information*;

b) for *compliance with a legal obligation* which requires processing by Union or Member

State law to which the controller is subject *or* for the *performance of a task carried out in the public interest or in the exercise of official authority* vested in the controller;

c) for *reasons of public interest in the area of public health* in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

d) for *archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)* in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

e) for the *establishment, exercise or defence of legal claims.*

The right to erasure is not an absolute one. For your curiosity, you can check the Google transparency report and see their compliance rate as well as the types of requests for erasure that are received per country.

You can check the Google transparency report here.

The enforcement of the right to erasure has also a geographical limitation. This has been clarified by the CJEU in the *Google v. CNIL* case and it is strictly linked to the fact that the right to data protection is not yet recognised as a human right.

Case C-507/17 *Google v CNIL* EU:C:2019:772

Relevant facts

The President of the CNIL (French Data Protection Authority) sent a formal notice to Google that, when granting a request from a natural person for links to web pages to be removed from the list of results displayed following a search conducted on the basis of that person's name, it must apply that removal to all its search engine's domain name extensions. Google refused to comply with that

formal notice, confining itself to removing the links in question from only the results displayed following searches conducted from the domain names corresponding to the versions of its search engine in the Member States.

CNIL, after finding that Google had failed to comply with the formal notice within the prescribed period, imposed a penalty on that company.

Relevant question asked to the Court

Must the "right to de-referencing" be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, to deploy the de-referencing to all of the domain names used by its search engine so that the links at issue no longer appear, irrespective of the place from where the search initiated on the basis of the requester's name is conducted, and even if it is conducted from a place outside the territorial scope of Directive [95/46]?

Arguments of the Court

[46] In the context of Regulation 2016/679, that right of a data subject to de-referencing is now based on Article 17 of that regulation, which specifically governs the 'right to erasure', also referred to, in the heading of that article, as the 'right to be forgotten'.

[47] Pursuant to Article 17(1) of Regulation 2016/679, a data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller has the obligation to erase personal data without undue delay where one of the grounds listed in that provision applies. Article 17(3) of that regulation specifies that Article 17(1) does not apply to the extent that processing is necessary for one of the reasons listed in the former provision. Those reasons include, in particular, under Article 17(3)(a) of that regulation, the exercise of the right of, inter alia, freedom of information of internet users.

....

[55] It is true that a de-referencing carried out on all the versions of a search engine would meet that objective in full.

[56] The internet is a global network without borders and search engines render the information and links contained in a list of results displayed following a search conducted on the basis of an individual's name ubiquitous (see, to that effect, judgments of 13 May 2014, *Google Spain and Google*, C-131/12, EU:C:2014:317, paragraph 80, and of 17 October 2017, *Bolagsupplysningen and Ilsjan*, C-194/16, EU:C:2017:766, paragraph 48).

[57] In a globalised world, internet users' access — including those outside the Union — to the referencing of a link referring to information regarding a person whose centre of interests is

situated in the Union is thus likely to have immediate and substantial effects on that person within the Union itself.

[58] Such considerations are such as to justify the existence of a competence on the part of the EU legislature to lay down the obligation, for a search engine operator, to carry out, when granting a request for de-referencing made by such a person, a de-referencing on all the versions of its search engine.

[59] That being said, it should be emphasised that numerous third States do not recognise the right to de-referencing or have a different approach to that right.

[60] Moreover, the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality (see, to that effect, judgment of 9 November 2010, *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09, EU:C:2010:662, paragraph 48, and Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017, EU:C:2017:592, point 136). Furthermore, the balance between the right to privacy and the protection of personal data, on the one hand, and the freedom of information of internet users, on the other, is likely to vary significantly around the world.

[61] While the EU legislature has, in Article 17(3)(a) of Regulation 2016/679, struck a balance between that right and that freedom so far as the Union is concerned (see, to that effect, today's judgment, *GC and Others (De-referencing of sensitive data)*, C-136/17, paragraph 59), it must be found that, by contrast, it has not, to date, struck such a balance as regards the scope of a de-referencing outside the Union.

[62] In particular, it is in no way apparent from the wording of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 or Article 17 of Regulation 2016/679 that the EU legislature would, for the purposes of ensuring that the objective referred to in paragraph 54 above is met, have chosen to confer a scope on the rights enshrined in those provisions which would go beyond the territory of the Member States and that it would have intended to impose on an operator which, like Google, falls within the scope of that directive or that regulation a de-referencing obligation which also concerns the national versions of its search engine that do not correspond to the Member States.

[63] Moreover, although Regulation 2016/679 provides the supervisory authorities of the Member States, in Articles 56 and 60 to 66 thereof, with the instruments and mechanisms enabling them, where appropriate, to cooperate in order to come to a joint decision based on weighing a data subject's right to privacy and the protection of personal data concerning him or her against the interest of the public in various Member States in having access to information, it must be found

that EU law does not currently provide for such cooperation instruments and mechanisms as regards the scope of a de-referencing outside the Union.

[64] It follows that, currently, there is no obligation under EU law, for a search engine operator who grants a request for de-referencing made by a data subject, as the case may be, following an injunction from a supervisory or judicial authority of a Member State, to carry out such a de-referencing on all the versions of its search engine.

(12.2.5) Right to restriction of processing

Under Article 18 of the GDPR, data subjects have the right to request the restriction of processing of their personal data in certain situations. This means that while the data is still with the controller, the latter cannot process it unless specific exceptions apply. The rightt to restriction is often used as a temporary safeguard, particularly when the accuracy of the data is contested or the individual has objected to the processing.

Article 18 GDPR – Right to restriction of processing

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment,

exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Recital 67 sheds some light on the methods that controllers can use in order to comply in practice with the exercise of the right to restriction.

Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.

(12.2.6) Right to data portability

Article 20 of the Regulation contains the right to data portability, allowing individuals to receive their personal data in a structured, commonly used and machine-readable format. It also gives them the right to transmit the data, where technically feasible, to another controller (service provider). This right aims to empower data subjects to retain control over their data and to facilitate switching between service providers. While theoretically the right has its clear merits, in practice it is difficult to exercise it. The exercice of the right is especially difficult with regards to transferring the data to other service providers in the digital society due to potential conflicts with other legal frameworks, as for example IP protection, as well as with regards to personal data being ofter intertwined with data of others.

Article 20 GDPR – Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

(12.2.7) Right to object

Article 21 GDPR gives individuals the right to object to the processing of their personal data, especially when it's based on legitimate interests or public interest. If the data subject objects, the controller must stop processing unless they can show strong overriding reasons. In case of data processed for direct marketing purposes, the data subject right to object is absolute, as it is indicated in the 2nd and 3rd paragraph of the article.

Article 21 GDPR – Right to object

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller

shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.
3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.
5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.
6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

(12.2.8) Right in relation to automated decision-making, including profiling

Article 22 GDPR gives individuals the right *not* to be subject to automated decisions, including profiling, that produce legal effects or that similarly and significantly effect the data subject. The right not to be subject to automated decisions is especially relevant at a time when AI technology is quickly developing. Automated decisions are only allowed under strict conditions following paragraphs 2, 3 and 4 of the article, and have found support in the AI act as well (e.g. the human in the loop concept as well as the risk categorisation when processing special categories of data).

Article 22 GDPR – Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Summary questions



An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://opentextbooks.rug.nl/dataprotectionanddigitalhumanrights/?p=48#h5p-23

(12.3) Obligations for the lawful processing of data

Up until this point, the discussion has been focused on the rights vested upon the data subject by the GDPR. Those rights are explicitly provided for by the Regulation and reflect the principles of data protection, which

were discussed under article 5 GDPR. They also relate to, in various ways, the legal bases listed in Article 6 GDPR to ensure that any data processing is lawful and legitimate.

The next step is to dive into the corresponding obligations which are prescribed by the GDPR on the controllers (and processors) of data. Following the same logic, the obligations also reflect the general principles of data processing (Article 5 GDPR). While some of the obligations of controllers directly follow the exercise of the data subject rights, other obligations are to be found in special articles of the GDPR.

(12.3.1) Obligations linked to the principle of information security

The principle of information security is contained in Article 5(1)(f) GDPR:

> [...] *processed in a manner that ensures appropriate security of the personal data*, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures [...]

The corresponding obligations are listed under the following provisions of the Regulation:

Article 32 GDPR – Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) the pseudonymisation and encryption of personal data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

In case there is a data breach, further obligations are contained in Article 33-34 of the Regulation. Firstly, a notification to the Supervisory Authority (SA) must be sent without undue delay, at the latest within the 72 hours after becoming aware of the breach. Secondly, individuals affected must also be informed, however, this only applies if the data breach poses a very high risk.

(12.3.2) Obligations linked to the principle of accountability

The principle of accountability in article 5(2) GDPR, is central to the obligations of controllers and processors.

> The controller shall be *responsible* for, and *be able to demonstrate compliance with*, paragraph 1 [...]

The corresponding obligation on controllers in order to be able to show compliance is provided for in article 30 GDPR. It has to be noted that small and medium size companies, with up to 250 workers, are excluded by the obligation of keeping records, unless they engage in processing operations mentioned in the fifth paragraph of the article.

In May 2025, the Commission adopted a Single Market Simplification proposal that aims to cut the administrative cost that derive from the GDPR obligations for companies by introducing targeted changes to the rules on record-keeping for small and medium-sized companies and organisations under 750 employees. Such proposal is done in light of the data driven innovation aims of the Union that aims to be a competing

actor in the global market and does not affect those situations when processing of personal data can be considered "high risk" under the GDPR.

Article 30 GDPR – Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

b) the purposes of the processing;

c) a description of the categories of data subjects and of the categories of personal data;

d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

f) where possible, the envisaged time limits for erasure of the different categories of data;

g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

b) the categories of processing carried out on behalf of each controller;

c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of

transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

(12.3.3) Other important obligations

The GDPR provides for other important obligations that controllers and processors must follow for lawful processing of personal data.

