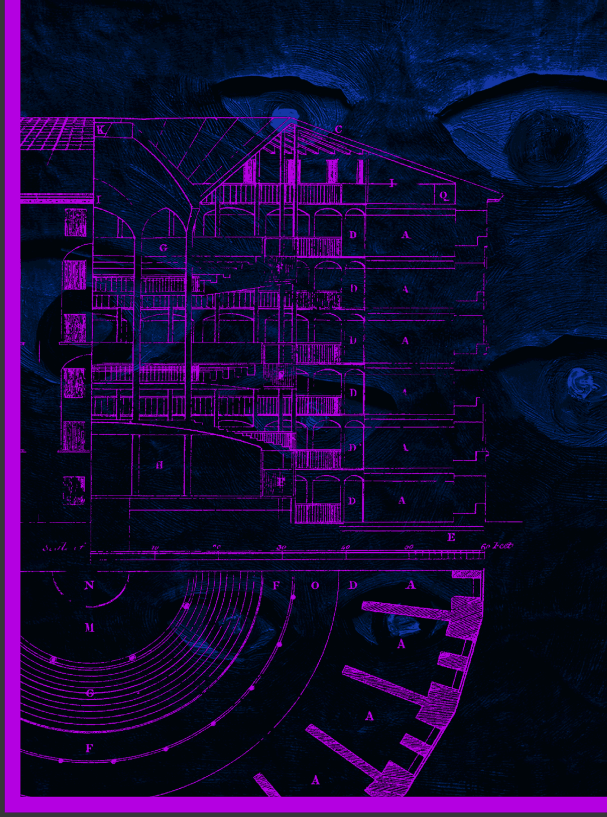
Edited by
Erik Tuchtfeld
Isabella Risini
Jakob Gašperin Wischhoff



Eyes Everywhere

Surveillance and Data Retention under the EU Charter

Verfassungsbooks

Contents

Erik Tuchtfeld Jakob Gašperin Wischhoff Isabella Risini Pre-fa. 12
Erik Tuchtfeld Eyes Every-where: The Pro-lif-er-a-tion of Pub-. 16
Joachim Herrmann More Pro-tec-tion for Vic-tims Through Da. 26
Erik Tuchtfeld Pro-tect-ing Vic-tims Without Mass Sur-veil-lan. 40
Lukas Martin Landerer Data Re-ten-tion: Between Fun-da-men. 58
Aqilah Sandhu Squar-ing the Circle: The CJEU between Fun-d. 70
Ana Bobić Pri-or-it-ising Mem-ber States Over Cit-izens: La Q. 82
Guido Westkamp An-onym-ity and Sur-veil-lance, Cre-ativ-ity. 92
Marcin Rojszczak Data Retention Laws and La Quadrature du. 104
Valentina Lana Aziz Z. Huq Spillovers and Un-ex-pec-ted In-te. 116
Elif Mendos Kuşkonmaz Of Minor Be-ne-fits and Ma-jor Costs. 126
Giulia Formici The Long and Wind-ing Road: The Data Re-ten. 136
Chiara Graziani Data Re-ten-tion in a Cross-Bor-der Per-spect-i. 148
André Bartsch Johanna Fink Jakob Mutter Marc André Boverm. 158
Thomas Christian Bächle New Me-dia, New Data and a Dark F. 170
Sarah Stummer A Right to An-onym-ity in the Di-gital Age: A. 180
Sabine Leutheusser-Schnarrenberger Isabella Risini Erik Tucht. 192

ISBN 978-3-819067-43-3
DOI 10.17176/20250326-133455-0
URN urn:nbn:de:0301-20250326-133455-0-8

Verfassungsbooks

Max Steinbeis Verfassungsblog gGmbH
Elbestraße 28/29
12045 Berlin
verfassungsblog.de
kontakt@verfassungsblog.de

Copyright remains with Erik Tuchtfeld, Isabella Risini, and Jakob Gašperin Wischhoff for their contributions and all contributing authors for their contributions.