- Data protection policies (Article 24(2) GDPR)
- Data protection by design and by default (Article 25 GDPR)
- Contracts with processors (Article 28 GDPR)
- Documentation of processing activities (Article 30 GDPR)
- Data Protection Impact Assessment (Article 35 GDPR)
- Prior consultation (Article 36 GDPR)
- Appointing a DPO (Articles 37-39 GDPR)

Question for self-reflection

- Have you ever exercised any of your data subject rights?
- In your opinion, is there a hierarchy between the principles of data processing? What about the data subject rights?
- Enter any internet website and read the cookie desclaimer. Is it GDPR compliant?
- What is the difference between the controllers obligations regarding 'data protection by design' and 'data protection by default'?

13. GDPR - THE ENFORCEMENT MECHANISM

Outline of the chapter

The aim of this Chapter is to introduce the enforcement mechanism provided for in the GDPR. For the effective exercise of rights as well as compliance with any obligation, the Regulation provides for both public and private enforcement. The first is related with the system of administrative fines. The second with enabling data subjects to claim before courts the violation of their rights. Understanding the role and tasks of Supervisory Authorities becomes very important in this framework.

The topics covered are:

- Supervisory Authorities (13.1)
- Lead Supervisory Authorities (13.2)
- Liability, compliants and remedies (13.3)

(13.1) Supervisory Authorities

Following the GDPR provisions, each Member State has created one or more Supervisory Authorities to supervise upon the enforcement of the Regulation in full autonomy. The Authorities play a major role for the protection of the rights of data subjects. Article 51 GDPR provides the following:

Article 51 GDPR – Supervisory Authority

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').
2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.
3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.

The independence of Supervisory Authorities is a very important characteristic of their functioning. As article 52 GDPR provides for, this independence can be seen both financially as well as with regards to the administrative organisation and position that the Supervisory Authorities have in the internal organisation of the states. The members of the Supervisory Authorities are to remain *independent* in the performance of their tasks and should neither receive nor request any outside influence or instruction nor should they engage in any other conflicting activities.

Article 52 GDPR – Independence

1. Each supervisory authority shall act with **complete independence** in performing its tasks and exercising its powers in accordance with this Regulation.
2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, **remain free from external influence**, whether direct or indirect, and shall neither seek nor take instructions from anybody.
3. Member or members of each supervisory authority shall **refrain from any action incompatible with their duties** and shall not, during their term of office, **engage in any incompatible occupation**, whether gainful or not.

4. Each Member State shall ensure that **each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers**, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.
5. Each Member State shall ensure that **each supervisory authority chooses and has its own staff** which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.
6. Each Member State shall ensure that **each supervisory authority is subject to financial control which does not affect its independence** and that it has separate, public annual budgets, which may be part of the overall state or national budget.

The Court of Justice of the EU has been going further in reinforcing the independence of the Supervisory Authorities. In the case C-362/14, *Schrems I* , The Court argued for the independence of Supervisory Authorities from the influence of the Europen Commission, while in case C-518/07, *Commission v. Germany*, they argued about independence from national public authorities.

Case C-362/14 *Schrems I* EU:C:2015:650

[41] The guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the monitoring of compliance with the provisions concerning protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. It was established in order to strengthen the protection of individuals and bodies affected by the decisions of those authorities. The establishment in Member States of independent supervisory authorities is therefore, as stated in recital 62 in the preamble to Directive 95/46, an essential component of the protection of individuals with regard to the processing of personal data (see judgments in Commission v Germany, C-518/07, EU:C:2010:125, paragraph 25, and Commission v Hungary, C-288/12, EU:C:2014:237, paragraph 48 and the case-law cited).

....

[51] The Commission may adopt, on the basis of Article 25(6) of Directive 95/46, a decision finding that a third country ensures an adequate level of protection. In accordance with the second

subparagraph of that provision, such a decision is addressed to the Member States, who must take the measures necessary to comply with it. Pursuant to the fourth paragraph of Article 288 TFEU, it is binding on all the Member States to which it is addressed and is therefore binding on all their organs (see, to this effect, judgments in Albako Margarinefabrik, 249/85, EU:C:1987:245, paragraph 17, and Mediaset, C-69/13, EU:C:2014:71, paragraph 23) in so far as it has the effect of authorising transfers of personal data from the Member States to the third country covered by it.

[52] Thus, until such time as the Commission decision is declared invalid by the Court, the Member States and their organs, which include their independent supervisory authorities, admittedly cannot adopt measures contrary to that decision, such as acts intended to determine with binding effect that the third country covered by it does not ensure an adequate level of protection. Measures of the EU institutions are in principle presumed to be lawful and accordingly produce legal effects until such time as they are withdrawn, annulled in an action for annulment or declared invalid following a reference for a preliminary ruling or a plea of illegality (judgment in Commission v Greece, C-475/01, EU:C:2004:585, paragraph 18 and the case-law cited).

[53] However, a Commission decision adopted pursuant to Article 25(6) of Directive 95/46, such as Decision 2000/520, cannot prevent persons whose personal data has been or could be transferred to a third country from lodging with the national supervisory authorities a claim, within the meaning of Article 28(4) of that directive, concerning the protection of their rights and freedoms in regard to the processing of that data. Likewise, as the Advocate General has observed in particular in points 61, 93 and 116 of his Opinion, a decision of that nature cannot eliminate or reduce the powers expressly accorded to the national supervisory authorities by Article 8(3) of the Charter and Article 28 of the directive.

...

[57] On the contrary, Article 28 of Directive 95/46 applies, by its very nature, to any processing of personal data. Thus, even if the Commission has adopted a decision pursuant to Article 25(6) of that directive, the national supervisory authorities, when hearing a claim lodged by a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him, must be able to examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the directive.

Case C-518/07 *Commission v Germany* EU:C:2010:125

[18] With regard, in the first place, to the wording of the second subparagraph of Article 28(1) of Directive 95/46, because the words 'with complete independence' are not defined by that directive, it is necessary to take their usual meaning into account. In relation to a public body, the term 'independence' normally means a status which ensures that the body concerned can act completely freely, without taking any instructions or being put under any pressure.

[19] Contrary to the position taken by the Federal Republic of Germany, there is nothing to indicate that the requirement of independence concerns exclusively the relationship between the supervisory authorities and the bodies subject to that supervision. On the contrary, the concept of 'independence' is complemented by the adjective 'complete', which implies a decision-making power independent of any direct or indirect external influence on the supervisory authority.

....

[25] The guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the supervision of compliance with the provisions on protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. It was established not to grant a special status to those authorities themselves as well as their agents, but in order to strengthen the protection of individuals and bodies affected by their decisions. It follows that, when carrying out their duties, the supervisory authorities must act objectively and impartially. For that purpose, they must remain free from any external influence, including the direct or indirect influence of the State or the *Länder*, and not of the influence only of the supervised bodies.

....

[30] In the light of the foregoing, the second subparagraph of Article 28(1) of Directive 95/46 is to be interpreted as meaning that the supervisory authorities responsible for supervising the processing of personal data outside the public sector must enjoy an independence allowing them to perform their duties free from external influence. That independence precludes not only any influence exercised by the supervised bodies, but also any directions or any other external influence, whether direct or indirect, which could call into question the performance by those authorities of their task consisting of establishing a fair balance between the protection of the right to private life and the free movement of personal data.

Supervisory Authorities have a large amount of tasks that extend from monitoring compliance with the data protection rules to giving advise to controllers and promoting the values imbeded in the regulation. The tasks are listed under the first paragraph of article 57 GDPR.

Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

a) monitor and enforce the application of this Regulation;

b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

d) promote the awareness of controllers and processors of their obligations under this Regulation;

e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;

h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

j) adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);

k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);

l) give advice on the processing operations referred to in Article 36(2);

m) encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);

n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);

o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);

p) draft and publish the requirements for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

r) authorise contractual clauses and provisions referred to in Article 46(3);

s) approve binding corporate rules pursuant to Article 47;

t) contribute to the activities of the Board;

u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and

v) fulfil any other tasks related to the protection of personal data.

For the performance of these tasks, Article 58 GDPR, in the first three paragraphs, lists the main powers of supervisory authorities. The powers can be grouped into three main groups : i. investigative; ii. corrective; and iii. advisory powers. As regulated under the 4th paragraph of the article, the exercise of the powers conferred on the supervisory authority is subject to appropriate safeguards, including effective judicial remedy and due process.

Article 58 GDPR – Powers

1. Each supervisory authority shall have all of the following **investigative powers**:

a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;

b) to carry out investigations in the form of data protection audits;

c) to carry out a review on certifications issued pursuant to Article 42(7);

d) to notify the controller or the processor of an alleged infringement of this Regulation;

e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;

f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

2. Each supervisory authority shall have all of the following **corrective powers**:

a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

e) to order the controller to communicate a personal data breach to the data subject;

f) to impose a temporary or definitive limitation including a ban on processing;

g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

3. Each supervisory authority shall have all of the following **authorisation and advisory powers**:

a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;

b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;

c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;

d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);

e) to accredit certification bodies pursuant to Article 43

f) to issue certifications and approve criteria of certification in accordance with Article 42(5);

g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);

h) to authorise contractual clauses referred to in point (a) of Article 46(3);

i) to authorise administrative arrangements referred to in point (b) of Article 46(3);

j) to approve binding corporate rules pursuant to Article 47.

The material and territorial jurisdiction of Supervisory Authorities is prescribed by Article 55 GDPR. The territorial jurisdiction is, in principle, limited to the territory of each Member State. There are exceptions to this rule. The first exception can be found in the second paragraph of the article. It refers to those situations when personal data are processed on the bases of legal obligations prescribed by national law (art 6(1)(c) GDPR) and the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (art 6(1)(e) GDPR). Other exceptions are linked to the cross-border nature of data processing and will be discussed below. The material jurisdiction is limited with regards to data processing by national courts acting in their judicial capacity.

Article 55 GDPR – Competence

1. Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

2. Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.
3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.

The territorial competence of Supervisory Authorities is also defined in article 4(22) GDPR. This competence can be linked with: i. the territorial establishment of a controller or processor; ii. with the residence of the data subject; or iii. with the place of lodging a complaint.

'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because:

a) the controller or processor is established on the territory of the Member State of that supervisory authority;

b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

c) a complaint has been lodged with that supervisory authority;

How to file a complaint?

Step-by-step information is provided in the webpage of the concerned Supervisory Authority.

Here you can find the information provided by the Dutch Supervisory Authority.

(13.2) Lead Supervisory Authorities

In the EU's internal market and especially in a digital society, it is clear that processing of data can easily cross the borders. This can be linked to the location of controllers and processors which might also have more

than one establishment, or simply to offering of goods and services to data subjects within the territory of the European Union, without any territorial restrictions. The definitions of article 4 GDPR contain also an explanation of 'cross-border processing' of personal data:

'cross-border processing' means either:

a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

The legitimate doubt in such cross-border situations is linked with the territorial jurisdiction of Supervisory Authorities. If each Supervisory Authority is concerned by processing activities linked to their territory, does this mean that more than one Authorities have jurisdiction in cross-border situations?

The GDPR has addressed these concerns by introducing the concept of Lead Supervisory Authorities in Article 56.

Article 56 GDPR – Competence of the lead supervisory authority

1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.
2. By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.
3. In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. Within a period of three weeks

after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.

4. Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).
5. Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61 and 62.
6. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.

Thus, Lead Supervisory Authority, is a single national Authority that is concerned by the data processing activity and has the competence to deal with the specific cross-border case due to the presence of certain conditions. The other concerned national Supervisory authorities, can assist and collaborate but do not have the competence to decide on such situations.

Article 60 GDPR – Cooperation between the lead supervisory authority and the other supervisory authorities concerned

1. The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.
2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for

monitoring the implementation of a measure concerning a controller or processor established in another Member State.

3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.
4. Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.
5. Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.
6. Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.
7. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.
8. By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.
9. Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the

supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof.

10. After being notified of the decision of the lead supervisory authority pursuant to paragraphs 7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other supervisory authorities concerned.
11. Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 66 shall apply.
12. The lead supervisory authority and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardised format.

In order to ensure the collaboration and consistent application of the GDPR among various Supervisory Authorities, the consistency mechanism is created. This mechanism is especially important where a supervisory authority intends to adopt a measure intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States.

Article 63 GDPR – Consistency mechanism

In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.

In a case with EU-wide impact, when there is a dispute between the Lead Supervisory Authority and the concerned national Supervisory authorities, or when requested by the Chair of the European Data Protection Board or the European Commission, the European Data Protection Board can issue a non-binding decision

(art 64 GDPR). If the national Supervisory Authority does not follow this decision, the Board can issue a binding decision addressed to the Lead Supervisory Authority and all the other national Supervisory Authorities concerned.

Article 65 GDPR – Dispute resolution by the Board

1. In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:

a) where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead supervisory authority and the lead supervisory authority has not followed the objection or has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation;

b) where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment;

c) where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board.

...

The European Data Protection Board has made use of article 65 GDPR and issued binding decisions in a number of cross-border situations. You can find these decisions here and will not be surprised to see that most of them deal with controllers that offer information communication services, as for example: Meta, TikTok, (previously) Twitter, etc.

For better understanding the role of the European Data Protection Board (formerly known as Article 29 Working Party) within the GDPR and distinguishing this role from the European Data Protection Supervisor that is responsible for the processing of data by Union institutions, please read the two Articles below.

Article 68 GDPR – European Data Protection Board

1. The European Data Protection Board (the 'Board') is hereby established as a body of the Union and shall have legal personality.
2. The Board shall be represented by its Chair.
3. The Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.
4. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, a joint representative shall be appointed in accordance with that Member State's law.
5. The Commission shall have the right to participate in the activities and meetings of the Board without voting right. The Commission shall designate a representative. The Chair of the Board shall communicate to the Commission the activities of the Board.
6. In the cases referred to in Article 65, the European Data Protection Supervisor shall have voting rights only on decisions which concern principles and rules applicable to the Union institutions, bodies, offices and agencies which correspond in substance to those of this Regulation

Article 52 Regulation (EU) 2018/1725 (of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC) – **European Data Protection Supervisor**

1. The European Data Protection Supervisor is hereby established.

2. With respect to the processing of personal data, the European Data Protection Supervisor shall

be responsible for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by Union institutions and bodies.

3. The European Data Protection Supervisor shall be responsible for monitoring and ensuring the application of the provisions of this Regulation and of any other Union act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a Union institution or body, and for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data. To those ends, the European Data Protection Supervisor shall fulfil the tasks set out in Article 57 and exercise the powers granted in Article 58.

....

(13.3) Liability, complaints and remedies

As it was stated at the start of this chapter, the GDPR provides both for public and for private enforcement.

(13.3.1) Public enforcement

The public enforcement consists in the complaints lodged before Supervisory Authorities. As already seen under article 58 GDPR, such Authorities have both investigative and corrective powers. They can start their investigations ex officio, or on the bases of complaints from data subjects.

Article 77 GDPR – Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

If the Supervisory Authority finds a breach of the GDPR, they have the power to impose administrative fines. These fines must be effective, proportionate, and dissuasive. The level of the fine depends on several factors, including the nature, gravity and duration of the infringement; whether the violation was committed intentionally or through negligence; the degree of cooperation shown by the organization; and any efforts made to limit harm to the affected individuals.

Please note that not any proved infringement is punished with a fine. The corrective powers of the Supervisory Authorities, as already discussed under Article 58(2) include also advise, reprimands, orders, etc.

The general conditions for imposing a fine are regulated under article 83 GDPR. The article establishes the upper threshold of the fines, leaving it to the Authorities to establish the exact amount in a specific situation. Under paragraph 4, the article lists those infringements that are punished with a low fine (up to 10 million Euros or 2% of the total worldwide annual turnover of the preceding financial year). Under paragraph 5, the article lists those infringements that are punished with a high fine (up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year).

Article 83 GDPR – General conditions for imposing administrative fines

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

a) the nature, gravity and duration of the infringement taking into account the nature scope or

purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

b) the intentional or negligent character of the infringement;

c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

e) any relevant previous infringements by the controller or processor;

f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

g) the categories of personal data affected by the infringement;

h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

b) the obligations of the certification body pursuant to Articles 42 and 43;

c) the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

b) the data subjects' rights pursuant to Articles 12 to 22;

c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

d) any obligations pursuant to Member State law adopted under Chapter IX;

e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

6. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

7. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

8. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

(13.3.2) Private enforcement

If an administrative fine is issued agains a controller or processor, the data subject does not receive any direct compensation. However, apart the public enforcement, data subjects have the possibility to bring an infringement case before a national court independently or simultaneously with the procedure before the

national Supervisory Authority. The case may be brought either in the courts of the Member State where the controller or processor is established or in the courts of the Member State where the individual resides.

Article 79 GDPR – Right to an effective judicial remedy against a controller or processor

1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.
2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

Any data subject that was suffering material or imaterial harm due to an infringement of the GDPR can seek compensation before a Court. The burden of prove in such cases is on the data subject and this makes the cases difficult to succeed given the information asymetry between data subjects and controllers and processors. Furthermore, as already seen under the Chapter about the GDPR obligations, most of these are imposed on controllers. Thus, processors have only residual liability in those situations when the infringement can be directly contributed to their actions that go beyond the instuctions received by controllers. When it is not possible to distinguish between the responsibility of controllers or processors or when more controllers and processors are involved, the rules on joint liability established under the 4th paragraph of aticle 82 GDPR apply. This legal regulation ensures that affected data subjects can receive full compensation, even if it is later necessary for the liable parties to settle the final distribution of responsibility among themselves.

Article 82 GDPR – Right to compensation and liability

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.
2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.
3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.
4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.
5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.
6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).

Compensation may be sought for both material damages, such as financial losses, and non-material damages, including emotional distress, reputational harm, or the feeling of loss of control over personal data. Also in favor of the data subject it is established that the claim can be brought before the national courts of the country where the controller or processor is established or alternatively, in the country where the individual normally resides. This flexibility ensures that data subjects do not have to pursue costly or difficult international litigation to enforce their rights.

The issue of compensation for damages, has been discussed by the CJEU in various instances. The establishment of infringement does not in itself give right to compensation. Thus, the burden of proof on the harm suffered stays with the data subject. It is good to know though that the degree of seriousness of the harm is not considered for compensation. A damage should be compensated independent from its amount.

Case C-300/21 *UI v Österreichische Post AG* EU:C:2023:370

[41] Similarly, Articles 83 and 84 of the GDPR, which permit the imposition of administrative fines and other penalties, have essentially a punitive purpose and are not conditional on the existence of individual damage. The relationship between the rules set out in Article 82 and those set out in Articles 83 and 84 shows that there is a difference between those two categories of provisions, but also complementarity, in terms of encouraging compliance with the GDPR, it being observed that the right of any person to seek compensation for damage reinforces the operational nature of the protection rules laid down by that regulation and is likely to discourage the reoccurrence of unlawful conduct.

[42] Last, it is important to note that the fourth sentence of recital 146 of the GDPR states that the rules laid down by the GDPR apply without prejudice to any claims for damages deriving from the violation of other rules of EU or Member State law.

[43] In the light of all of the foregoing reasons, the answer to Question 1 is that Article 82(1) of the GDPR must be interpreted as meaning that the mere infringement of the provisions of that regulation is not sufficient to confer a right to compensation

....