The cover is based on Jeremy Bentham's plan of a panopticon prison, drawn by Willey Reveley in 1791.
Cover Design by Till Stadtbäumer. The cover was partially created using AI.

This work is licensed under CC BY-SA 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-sa/4.0/. Different licenses may apply to images in this book as indicated.

Funded by the European Union

focus
FUNDAMENTALS OF EU CHARTER USE IN SOCIETY

FOCUS is a project which aims to raise public awareness of the EU Charter of Fundamental Rights, its value, and the capacity of key stakeholders for its broader application.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them. FOCUS project is funded by the European Commission's Citizens, Equality, Rights and Values (CERV) programme and has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101143236.

Edited by
Erik Tuchtfeld, Isabella Risini & Jakob Gašperin Wischhoff

Eyes Everywhere

Surveillance and Data Retention under the EU Charter

Verfassungsbooks
ON MATTERS CONSTITUTIONAL

Contributing Authors

André Bartsch

André Bartsch is a Doctoral Researcher at the Department of Public Law of the Max Planck Institute for the Study of Crime, Security and Law in Freiburg.

Ana Bobić

Ana Bobić is Principal Investigator of the DFG-funded project "Judicial Conflict and the Reconfiguration of control in the EU" at the Jacques Delors Centre, Hertie School.

Marc André Bovermann

Marc André Bovermann is a Doctoral Researcher at the Department of Public Law of the Max Planck Institute for the Study of Crime, Security and Law in Freiburg.

Thomas Christian Bächle

Thomas Christian Bächle is Head of the Digital Society Research Programme at the Humboldt Institute for Internet and Society in Berlin and a Researcher at the University of Bonn.

Johanna Fink

Johanna Fink is a Doctoral Researcher at the Department of Public Law of the Max Planck Institute for the Study of Crime, Security and Law in Freiburg.

Giulia Formici

Giulia Formici is an Assistant Professor (Senior Researcher) in Public Comparative Law at the University of Parma.

Jakob Gašperin Wischhoff

Jakob Gasperin Wischhoff is the Deputy Editor-in-Chief at Verfassungsblog, focusing on European Union law. He is also a Principal Investigator of the FOCUS Research Project, which examines the EU Charter. He holds a PhD from Humboldt University of Berlin.

Chiara Graziani

Chiara Graziani is Assistant Professor in Comparative Public Law at Bocconi University, Milan.

Joachim Herrmann

Joachim Herrmann is Bavarian State Minister of the Interior, for Sport and Integration.

Aziz Z. Huq

Aziz Z. Huq is the Frank and Bernice J. Greenberg Professor of Law at the University of Chicago.

Elif Mendos Kuşkonmaz

Elif Mendos Kuşkonmaz is a Lecturer in Law at the University of Essex.

Valentina Lana

Valentina Lana is a Lecturer at Sciences Po and an Attorney currently working in compliance consulting.

Lukas Martin Landerer

Lukas Martin Landerer is a Lawyer for Public Law at W2K Rechtsanwälte based in Freiburg.

Sabine Leutheusser-Schnarrenberger

Sabine Leutheusser-Schnarrenberger is a Board Member of the Friedrich Naumann Foundation for Freedom. From 1992-1996 and from 2009-2013 she was the Federal Minister of Justice of Germany.

Jakob Mutter

Jakob Mutter is a Doctoral Researcher at the Department of Public Law of the Max Planck Institute for the Study of Crime, Security and Law in Freiburg.

Isabella Risini

Isabella Risini is a Senior Editor at Verfassungsblog. She holds a doctorate from Ruhr-University, Bochum and an LL.M. from Chicago-Kent College of Law. She is a Professor at Technical University Georg Agricola in Bochum.

Marcin Rojszczak

Marcin Rojszczak is an Assistant Professor at the Faculty of Law and Administration, Gdańsk University. His research focuses on the areas of IT security and protection of privacy on the internet.