[45] In the first place, the GDPR does not define the concept of 'damage' for the purposes of the application of this instrument. Article 82 of that regulation confines itself to expressly stating that not only 'material damage' but also 'non-material damage' may give rise to a right to compensation, without any reference being made to any threshold of seriousness.

[46] In the second place, the context of that provision also tends to indicate that the right to compensation is not subject to the condition that the damage in question has reached a certain threshold of seriousness. The third sentence of recital 146 of the GDPR states that 'the concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation'. It would be contrary to that broad conception of 'damage', favoured by the EU legislature, if that concept were limited solely to damage of a certain degree of seriousness.

....

[49] Making compensation for non-material damage subject to a certain threshold of seriousness would risk undermining the coherence of the rules established by the GDPR,

since the graduation of such a threshold, on which the possibility or otherwise of obtaining that compensation would depend, would be liable to fluctuate according to the assessment of the courts seised.

....

[59] In the light of all of the foregoing considerations, the answer to Question 2 is that Article 82 of the GDPR must be interpreted as meaning that, for the purposes of determining the amount of damages payable under the right to compensation enshrined in that article, national courts must apply the domestic rules of each Member State relating to the extent of financial compensation, provided that the principles of equivalence and effectiveness of EU law are complied with.

Also in support of data subjects, Article 80 GDPR gives them the right to mandate a non-profit organization or association to act on their behalf in lodging complaints or pursuing legal remedies. This allows for collective representation and support, particularly in complex or large-scale cases involving systemic data protection violations.

NOYB, a non-governmental organisation based in Vienna and founded by Maximilian Schrems, is very active in this field. They have initiated many cases that we study today and that have been fined by Supervisory Authorities. Following the Collective Redress Directive (EU) 2020/1828, they have obtained the right to start class actions in Austria and Ireland for the protection of consumers.

Article 80 – Representation of data subjects

1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

Brainstorming exercise

Read the following statement and give your own opinion about the merits and de-merits of it:

"Despite the fact that the GDPR allows public and private enforcement to be initiated independently, private enforcement must follow public enforcement."

14. GDPR - DATA TRANSFERS TO THIRD COUNTRIES

Outline of the chapter

The focus of this chapter is to introduce the rules and measures envisaged by the GDPR for safe and secure transfer of data outside the Union. In the global digital economy such international transfers of personal data are common. The Regulation aims to ensure that the level of protection of data subjects in the EU is not undermined when their data are transferred to third countries. Otherwise, the whole data protection system is jeopardised.

The topics discussed are:

- International data transfers (14.1)
- Adequacy decisions (14.2)
- Other appropriate safeguards for transferring data to third countries (14.3)
- Derrogations for specific situations (14.4)

(14.1) International data transfers

Contemporary digital ecomomy would be unthinkable without international data flow. For instance, students at the University of Groningen have access to multiple digital libraries – some of which belong and are managed outside the European Union. To get access to those resources, students at the University provide their personal student emails, their student numbers and their educational institution. This information easily fits the definition of personal data under article 4(1) GDPR. The examples of data transfers to third countries are, in fact numerous – purchases from Amazon, streaming on Netflix, using Google applications, etc.

The rapid development of the global digital market is acknowledged by the GDPR in its Recital 101:

Flows of personal data to and from countries outside the Union and international organisations are *necessary for the expansion of international trade and international cooperation*. The increase in such flows has raised *new challenges and concerns* with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, *the level of protection of natural persons ensured in the Union by this Regulation should not be undermined*, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, *transfers to third countries and international organisations may only be carried out in full compliance with this Regulation*. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.

Brainstorming

A Spanish student that is currently enrolled at the University of Groningen, wants to switch from an EU-based health and fitness app to a US-based one. The student downloads his workout data and uploads it to the new app. No formal agreement exists between the two companies and the student initiated the transfer himself.

- *Does this kind of activity fall under the material scope of application of the GDPR?*

Let us suppose that the activity falls under the scope of application of the GDPR.

- *In your opinion, would such activity qualify as international data transfer?*
- *Who would qualify as data subject, controller and processor in this case?*

Transfers of personal data are often necessary, but lack of effective safeguards would expose data subjects to multiple and potentially grave risks.

For these reasons, the GDPR has constructed tools and mechanisms to ensure that its objectives will not

be compromised and the rights of data subjects will be safeguarded when their data leave the territory of the European Union.

Article 44 GDPR – General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

(14.2) Adequacy decisions

The mechanism of adequacy decisions is described in article 45 GDPR. According to it, an international transfer of data can take place if the Commission has declared that the third state/region/organization ensures an *adequate* level of protection. The data are transfered to countries that have an adequacy decision in the same way as if they were transferred within the territory of the European Union.

The adoption procedure of the adequacy decision includes the following steps:

- a *proposal* from the European Commission;
- an *opinion* of the European Data Protection Board;
- an *approval* from representatives of EU countries;
- the *adoption* of the decision by the European Commission.

Article 45 GDPR – Transfers on the basis of an adequacy decision

> 1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.[...]

The effect of an adopted adequacy decision is that data controllers can freely transfer data to the third country without any further safeguard checks being necessary.

The European Commission has so far recognized adopted adequacy decisions only with a limited number of countries and territories. You can find the list here.

As clearly stated in the 2nd paragraph of article 45 GDPR, there are 3 main criterias that the Commission asseses in order to decide if a 3rd country offers or not an adequate level of data protection: i. the respect for the rule of law, human rights and fundamental freedoms; ii. the existence and effective functioning of one or more independent supervisory authorities; iii. the international commitments the third country or international organisation concerned has entered into.

> 2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:
>
> a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
>
> b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
>
> c) the international commitments the third country or international organisation concerned has

entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data. [...]

The core element of an adequacy decision is the assessment that the third country offers an *adequate level of protection* of personal data. The CJEU has clarified the meaning of the phrase by considering that adequate does not mean 'identical level of protection' but it means 'essentially equivalent'.

Case C-362/14 *Schrems I* EU:C:2015:650

[74] It is clear from the express wording of Article 25(6) of Directive 95/46 that it is the legal order of the third country covered by the Commission decision that must ensure an adequate level of protection. Even though the means to which that third country has recourse, in this connection, for the purpose of ensuring such a level of protection may differ from those employed within the European Union in order to ensure that the requirements stemming from Directive 95/46 read in the light of the Charter are complied with, those means must nevertheless prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union.

[75] Accordingly, when examining the level of protection afforded by a third country, the Commission is obliged to assess the content of the applicable rules in that country resulting from its domestic law or international commitments and the practice designed to ensure compliance with those rules, since it must, under Article 25(2) of Directive 95/46, take account of all the circumstances surrounding a transfer of personal data to a third country.

[76] Also, in the light of the fact that the level of protection ensured by a third country is liable to change, it is incumbent upon the Commission, after it has adopted a decision pursuant to Article 25(6) of Directive 95/46, to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified. Such a check is required, in any event, when evidence gives rise to a doubt in that regard.

The history of the agreements between the EU and the USA with regards do data transfers is of particular interest. Not only because the EU and us as individual rely a lot on services provided by US companies (think of

Meta, X, Amazon, etc.), but also because of the different standard on the protection of personal data between the two jurisdictions. There has not been an adequacy decision *stricto sensu* between the EU and the USA for the transferral of personal data. The decisions of 2000 "Safe harbour " and 2016 'Privacy shield' have relied on declarations of self compliance of commercial companies in the US with the EU legal framework without finding that the US legal framework provided adequate protection for EU data subjects. Both these decisions were invalidated by the Court of Justice of the EU in the Schrems I and Schrems II decisions.

Case C-362/14 *Schrems I* EU:C:2015:650

[92] Furthermore and above all, protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary (judgment in Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraph 52 and the case-law cited).

[93] Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail (see, to this effect, concerning Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54), judgment in Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 57 to 61).

[94] In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter (see, to this effect, judgment in Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraph 39).

[95] Likewise, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as

enshrined in Article 47 of the Charter. The first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law (see, to this effect, judgments in Les Verts v Parliament, 294/83, EU:C:1986:166, paragraph 23; Johnston, 222/84, EU:C:1986:206, paragraphs 18 and 19; Heylens and Others, 222/86, EU:C:1987:442, paragraph 14; and UGT-Rioja and Others, C-428/06 to C-434/06, EU:C:2008:488, paragraph 80).

[96] As has been found in particular in paragraphs 71, 73 and 74 of the present judgment, in order for the Commission to adopt a decision pursuant to Article 25(6) of Directive 95/46, it must find, duly stating reasons, that the third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order, a level that is apparent in particular from the preceding paragraphs of the present judgment.

[97] However, the Commission did not state, in Decision 2000/520, that the United States in fact 'ensures' an adequate level of protection by reason of its domestic law or its international commitments.

[98] Consequently, without there being any need to examine the content of the safe harbour principles, it is to be concluded that Article 1 of Decision 2000/520 fails to comply with the requirements laid down in Article 25(6) of Directive 95/46, read in the light of the Charter, and that it is accordingly invalid.

Case C-311/18 *Schrems II* EU:C:2020:559

[178] In the present case, the Commission's finding in the Privacy Shield Decision that the United States ensures an adequate level of protection for personal data essentially equivalent to that guaranteed in the European Union by the GDPR, read in the light of Articles 7 and 8 of the Charter, has been called into question, inter alia, on the ground that the interference arising from the surveillance programmes based on Section 702 of the FISA and on E.O. 12333 are not covered by requirements ensuring, subject to the principle of proportionality, a level of protection essentially

equivalent to that guaranteed by the second sentence of Article 52(1) of the Charter. It is therefore necessary to examine whether the implementation of those surveillance programmes is subject to such requirements, and it is not necessary to ascertain beforehand whether that third country has complied with conditions essentially equivalent to those laid down in the first sentence of Article 52(1) of the Charter.