Aqilah Sandhu

Aqilah Sandhu is a Postdoctoral Researcher at the Chair of Constitutional, Administrative and EU Law and Legislative Studies (Prof. Dr. Matthias Rossi) at the University of Augsburg and is currently seconded to the Federal Constitutional Court as a Research Assistant.

Sarah Stummer

Sarah Stummer is the Deputy Head of Department at Fraunhofer SIT and a Researcher at ATHENE.

Erik Tuchtfeld

Erik Tuchtfeld is a Research Fellow at the Max Planck Institute for Comparative Public Law and International Law in Heidelberg, where he heads the humanet3 group. He is an Associate Editor at Verfassungsblog.

Isabelle Weiss

Isabelle Weiss is a Researcher at the Department of Public Law of the Max Planck Institute for the Study of Crime, Security and Law in Freiburg.

Guido Westkamp

Guido Westkamp holds the Chair in Intellectual Property, Media, and Comparative Law at Queen Mary University of London and is a Visiting Professor at the Institute for Information, Media, and Telecommunication Law in Münster.

Content

Erik Tuchtfeld, Jakob Gašperin Wischhoff& Isabella Risini
Preface 11

Erik Tuchtfeld
Eyes Everywhere: The Proliferation of Public and Private Surveillance under the EU Charter 15

Joachim Herrmann
More Protection for Victims Through Data Retention: On the Introduction of a Minimum Data Retention Period for IP Addresses After *La Quadrature du Net II* 25

Erik Tuchtfeld
Protecting Victims Without Mass Surveillance: A Response to Joachim Herrmann 39

Lukas Martin Landerer
Data Retention: Between Fundamental Rights and Integration 57

Aqilah Sandhu
Squaring the Circle: The CJEU between Fundamental Rights Guardian and Architect of a Security Union 69

Ana Bobić
Prioritising Member States Over Citizens: *La Quadrature du Net II* and the Growing Space for Member State Preferences 81

Guido Westkamp
Anonymity and Surveillance, Creativity and Copyright: Disrupting the Balance Between Users, Authors, Exploiters, and Platforms 91

Marcin Rojszczak
Data Retention Laws and *La Quadrature du Net II*: A Necessary Adjustment to a Timely Problem 103

Valentina Lana& Aziz Z. Huq
Spillovers and Unexpected Interactions: Reading the *La Quadrature du Net II* Decision in Context 115

Elif Mendos Kuşkonmaz
Of Minor Benefits and Major Costs: Reformulating the Fundamental Rights Question of the Privatisation of Surveillance in *La Quadrature du Net II* 125

Giulia Formici
The Long and Winding Road: The Data Retention Discipline in the European Union Between Judicial Intervention and Legislative Resistance 135

Chiara Graziani
Data Retention in a Cross-Border Perspective: Latest Insights from the European Union and the United States 147

André Bartsch, Johanna Fink, Jakob Mutter, Marc André Bovermann& Isabelle Weiss
Testing the Waters of Private Data Pools: How a General Surveillance Account Could Cover Privately Collected Data 157

Thomas Christian Bächle
New Media, New Data and a Dark Foreboding: Surveillance as Observation, Simulation, and Weapon 169

Sarah Stummer
A Right to Anonymity in the Digital Age: A Discussion of the Opportunities, Risks and Limitations 179

Sabine Leutheusser-Schnarrenberger, Isabella Risini& Erik Tuchtfeld
The Challenges of Nuance: Five Questions to Sabine Leutheusser-Schnarrenberger 191

Erik Tuchtfeld, Jakob Gašperin Wischhoff & Isabella Risini

Preface

The controversies surrounding data retention and mass surveillance reflect a foundational dilemma for the resilience of liberal societies. While some argue that extensive surveillance is a necessary tool to effectively provide security, others emphasize that blanket data collection itself constitutes a departure from liberal core values and carries an inherent risk of abuse, not only by authoritarian forces.

This fundamental conflict goes far beyond the discussion of public data collection. It coincides with a data-driven economy that is based on the complete and constant monitoring of human behavior online. Against this backdrop, the boundaries between state and private surveillance are becoming increasingly blurred, with governments and Big Tech companies increasingly collaborating and eventually becoming inextricably intertwined (as it is currently unfolding in the US). The *Eyes Everywhere* Symposium on Verfassungsblog responds to a pressing need to continuously engage legal, political, and societal perspectives in dialogue. In response to the Court of Justice of the European Union's plenary decision in *La Quadrature du Net II* (C-470/21) last year, leading scholars and practitioners from across Europe and the United States have contributed analyses that expose the legal fault lines, technological and economic realities, and societal implications of contemporary surveillance systems.

By bringing these various views together, this book aims to preserve and propel the critical debates sparked by the respective case law and discussed at the Symposium. It speaks to lawyers, policymakers, and anyone else who refuses to accept the gradual rise of surveillance as inevitable. May it provoke, challenge, and, above all, keep the debate surrounding the underlying tension between privacy and security alive, ultimately leading to a more robust and nuanced protection of fundamental rights in the digital age.

We are genuinely thankful to the FOCUS project, which not only funded for this book but also significantly extended the reach of these academic discussions. Moreover, we thank our DRI partners for their assistance and coordination. Furthermore, we express our gratitude to Jakob Weickert, Till Stadtbäumer, Evin Dalkilic, Verena Vortisch, and Marietta Ostendorf, who have supported this endeavor from the initial concept to the final editing, making this volume possible. Lastly, this book would not have been possible without the dedicated and critical contributions of its authors. Your insightful analysis and sharp wit are the heart of this volume, and we are grateful for the opportunity to work with and learn from you.

Erik Tuchtfeld

Eyes Everywhere

The Proliferation of Public and Private Surveillance under the EU Charter

Ten years after its groundbreaking judgment declaring the Data Retention Directive incompatible with Articles 7 and 8 of the EU Charter of Fundamental Rights, the Full Court significantly eased its previous strict requirements. On 30 April 2024, it issued *La Quadrature Du Net II* (C-470/21) and declared for the first time the general and indiscriminate retention of IP addresses permissible for the purpose of fighting general crime. The Court assumed the need for such retention measures to prevent systemic impunity for crimes committed online. However, the more data is collected online, the more detailed the virtual profiles of individuals become. This raises fundamental questions about online privacy: Are citizens becoming transparent to government agencies in an age of massive private data collection? Must the surveillance enterprise be understood as a public-private partnership, encompassing all areas of human life, and does the EU Charter provide sufficient safeguards to protect the people?

Given the Court of Justice of the European Union's (CJEU) fundamental change of heart, we have brought together a range of scholars and practitioners from Europe and beyond with different disciplinary backgrounds to contextualise the said judgment and to situate it within a broader debate on mass data retention, online surveillance, and anonymity, highlighting the interaction between private and public actors. Moreover, this edited volume discusses the impact of the judgment on fundamental rights under the EU Charter, while also highlighting the state of online surveillance facilitated by the mass storage of private data.

The contributions offer varying perspectives on data retention measures and normative assessments of the Court's ruling. Some authors emphasize the need for enhanced online law enforcement tools, while others critically highlight how the unprecedented

amounts of data, collected by private corporations for commercial purposes, serve as a source of information in criminal proceedings.