[179] In that regard, as regards the surveillance programmes based on Section 702 of the FISA, the Commission found, in recital 109 of the Privacy Shield Decision, that, according to that article, 'the FISC does not authorise individual surveillance measures; rather, it authorises surveillance programs (like PRISM, UPSTREAM) on the basis of annual certifications prepared by the Attorney General and the Director of National Intelligence (DNI)'. As is clear from that recital, the supervisory role of the FISC is thus designed to verify whether those surveillance programmes relate to the objective of acquiring foreign intelligence information, but it does not cover the issue of whether 'individuals are properly targeted to acquire foreign intelligence information'.

[180] It is thus apparent that Section 702 of the FISA does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes. In those circumstances and as the Advocate General stated, in essence, in points 291, 292 and 297 of his Opinion, that article cannot ensure a level of protection essentially equivalent to that guaranteed by the Charter, as interpreted by the case-law set out in paragraphs 175 and 176 above, according to which a legal basis which permits interference with fundamental rights must, in order to satisfy the requirements of the principle of proportionality, itself define the scope of the limitation on the exercise of the right concerned and lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards.

[181] According to the findings in the Privacy Shield Decision, the implementation of the surveillance programmes based on Section 702 of the FISA is, indeed, subject to the requirements of PPD-28. However, although the Commission stated, in recitals 69 and 77 of the Privacy Shield Decision, that such requirements are binding on the US intelligence authorities, the US Government has accepted, in reply to a question put by the Court, that PPD-28 does not grant data subjects actionable rights before the courts against the US authorities. Therefore, the Privacy Shield Decision cannot ensure a level of protection essentially equivalent to that arising from the Charter, contrary to the requirement in Article 45(2)(a) of the GDPR that a finding of equivalence depends, inter alia, on whether data subjects whose personal data are being transferred to the third country in question have effective and enforceable rights.

....

[185] In those circumstances, the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to the United States, which the Commission assessed in the Privacy Shield Decision, are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required, under EU law, by the second sentence of Article 52(1) of the Charter.

....

[192] Furthermore, as regards both the surveillance programmes based on Section 702 of the FISA and those based on E.O. 12333, it has been noted in paragraphs 181 and 182 above that neither PPD-28 nor E.O. 12333 grants data subjects rights actionable in the courts against the US authorities, from which it follows that data subjects have no right to an effective remedy.

....

[197] Therefore, the ombudsperson mechanism to which the Privacy Shield Decision refers does not provide any cause of action before a body which offers the persons whose data is transferred to the United States guarantees essentially equivalent to those required by Article 47 of the Charter.

[198] Therefore, in finding, in Article 1(1) of the Privacy Shield Decision, that the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in that third country under the EU-US Privacy Shield, the Commission disregarded the requirements of Article 45(1) of the GDPR, read in the light of Articles 7, 8 and 47 of the Charter.

[199] It follows that Article 1 of the Privacy Shield Decision is incompatible with Article 45(1) of the GDPR, read in the light of Articles 7, 8 and 47 of the Charter, and is therefore invalid.

A new data transfer agreement, this time known as the '[EU-US data privacy framework]' was adopted in 2023. This time the Commission has adopted the decision in the form of an adequacy decision. The main points of this decision include:

- the possibility for US companies to voluntarily join the EU-US Data Privacy Framework
- the possibility for EU data subjects to benefit from several redress avenues (including free of charge complaints before independent dispute resolution mechanisms and an arbitration panel)
- limited access to personal data by US intelligence agencies only when considered as necessary and proportionate to protect national security
- the possibility for EU data subjects to obtain redress regarding the collection and use of their data by US intelligence agencies before an independent and impartial redress mechanism, which includes a newly created Data Protection Review Court. This Court will independently investigate and

resolve complaints and adopt binding remedial measures.

(14.3) Other appropriate safegards for transferring data to third countries

In the absence of an adequacy decision, Article 46 GDPR provides for transferral of data to 3rd countries when appropriate safeguards are in place. These appropriate safeguards, following the second paragraph of the article are:

> The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:
>
> a) a legally binding and enforceable instrument between public authorities or bodies;
>
> b) binding corporate rules in accordance with Article 47;
>
> c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
>
> d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
>
> e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
>
> f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

The aim of the appropriate safeguards is to ensure protection of data subjects' rights in those situations when the legal framework of the 3rd country is not considered in itself as adequate. In *Schrems II,* the Court of Justice of the EU argued that controllers, after using one of the adequate safeguards listed in the law, still remain responsible for assessing that these allow for an appropriate protection of data subjects in the legal framework of the 3rd country.

Case C-311/18 *Schrems II* EU:C:2020:559

[105] Therefore, the answer to the second, third and sixth questions is that Article 46(1) and Article 46(2)(c) of the GDPR must be interpreted as meaning that the appropriate safeguards, enforceable rights and effective legal remedies required by those provisions must ensure that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union by that regulation, read in the light of the Charter. To that end, the assessment of the level of protection afforded in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country, in particular those set out, in a non-exhaustive manner, in Article 45(2) of that regulation.

(14.4) Derogations for specific situations

In the absence of an adequacy decision and appropriate safeguards, data can be exceptionally transferred to 3rd countries following the special derrogations contained in Article 49 GDPR. This rule is the last option for third states/regions/organizations where neither Article 45 GDPR nor Article 46 GDPR are applicable. As such, a data transfer based on derrogations may take place only if it is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.

The list of derrogations for specific situation can be found in the first paragraph of article 49 GDPR.

Article 49 GDPR – Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

d) the transfer is necessary for important reasons of public interest;

e) the transfer is necessary for the establishment, exercise or defence of legal claims;

f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://opentextbooks.rug.nl/dataprotectionanddigitalhumanrights/?p=50#h5p-25

-

15. PERSONAL DATA AND LAW ENFORCEMENT ACTIVITIES

Outline of the chapter

This chapter will focus on the use of personal data in law enforcement activities. It will discuss the case of data retention within the EU as well as the consequences of the invalidation of the Data Retention Directive. Furthermore, it will introduce another EU legal instrument for the harmonization of law enforcement activities related to data processing and exchange of personal data, namely the Law Enforcement Directive (LED).

The topics discussed are:

- Changes in law enforcement procedures (15.1)
- The Law Enforcement Directive (15.2)
- Data retention for law enforcement purposes (15.3)
- Predictive policing and the AI act (15.4)

(15.1) Changes in law enforcement procedures

With the rapid advancement of technologies, the tools that law enforcement authorities have at disposition for investigation and especially for surveillance have changed significantly. Physical surveillance has transformed into dataveillance. The amount of data that we continuously create and leave behind, as for example location data, communication data, etc., makes any physical surveillance superfluous. We carry with us state of art surveillance tools. It is enough to think of the smart devices and all the apps that we use daily. The change in the ways and technology used for surveillance, has made it easier and normal to shift from targetted surveillance to mass surveillance. This has inevitably led to distortion of the classic legal safeguards that must be provided to individuals. Such may include, for example, the right to presumption of innocence and the right not to incriminate oneself that were already studied under the right to a fair trial covered in Chapter 6 of this book.

Due to the almost unrebuttable nature of digital evidence, the right to presumtion of innocence has shifted to an almost presumption of guilt. This brings a shift in the the burden of proof requiring that the suspect activily needs to prove the innocence.[1]

The dilution of the right not to incriminate oneselve, was also discussed under chapter 6. While one is not obliged to provide his passwords for a criminal investigation, in 2021 the Dutch Supreme Court ruled that forcing suspects to provide access to their smartphone with a fingerprint is not a breach of the privilege against self-incrimination.[2]

Since the preventive, investigative, detective, etc. activities of Law Enforcement authorities clearly fall under the definition of State interference with the private sphere of individuals, the right to privacy has been extensively used for the protection of individuals from unlawful interferences. These can be also seen in the extensive case law from the ECtHR. However, the right to privacy does not protect individuals with regards to unlawful processing of their personal data. Below you can find examples that show that the right to privacy is not enough.

a. Surveillance of individuals in public spaces

ECtHR, *P.G. and J.H. v. the United Kingdom*, Application no. 44787/98, 25 December 2001

> [57] There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. ***Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain***.

1. Milaj-Weishaar, J., & Mifsud Bonnici, J. (2014). Unwitting subjects of surveillance and the presumption of innocence. Computer Law & Security Review, 30(4), 419-428

2. https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:HR:2021:202

Following the reasoning of the ECtHR in the case above, the right to privacy will protect personal data of individuals collected in open space only when a permanent or systematic recording has taken place. Thus, not all data and not in all circumstances. The right to data protection, on the other side, focuses on protecting personal data as defined under article 4(1) GDPR, without distinguishing between the public or not nature of the data. While an interference with the private life of the individual for activities taking place in public will not always fall under the protection of the right to privacy, it will fall under the protection of the right to data protection.

b. Identified or identifiable individual

ECtHR, *Friedl v Austria*, application No. 15225/89, 19 May 1994

[49] In the present case, the Commission has noted the following elements: first, there was no intrusion into the "inner circle" of the applicant's private life in the sense that the authorities entered his home and took the photographs there; secondly, the photographs related to a public incident, namely a manifestation of several persons in a public place, in which the applicant was voluntarily taking part; and thirdly, they were solely taken for the purposes, on 17 February 1988, of recording the character of the manifestation and the actual situation at the place in question, e.g. the sanitary conditions, and, on 19 February 1988, of recording the conduct of the participants in the manifestation in view of ensuing investigation proceedings for offences against the Road Traffic Regulations.

[50] In this context, the Commission attaches weight to the assurances given by the respondent Government according to which the individual persons on the photographs taken remained anonymous in that no names were noted down, the personal data recorded and photographs taken were not entered into a data processing system, and no action was taken to identify the persons photographed on that occasion by means of data processing.