The politics of mass data retention

The first two contributions consist of an exchange between **Joachim Herrmann**, the Bavarian Minister of the Interior, and me, **Erik Tuchtfeld**, on the politics of mass data retention. Herrmann calls for the introduction of mass data retention of IP addresses in Germany to effectively protect victims of hate speech and violence. He highlights that the internet has become a stage for serious crimes – from the exchange of child sexual abuse material to the widespread dissemination of hate speech – which has been recognized by the European Court of Justice, eventually reducing the intensity of its judicial review. In Herrmann's view, this is a welcoming development, as it is primarily the task of the democratic legislator to balance conflicting fundamental rights and decide on the proportionality of legislative measures. In my replica, I emphasize that it is a main feature of the rule of law that such a balancing can only take place within the framework defined by constitutions. It is the core task of constitutional courts to assess the proportionality of a measure in question. Since the amount of personal data generated by individuals and stored by private and public institutions has never been larger, I challenge Herrmann's finding that the storage of citizens' data must be increased. Instead, targeted measures against suspects should be deployed, which would be sufficient to enhance law enforcement online.

La Quadrature du Net II - revolution or evolution?

The second cluster of contributions analyzes the judgment *La Quadrature Du Net II* in detail. **Lukas Martin Landerer** reads the decision through the lens of the CJEU's role as motor of integration. While the more recent judgments on data retention have been criticized as weakening the fundamental rights protection of European citizen, Landerer points out that this was the only chance for the Court – already facing threats of *ultra vires* proceedings – to avoid an escalation of the tensions with Member States. In this context, particularly France and Belgium stand out as two Member States relying heavily on data retention, so that the exceptional permission to store data was effectively turned into the rule.

It is the lack of clarity in Union law as well as in the ECJ's jurisprudence which causes a constant struggle between the Member States and the Court, **Aqilah Sandhu** argues. She reads the never-ending data retention saga as a failure of the EU legislator, as it did not manage to re-draft a clear and unambiguous legal basis for data retention in the EU.

Ana Bobić also reflects on the judgment's significance for European integration. She argues that the Court increases the Member States' margins for national solutions, and, as a consequence, reduces the protection of individuals and their rights. In her opinion, this constitutes a general normative shift in European Union law, also shown in budgetary, asylum, and migration policy.

Furthermore, the judgment distorts the delicate balance between users, authors, exploiters, and platforms in the field of copyright law, **Guido Westkamp** argues. In this complex matrix of different interests, the judgment incentivises and reinforces broad enforcement strategies targeting users, and disregards user an-

onymity as a central condition for the exercise of communicative and creative freedoms.

Marcin Rojszczak reconstructs the ten-year-old history of the CJEU's jurisprudence on mass data retention and concludes that last year's decision complements the existing line of jurisprudence. However, he laments the lack of depth in the Court's explanation of the relationship between the collection and processing of low-sensitivity data and their subsequent use by state authorities. This gap, he predicts, will lead to more rulings on the matter in the future.

Valentina Lana and **Aziz Z. Huq** analyze the spillover effects of the judgment, stemming from the interaction of the decision with other bodies of law, such as the GDPR and the DSA, and commercial practice related to data. They are "enriching and complicating" the decision trough contextualization and, among others, identify an expansion of the right to a human decision beyond the established scope in European Union law.

A more critical approach is taken by **Elif Mendos Kuşkonmaz**. In her opinion, the Court's findings cement intrusive practices stemming from the fight against counterterrorism as regular state practice for all kinds of crime. In her analysis of the proportionality of general data retention schemes, she highlights the zero-risk imperative which drives current approaches. In consequence, everyone is treated like a suspect and must be monitored. With regard to data transfers in third countries outside the EU, she argues that the increasingly lower level of protection of fundamental rights in the Union must also be taken into consideration when evaluating the adequacy of foreign data protection regimes, such as the UK's.

Giulia Formici describes the Italian data retention regime, which for a long time remained unimpressed by the CJEU's judg-

ments. Most recently, however, also the Italian legislation, in particular with its broad interpretation of "serious crimes" justifying data retention, came under the scrutiny of the CJEU. In her opinion, the increasing tension between Member States and the CJEU in its attempt to constitutionalize mass surveillance practices should be resolved by the European legislator. While this does not necessarily mean that all national data retention regimes must be harmonized, a concrete set of shared basic principles and safeguards could help Member States to navigate through the complex requirements set out in the Court's case law.

Chiara Graziani analyses the different legal regimes in Europe and the United States and warns that a lowering of privacy standards might be dictated by sheer economic power. In particular, she emphasizes the possibilities of the US government to access the private data pools of US-based Big Tech companies, even when they store their data on European soil, and the lack of judicial control mechanisms to limit such data access.

Privacy in times of surveillance capitalism

The third cluster deals with collection of personal data by private corporations, often prominently dubbed as "surveillance capitalism" (Zuboff), and the access that law enforcement authorities enjoy to these data pools. **André Bartsch**, **Johanna Fink**, **Jakob Mutter**, **Marc Bovermann**, and **Isabelle Weiss** jointly call for more attention to these private data collections when assessing the extent of government surveillance. To this end, they propose a "general surveillance account" (*Überwachungsgesamtrechnung*) covering the access of law enforcement agencies to private data pools. Such a "general surveillance account" must not only include a normative analysis of the surveillance measures but needs to be

based on a solid empirical foundation. Thus, more reporting obligations for law enforcement agencies are needed.

This process of a weaponization of surveillance is also emphasized by **Thomas Christian Bächle**, who describes how techniques of datafication, profiling, targeting and recommending, which were developed by social media platforms to display ads to potential customers, are used by private-public cyberintelligence services to identify combatants and terrorists. Furthermore, he describes how the object of surveillance has expanded in recent times, shifting away from the mere description of what people do to the prediction of what they will do based on probabilities linked to their profiles. To this end, modern technologies analyse voices, gestures, and facial expressions to understand the inside of an individual's mind. If such technologies were to be implemented on a large scale, Bächle concludes, the criminal law of the future might punish the mere thought of committing an illegal act as a violation of the law.

Anonymity in the digital world

To diminish the effects of constant surveillance in the digital realm, many people disguise their civil identity. **Sarah Stummer** underlines the importance of anonymity for many internet users according to recent surveys and explains its relative character. While an individual might be anonymous in relation to other internet users, it can still be identifiable for law enforcement authorities. A right to anonymity, independent of its concrete legal construction, is not absolute, but only granted within certain limits. In her opinion, the ECJ's latest decision considers this, allowing law enforcement to identify internet users and effectively protect victims of online crime.

The book is concluded by an interview with **Sabine Leutheusser-Schnarrenberger**, who was, *inter alia*, Federal Minister of Justice and member of the Bavarian Constitutional Court. We shed some light on the relationship of means and ends, and how they relate over time, when it comes to surveillance.

No conclusion, but some thoughts on an ongoing debate

The debate on data retention has remained as lively as ever over the past 20 years. In this edited volume, we move beyond the technical details of the ECJ's *La Quadrature du Net II* decision to situate it within a broader discussion on anonymity and surveillance, European unity and the EU's boundaries, and the public obligation to store data in an era of constant commercial tracking.

The question of how and when the retention of personal data without any concrete suspicion is legitimate remains at the core of current domestic security policy. In 2024 alone, the ECJ issued the *La Quadrature du Net II* Decision on the retention of communication metadata, the ECtHR ruled in *Podchasov*[1] on access to the content of communications,[2] and the German parliament voted in favor of biometric surveillance of the internet.[3] The latter is a measure that requires the creation of large databases containing all personal images available online.

This highlights how the current debate extends from IP address retention to biometric databases, gaining new momentum with the rise of AI applications. These technologies promise to sift through vast data collections, analyzing and systematizing data points to capture and interpret the often unpredictable and erratic nature of human behaviour.

In times when the legislators' judgment is clouded by fears of potential dangers, it is up to the courts – most notably the ECJ – to

keep an eye on the bigger picture and protect the civil and political freedoms enshrined in the Union's Charter.

References

1. European Court of Human Rights, *Podchasov v. Russia* (Appl. No. 33696/19), Judgment of 13 February 2024.
2. Erik Tuchtfeld, 'No Backdoor for Mass Surveillance' (2024) *Verfassungsblog*.
3. Svea Windwehr, 'Germany Rushes to Expand Biometric Surveillance' *Electronic Frontier Foundation* (7 October 2024), https://www.eff.org/deeplinks/2024/10/germany-rushes-expand-biometric-surveillance.