[51] Bearing these factors in mind, the Commission finds that the taking of photographs of the applicant and their retention do not amount to an interference with his right to respect for his private life within the meaning of Article 8 para. 1 (Art. 8-1) of the Convention.

In the above case it was ruled that there is a distinction to be made with reference to taking and keeping of photographs depending on the purpose. Taking photos without identifying subjects is not considered to interfere with art. 8(1) ECHR. Thus, no interference with the right to privacy. However, under the right to data protection, a data subject is protected also when not directly identified but being identifiable. This is

clearly stated in the defidition of article 4(1) GDPR as well as the case law of the CJEU discussed in Chapter 10 of this book.

c. Incidental collection of data or incidental surveillance

ECtHR, *Kruslin v France*, application no 11801/85 25 April 1990

[34] The Court does not in any way minimise the value of several of the safeguards, in particular the need for a decision by an investigating judge, who is an independent judicial authority; the latter's supervision of senior police officers and the possible supervision of the judge himself by the Indictment Division, by trial courts and courts of appeal and, if need be, by the Court of Cassation; the exclusion of any "subterfuge" or "ruse" consisting not merely in the use of telephone tapping but in an actual trick, trap or provocation; and the duty to respect the confidentiality of relations between suspect or accused and lawyer.

It has to be noted, however, that only some of these safeguards are expressly provided for in Articles 81, 151 and 152 of the Code of Criminal Procedure. Others have been laid down piecemeal in judgments given over the years, the great majority of them after the interception complained of by Mr Kruslin (June 1982). Some have not yet been expressly laid down in the case-law at all, at least according to the information gathered by the Court; the Government appear to infer them either from general enactments or principles or else from an analogical interpretation of legislative provisions – or court decisions – concerning investigative measures different from telephone tapping, notably searches and seizure of property. Although plausible in itself, such "extrapolation" does not provide sufficient legal certainty in the present context.

Thus, in cases of incidental collection of data, the right to privacy is not considered automatically as infringed in light with the margin of appreciation left to the States for as long as there is the possibility to challenge the surveilling mandate before national courts. However, such situation qualifies as an infringement of the right to data protection since two of the principles of article 5 GDPR are infringed: the principle of purpose limitation (art 5(1)(b)) and the principle of data minimisation (art 5(1)(c)).

The example below shows a situation that would have not been falling under the violation of the right to privacy for all the 3 situations explained above: i. activity taking place in public; ii. no identification of data subjects; iii. incidental collection of data. However, a fine was issued for violation of the GDPR.

The Dutch Supervisory Authority fined the municipality of Enschede with EUR 600,000 in 2021. The municipality had installed special measurement boxes to measure crowds in the city center. Sensors in the measurement boxes detected the wifi signals from the cell phones of passers-by and registered them with a code. Based on the registered codes, it was possible to calculate how busy the city center was. However, this also made it possible to track which measurement box a particular cell phone passed by, making it possible to track the movement of passers-by.

(15.2) The Law Enforcement Directive (LED)

The LED is an EU secondary legal instrument which harmonizes the requirements for the processing of data in law enforcement activities. It replaces the 2008 Council Framework Decision and has a broader scope of application – in addition to covering activities aimed at preventing, investigating, detecting and prosecuting criminal offences, it also covers prevention of threats to public (not national) security. The rules on data processing in the LED are aligned with those established by the GDPR in order to ensure that the general principles are applicable and thus individuals retain their rights, including compensation and access to supervisory authorities.

There are various reasons why the processing of data in the framework of law enforcement activities are regulated in a separate Directive and not in the GDPR. The first and main reason lies in the fact that criminal law and procedure are not harmonised at EU level. As a result, national criminal law procedures vary from one Member State to another. As such, the field is better suited for harmonization through directives as opposed to regulations.

The second reason is linked with the standards for protecting data subjects. Given the nature of law enforcement activities, and especially the operational needs of authorities for data during the performance of their tasks, LED offers lower and varied safeguards for data subjects, depending on their status as: victims, witnesses, suspects, etc. The 'transparency' requirements in the LED, for example, are reduced. This is justified by the nature of law enforcement tasks. For the same reasons, data subject rights are also limited in cases when the right:

- obstructs an official/legal inquiry, investigation or procedure;
- prejudices the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- jeopardizes public security, national security or the rights and freedoms of others;
- requirement of accuracy should not appertain to accuracy of statement but merely to the fact that a

specific statement has been made.

Recital 30 LED – The principle of accuracy of data should be applied while taking account of the nature and purpose of the processing concerned. In particular in judicial proceedings, statements containing personal data are based on the subjective perception of natural persons and are not always verifiable. Consequently, the requirement of accuracy should not appertain to the accuracy of a statement but merely to the fact that a specific statement has been made.

.....

Recital 47 LED – A natural person should have the right to have inaccurate personal data concerning him or her rectified, in particular where it relates to facts, and the right to erasure where the processing of such data infringes this Directive. However, the right to rectification should not affect, for example, the content of a witness testimony. A natural person should also have the right to restriction of processing where he or she contests the accuracy of personal data and its accuracy or inaccuracy cannot be ascertained or where the personal data have to be maintained for purpose of evidence. In particular, instead of erasing personal data, processing should be restricted if in a specific case there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject. In such a case, restricted data should be processed only for the purpose which prevented their erasure. Methods to restrict the processing of personal data could include, inter alia, moving the selected data to another processing system, for example for archiving purposes, or making the selected data unavailable. In automated filing systems the restriction of processing should in principle be ensured by technical means. The fact that the processing of personal data is restricted should be indicated in the system in such a manner that it is clear that the processing of the personal data is restricted. Such rectification or erasure of personal data or restriction of processing should be communicated to recipients to whom the data have been disclosed and to the competent authorities from which the inaccurate data originated. The controllers should also abstain from further dissemination of such data.

Recital 48 LED – Where the controller denies a data subject his or her right to information, access to or rectification or erasure of personal data or restriction of processing, the data subject should have the right to request that the national supervisory authority verify the lawfulness of the processing. The data subject should be informed of that right. Where the supervisory authority acts on behalf of the data subject, the data subject should be informed by the supervisory authority at least that all necessary verifications or reviews by the supervisory

authority have taken place. The supervisory authority should also inform the data subject of the right to seek a judicial remedy.

(15.2.1) LED personal and material scope of application

To understand if the GDPR or LED is the applicable law in a specific situation, one must take a closer look at their scopes and purposes. While the GDPR has a wide material and personal scope, the LED applies only to competent authorities when exervising law enforcement purposes. For reaching this conclusion, Articles 1(1), 2(1) and 3(7-9) LED need to be considered jointly.

Article 1(1) LED – Subject-matter and objectives

1. This Directive lays down the rules relating to the protection of natural persons with regard to the **processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.**

Article 2(1) LED – Scope

1. This Directive applies to the **processing of personal data by competent authorities** for the purposes set out in Article 1(1).

Article 3(7-9) LED – Definitions

7. 'competent authority' means:

a) **any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security**; or

b) **any other body or entity entrusted by Member State law to exercise public authority and public powers** for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

8. **'controller' means the competent authority** which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

9. **'processor' means a natural or legal person, public authority, agency or other body** which processes personal data on behalf of the controller;

(15.3) Data retention for law enforcement purposes

The EU Data Retention Directive (2006/24/EC), adopted in 2006, required Member States to store metadata from electronic communications (such as phone calls, emails, and text messages) for a period of 6 months up to 2 years. The purpose was to assist law enforcement authorities in combating serious crime, including terrorism. The metadata retained included information such as call duration, location, device, communication participants, etc., but not the content of the communications. .

The Court of Justice of the European Union annulled the Data Retention Directive (2006/24/EC) in its *Digital Rights Ireland* judgment (Joined cases C-293/12 and C-594/12) on 8 April 2014, with *ex tunc* effect, meaning it was void retroactively as if it had never been in force. The Court ruled that the Directive violated fundamental rights under the EU Charter of Fundamental Rights, specifically the right to privacy (Article 7 CFR) and the right to data protection (Article 8 CFR). It found the Directive disproportionate, as it required

indiscriminate and bulk retention of metadata from all individuals, regardless of any link to criminal activity, and lacked sufficient safeguards against abuse or misuse of retained data.[3]

Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* EU:C:2014:238

33. To establish the existence of an interference with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way (see, to that effect, Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* EU:C:2003:294, paragraph 75) [...]

37. It must be stated that the interference caused by Directive 2006/24 with the fundamental rights laid down in Articles 7 and 8 of the Charter is, as the Advocate General has also pointed out, in particular, in paragraphs 77 and 80 of his Opinion, wide-ranging, and it must be considered to be particularly serious. Furthermore, as the Advocate General has pointed out in paragraphs 52 and 72 of his Opinion, the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.

Justification of the interference with the rights guaranteed by Articles 7 and 8 of the Charter

38. Article 52(1) of the Charter provides that any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

39. So far as concerns the essence of the fundamental right to privacy and the other rights laid down in Article 7 of the Charter, it must be held that, even though the retention of data required by Directive 2006/24 constitutes a particularly serious interference with those

3. Milaj, J. (2015). Invalidation of the data retention directive – Extending the proportionality test. Computer Law & Security Review, 31(5), 604-617. https://doi.org/10.1016/j.clsr.2015.07.004

rights, it is not such as to adversely affect the essence of those rights given that, as follows from Article 1(2) of the directive, the directive does not permit the acquisition of knowledge of the content of the electronic communications as such [...]

41. As regards the question of whether that interference satisfies an objective of general interest, it should be observed that, whilst Directive 2006/24 aims to harmonise Member States' provisions concerning the obligations of those providers with respect to the retention of certain data which are generated or processed by them, the material objective of that directive is, as follows from Article 1(1) thereof, to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. The material objective of that directive is, therefore, to contribute to the fight against serious crime and thus, ultimately, to public security [...]

44. It must therefore be held that the retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by Directive 2006/24, genuinely satisfies an objective of general interest.

45.l In those circumstances, it is necessary to verify the proportionality of the interference found to exist [...]

49. As regards the question of whether the retention of data is appropriate for attaining the objective pursued by Directive 2006/24, it must be held that, having regard to the growing importance of means of electronic communication, data which must be retained pursuant to that directive allow the national authorities which are competent for criminal prosecutions to have additional opportunities to shed light on serious crime and, in this respect, they are therefore a valuable tool for criminal investigations. Consequently, the retention of such data may be considered to be appropriate for attaining the objective pursued by that directive [...]

51. As regards the necessity for the retention of data required by Directive 2006/24, it must be held that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight [...]

56. As for the question of whether the interference caused by Directive 2006/24 is limited to what is strictly necessary, it should be observed that, in accordance with Article 3 read in conjunction with Article 5(1) of that directive, the directive requires the retention of all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and

> Internet telephony. It therefore applies to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives. Furthermore, in accordance with Article 3 of Directive 2006/24, the directive covers all subscribers and registered users. It therefore entails an interference with the fundamental rights of practically the entire European population [...]
>
> 58. Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy [...]
>
> 64. Furthermore, that period is set at between a minimum of 6 months and a maximum of 24 months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary [...]
>
> 69. Having regard to all the foregoing considerations, it must be held that, by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter [...]
>
> 71. Consequently, the answer to the second question, parts (b) to (d), in Case C-293/12 and the first question in Case C-594/12 is that **Directive 2006/24 is invalid**.

However, despite the invalidation of the Directive, Member States continued to maintain their national laws on data retention. This was based on the EU principle of subsidiarity in shared competences. If the EU has not occupied the field, the Member States can have their national regulation in place. The CJEU has discussed the topick of data retention in a number of judgments following the *Digital Rights Ireland* case. In *Tele2 Sverige*, national data retention laws for the purposes of law enforcement are discussed.

Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* EU:C:2016:970

103. Further, while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight.

Note: see by analogy in relation to Directive 2006/24, the *Digital Rights* judgment, paragraph 51.

Member States have also introduced national laws for data retention for the purposes of national security. Despite the fact that national security falls outside the scope of application of EU law, as provided for in article 4(2) TEU, the CJEU has linked such cases to the functioning of the internal market since the providers of electronic communication services are operators in the internal market.

Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* EU:C:2020:790

44. Article 4(2) TEU, to which the governments listed in paragraph 32 above have made reference, cannot invalidate that conclusion. Indeed, according to the settled case-law of the Court, although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law [...]

48. By contrast, where the Member States directly implement measures that derogate from the rule that electronic communications are to be confidential, without imposing processing obligations on providers of electronic communications services, the protection of the data of the persons concerned is not covered by Directive 2002/58, but by national law only, subject to the application of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on

the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89), with the result that the measures in question must comply with, inter alia, national constitutional law and the requirements of the ECHR.

49. Having regard to the foregoing considerations, the answer to the first question is that Article 1(3), Article 3 and Article 15(1) of Directive 2002/58, read in the light of Article 4(2) TEU, must be interpreted as meaning that national legislation enabling a State authority to require providers of electronic communications services to forward traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security falls within the scope of that directive [...]

60. In addition, it is apparent from the third sentence of Article 15(1) of Directive 2002/58 that the Member States are not permitted to adopt legislative measures to restrict the scope of the rights and obligations provided for in Articles 5, 6 and 9 of that directive unless they do so in accordance with the general principles of EU law, including the principle of proportionality, and with the fundamental rights guaranteed in the Charter. In that regard, the Court has previously held that the obligation imposed on providers of electronic communications services by a Member State by way of national legislation to retain traffic data for the purpose of making it available, if necessary, to the competent national authorities raises issues relating to compatibility not only with Articles 7 and 8 of the Charter, relating to the protection of privacy and to the protection of personal data, respectively, but also with Article 11 of the Charter, relating to the freedom of expression (see, to that effect, judgments of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 25 and 70, and of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 91 and 92 and the case-law cited) [...]

62. Thus, the interpretation of Article 15(1) of Directive 2002/58 must take account of the importance both of the right to privacy, guaranteed in Article 7 of the Charter, and of the right to protection of personal data, guaranteed in Article 8 thereof, as derived from the case-law of the Court, as well as the importance of the right to freedom of expression, given that that fundamental right, guaranteed in Article 11 of the Charter, constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU, the Union is founded [...]

64. Indeed, as can be seen from Article 52(1) of the Charter, that provision allows limitations to be placed on the exercise of those rights, provided that those limitations are provided for by law, that they respect the essence of those rights and that, in compliance with the principle of proportionality, they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others [...]

82. In the light of all the foregoing considerations, the answer to the second question is that Article 15(1) of Directive 2002/58, read in the light of Article 4(2) TEU and Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation enabling a State authority to require providers of electronic communications services to carry out the general and indiscriminate transmission of traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security.

Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v Premier ministre and Others* EU:C:2020:791

[137] Thus, in situations such as those described in paragraphs 135 and 136 of the present judgment, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not, in principle, preclude a legislative measure which permits the competent authorities to order providers of electronic communications services to retain traffic and location data of all users of electronic communications systems for a limited period of time, as long as there are sufficiently solid grounds for considering that the Member State concerned is confronted with a serious threat, as referred to in paragraphs 135 and 136 of the present judgment, to national security which is shown to be genuine and present or foreseeable. Even if such a measure is applied indiscriminately to all users of electronic communications systems, without there being at first sight any connection, within the meaning of the case-law cited in paragraph 133 of the present judgment, with a threat to the national security of that Member State, it must nevertheless be considered that the existence of that threat is, in itself, capable of establishing that connection.

[138] The instruction for the preventive retention of data of all users of electronic communications systems must, however, be limited in time to what is strictly necessary. Although it is conceivable that an instruction requiring providers of electronic communications services to retain data may, owing to the ongoing nature of such a threat, be renewed, the duration of each instruction cannot exceed a foreseeable period of time. Moreover, such data retention must be subject to limitations and must be circumscribed by strict safeguards making it possible to protect effectively the personal data of the persons concerned against the risk of abuse. Thus, that retention cannot be systematic in nature.

[139] In view of the seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter resulting from a measure involving the general and indiscriminate retention of data, it must be ensured that recourse to such a measure is in fact limited to situations in which there is a serious threat to national security as referred to in paragraphs 135 and 136 of the present judgment. For that purpose, it is essential that decisions giving an instruction to providers of electronic communications services to carry out such data retention be subject to effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed.

More recently, the CJEU has also ruled with regards to the admissibility of evidence based on data retention practices that have been invalidated.

Joined Cases C-339/20 *VD* and C-397/20 *SR*

[105] In that regard, it is sufficient to refer to the Court's case-law, in particular to the principles recalled in paragraphs 41 to 44 of the judgment of 2 March 2021, Prokuratuur (Conditions of access to data relating to electronic communications) (C-746/18, EU:C:2021:152), from which it follows that such admissibility falls, in accordance with the principle of the procedural autonomy of the Member States, within the scope of national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness.

[106] As regards the latter principle, it should be noted that it requires national criminal courts to disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law or by means of access of the competent authority to those data in breach of EU law, in the context of criminal proceedings against persons suspected of having committed criminal offences, where those persons are not in a position to comment effectively on that information and that evidence and they pertain to a field of which the judges have no knowledge and are likely to have a preponderant influence on the findings of fact (see, to that effect, judgment of 2 March 2021, Prokuratuur (Conditions of access to data relating to electronic communications), C-746/18, EU:C:2021:152, paragraph 44 and the case-law cited).

[107] In the light of the findings above, the answer to the second and third questions in the present

cases is that EU law must be interpreted as precluding a national court from restricting the temporal effects of a declaration of invalidity which it is required to make, under national law, with respect to provisions of national law which, first, require operators providing electronic communications services to retain generally and indiscriminately traffic data and, second, allow such data to be submitted to the competent financial authority, without prior authorisation from a court or independent administrative authority, owing to the incompatibility of those provisions with Article 15(1) of Directive 2002/58 read in the light of the Charter. The admissibility of evidence obtained pursuant to provisions of national law that are incompatible with EU law is, in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness.

15.4 Predictive policing and the AI Act

The AI act has introduced a number of provisions that are linked with the use of AI in the work of law enforcement authorities.

Certain uses of AI for law enforcement are prohibited. We find these under article 5 AI act.

Article 5 AI act

Para 1(d) – the placing on the market, the putting into service for this specific purpose, or the use of an AI system for making **risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence**, based solely on the profiling of a natural person or on assessing their personality traits and characteristics; this prohibition shall not apply to AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity;

Para 1(e) – the placing on the market, the putting into service for this specific purpose, or the use of AI systems that create or expand **facial recognition databases** through the untargeted scraping of facial images from the internet or CCTV footage;

...

Para 1(h) – the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, unless and in so far as such use is strictly necessary for one of the following objectives:

i. the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons;

ii. the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack;

iii. the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years.

Point (h) of the first subparagraph is without prejudice to Article 9 of Regulation (EU) 2016/679 for the processing of biometric data for purposes other than law enforcement.

2. The use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement for any of the objectives referred to in paragraph 1, first subparagraph, point (h), shall be deployed for the purposes set out in that point only to confirm the identity of the specifically targeted individual, and it shall take into account the following elements:

(a) the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm that would be caused if the system were not used;

(b) the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences.

In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement for any of the objectives referred to in paragraph 1, first subparagraph, point (h), of this Article shall comply with necessary and proportionate safeguards and conditions in relation to the use in accordance with the national law authorising the use thereof, in particular as regards the temporal, geographic and personal limitations. The use of the 'real-time' remote biometric identification system in publicly accessible spaces shall be authorised only if the law enforcement authority has completed a fundamental rights impact assessment as provided for in Article 27 and has registered the system in the EU database according to Article 49. However, in duly justified cases of urgency, the use of such systems may be

commenced without the registration in the EU database, provided that such registration is completed without undue delay.

3. For the purposes of paragraph 1, first subparagraph, point (h) and paragraph 2, each use for the purposes of law enforcement of a 'real-time' remote biometric identification system in publicly accessible spaces shall be subject to a prior authorisation granted by a judicial authority or an independent administrative authority whose decision is binding of the Member State in which the use is to take place, issued upon a reasoned request and in accordance with the detailed rules of national law referred to in paragraph 5. However, in a duly justified situation of urgency, the use of such system may be commenced without an authorisation provided that such authorisation is requested without undue delay, at the latest within 24 hours. If such authorisation is rejected, the use shall be stopped with immediate effect and all the data, as well as the results and outputs of that use shall be immediately discarded and deleted.

The competent judicial authority or an independent administrative authority whose decision is binding shall grant the authorisation only where it is satisfied, on the basis of objective evidence or clear indications presented to it, that the use of the 'real-time' remote biometric identification system concerned is necessary for, and proportionate to, achieving one of the objectives specified in paragraph 1, first subparagraph, point (h), as identified in the request and, in particular, remains limited to what is strictly necessary concerning the period of time as well as the geographic and personal scope. In deciding on the request, that authority shall take into account the elements referred to in paragraph 2. No decision that produces an adverse legal effect on a person may be taken based solely on the output of the 'real-time' remote biometric identification system. [...]

Other uses of AI are considered as high risk for the protection of the rights of individuals. We find these under Annex III of the AI Act. In these cases, the use of AI technology is not prohibited, but strict safeguards need to be followed in compliance with the provisions of the Act.

AI Act Annex III – High-risk AI systems referred to in Article 6(2)

High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas:

1. Biometrics, in so far as their use is permitted under relevant Union or national law:

a. remote biometric identification systems.

This shall not include AI systems intended to be used for biometric verification the sole purpose of which is to confirm that a specific natural person is the person he or she claims to be;

b. AI systems intended to be used for biometric categorisation, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics;

c. AI systems intended to be used for emotion recognition.

...

6. Law enforcement, in so far as their use is permitted under relevant Union or national law:

(a) AI systems intended to be used by or on behalf of law enforcement authorities, or by Union institutions, bodies, offices or agencies in support of law enforcement authorities or on their behalf to assess the risk of a natural person becoming the victim of criminal offences;

(b) AI systems intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices or agencies in support of law enforcement authorities as polygraphs or similar tools;

(c) AI systems intended to be used by or on behalf of law enforcement authorities, or by Union institutions, bodies, offices or agencies, in support of law enforcement authorities to evaluate the reliability of evidence in the course of the investigation or prosecution of criminal offences;

(d) AI systems intended to be used by law enforcement authorities or on their behalf or by Union institutions, bodies, offices or agencies in support of law enforcement authorities for assessing the risk of a natural person offending or re-offending not solely on the basis of the profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680, or to assess personality traits and characteristics or past criminal behaviour of natural persons or groups;

(e) AI systems intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices or agencies in support of law enforcement authorities for the profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of the detection, investigation or prosecution of criminal offences.

16. MODERN CHALLENGES AND FINAL REFLECTIONS

Chapter outline

Without aiming to be exhaustive, the main aim of this last chapter of the book is to provide a quick reflection in the way the data protection legal framework has operated thus far in the Union. Furthermore, it introduces current developments and challenges that the legal framework is facing due to data driven innovation developments.

In 2016, when the new data protection package was introduced in the European Union, including the GDPR, LED, and other laws, it was a clear achievement in the field. While technology and digital services are advancing daily, clear data protection rules gave the message that technology should develop in compliance with legal rules to benefit the people and not vice versa. Controllers were presented with one set of harmonized rules for all their processing activities in the Union and data subjects with a set of rights that were meant to give them back control over their data. The extra territorial scope of application of the GDPR, ensured that data subjects in the EU are protected independently of the location of the controllers and processors.

Big corporations in various sectors of the digital economy faced high fines, the highest thus far being the 1.2 billion Euro fine that Meta received in May 2023 for violating the rules on transfers of data to the US based on the appropriate standards of article 46 GDPR.

At the same time, the so called, Brussels effect, motivated third countries, including China, to adopt national rules mirroring the GDPR provisions in order to help their businesses and digital corporations to continue processing data from the EU. The GDPR rules are seen as the gold standard for the introduction of new data protection policies around the world.

However, almost 10 years after the adoption, the initial success story and enthusiasm of the GDPR is showing some cracks. While Supervisory Authorities that follow the same rules and procedures are created and operate in all the Member States, they have not been able to enforce the rules in a harmonized way. Each

Member State of the Union has its own legal tradition and priorities. With regards to the GDPR, different approaches are seen in the way the law is enforced. Some countries, as for example Spain, are focusing on small perpetrators, others, like the Netherlands are focusing on serious infringements. Thus, the incentives for compliance towards controllers in various Member States differ. The second report on the implementation of the GDPR shows that:

> Data protection authorities have launched over 20 000 own-initiative investigations.
>
> They collectively receive over 100 000 complaints per year.
>
> The median time for data protection authorities to handle complaints (from receipt to closure of the case) ranges from 1 to 12 months, and is 3 months or less in five Member States (Denmark (1 month), Spain (1.5 months), Estonia (3 months), Greece (3 months) and Ireland (3 months)).
>
> Over 20 000 complaints have been resolved through amicable settlement. It is most commonly used in Austria, Hungary, Luxembourg and Ireland.
>
> In 2022, data protection authorities in Germany adopted the highest number of decisions imposing a corrective measure (3 261), followed by Spain (774), Lithuania (308) and Estonia (332). The lowest number of corrective measures was imposed in Liechtenstein (8), Czechia (8), Iceland (10), the Netherlands (17) and Luxembourg (22).
>
> Data protection authorities have imposed over 6 680 fines amounting to around EUR 4.2 billion. The authority in Ireland has imposed the highest total amount of fines (EUR 2.8 billion) followed by Luxembourg (EUR 746 million), Italy (EUR 197 million) and France (EUR 131 million). Liechtenstein (EUR 9 600), Estonia (EUR 201 000) and Lithuania (EUR 435 000) have imposed the lowest amount of fines.

The high fines issued on big tech companies show the seriousness of Supervisory Authorities with regards to GDPR infringements, but at the same time have been hardly having the desired deterrent effects. In the list of fines, companies like Meta appear to be repeat offenders. In other cases, like with regards to the US company ClearView AI, the execution of multiple fines given by different Supervisory Authorities seems difficult to be achieved due to the lack of any assets in the EU.

In the current data driven economy, the original right-based approach of the GDPR, focusing on the protection of the fundamental right to data protection as embedded in the EU Charter of Fundamental Rights was seen as too restrictive. A risk-based approach was quickly supported. The adoption of other laws in the European Union that are closely linked to the GDPR due to reliance on personal data processing for various purposes, like the Data Act, Data Governance Act, Digital Services Act, AI Act, etc. as well as the creation

of common European Data Spaces, focus mainly on the internal market and rely on this risk-based approach. Thus, the standards of data protection as a fundamental right are weakened in various ways.

In September 2024, a report outlining the barriers to growth that Europe currently faces was published. In this report, from former European Central Bank President Mario Draghi, highlights the fact that Europe needs to re-focus the energies if it wants to be a player in the global digital economy.

> If Europe cannot become more productive, we will be forced to choose. We will not be able to become, at once, a leader in new technologies, a beacon of climate responsibility and an independent player on the world stage. We will not be able to finance our social model. We will have to scale back some, if not all, of our ambitions.

In this framework, the GDPR is seen as too restrictive, complicated and a heavy burden for small and medium size enterprizes. The costs that SMEs face for compliance with the GDPR are calculated as extensive and prohibitive for innovation. Thus, the report advocates for regulatory light-handed rules to promote EU investment and innovation instead of stronger ex ante regulatory safeguards for fundamental rights and product safety.

> Finally, while the ambitions of the EU's GDPR and AI Act are commendable, their complexity and risk of overlaps and inconsistencies can undermine developments in the field of AI by EU industry actors. The differences among Member States in the implementation and enforcement of the GDPR (as detailed in the Governance Chapter), as well as overlaps and areas of potential inconsistency with the provisions of the AI Act create the risk of European companies being excluded from early AI innovations because of uncertainty of regulatory frameworks as well as higher burdens for EU researchers and innovators to develop homegrown AI. As in global AI competition 'winner takes most' dynamics are already prevailing, the EU faces now an unavoidable trade-off between stronger ex ante regulatory safeguards for fundamental rights and product safety, and more regulatory light-handed rules to promote EU investment and innovation, e.g. through sandboxing, without lowering consumer standards.

At the time of writing, a reform of the GDPR is being discussed. On one side this reform initiated in 2023 aims

to simplify the work of Supervisory Authorities and to speed up disputes that have a cross-border dimension by introducing strict deadlines for each stage of the procedure before the Authorities.

On the other side, following the Draghi report, in May 2025, the Commission presented an additional proposal to cut €300 million in annual administrative cost for Small and Medium Enterprises (SMEs) and Small and Mid-Caps companies (SMCs). As a result, targeted changes to the rules on record-keeping for small and medium-sized companies and organisations under 750 employees are proposed. The proposal does not affect the rest of the provisions of the GDPR.

This is just a quick synopsis of the current state of affairs in European data protection law. As technology evolves, also priorities in the field of data protection change making the right to data protection an ever complicated, dynamic and why not.... a fascinating one.