Joachim Herrmann

More Protection for Victims Through Data Retention

On the Introduction of a Minimum Data Retention Period for IP Addresses After La Quadrature du Net II

"Goodbye data retention", proclaimed former Federal Minister of Justice Sabine Leutheusser-Schnarrenberger,[1] after the European Court of Justice (ECJ) upheld its restrictive jurisprudence on the storage and disclosure of telecommunication traffic data for national security purposes in its 2020 decision *Privacy International* (C-623/17), despite vehement criticism from Member States. However, as the recent judgment by the ECJ (*La Quadrature Du Net II* (C-470/21)) shows, it is just not possible to make such apodictic statements in the field of legal policy. The threat level determines the proportionality of the means – both of which are subject to the perpetual flux of time.

The ECJ's La Quadrature du Net II judgment

With its full court judgment of April 30, 2024, the ECJ has further developed its requirements for the "general and indiscriminate retention of data" of IP addresses: a legal obligation to retain data can not only be contemplated for "objectives of combating serious crime or preventing serious threats to public security" (paras. 77 and 95), but also, under certain circumstances, for "combating criminal offences in general" (paras. 92 and 103). Without access to IP addresses, the Court argues, there would be "a real risk of systemic impunity not only for criminal offences infringing copyright or related rights but also for other types of criminal offences committed online or the commission or preparation of which is facilitated by the specific characteristics of the internet" (para. 119). The ECJ's response to those who, at the mere mention of the words "data retention" – a misleading term in my opinion[2] – reflexively evoke the Orwellian surveillance state is that the storage of IP addresses "does not constitute a serious interference with the privacy of the holders of those addresses, since those data do not al-

low precise conclusions to be drawn about their private life" (para. 103).

The Charter of Fundamental Rights is not a "super police act"

If the opponents of such a data retention obligation nevertheless complain that the judgment is a "misfortune"[3], a "disappointment"[4] and a "sad reversal in the protection of privacy"[5], they fail to recognise that assessments of proportionality must necessarily adapt to changes of the state of security. The judgment was only a surprise for those who are of the opinion that the balancing of fundamental rights results in absolute standards, which the ECJ had created once and for all for the field of data retention with its landmark decision *Digital Rights Ireland* (C-293/12 and C-594/12) of 2014. However, this exceeds the competences of judicial legal interpretation. As the German Federal Constitutional Court (FCC) clarified, the "fundamental rights of the Basic Law, the guarantees of the European Convention on Human Rights (ECHR) and the Charter of Fundamental Rights of the European Union are rooted primarily in common constitutional traditions of the Member States and are thus a manifestation of common European and universal values"[6], but they do not define the details of the investigative powers of law enforcement. Detailed and differentiated limits for interferences with fundamental rights, as, for example, prescribed in Article 13 (3-5) of the German Constitution (protecting the inviolability of the home), are the result of a particular and intense political controversy surrounding the "great eavesdropping offensive" – a similarly misleading framing from the same political camp – and an absolute exception. Comparatively, such detailed requirements for the purposes and limits for storing and accessing telecommunication traffic data do

neither exist in the fundamental rights catalogues of the ECHR and the EU Charter of Fundamental Rights nor in other provisions of the German Constitution.

On the contrary: the values protected by fundamental rights are actually in conflict. On the level of Union law, there are the fundamental rights to respect for privacy and personal data protection, arising from Articles 7 and 8 of the EU Charter of Fundamental Rights, for those whose traffic data is stored and may, where applicable, be accessed. However, fundamental rights are not only rights of defence against state interventions, but also include duties to protect those who are victims of crime. Thus, some have even argued that the complete abandonment of data retention obligations would be incompatible with fundamental rights (see Fischer[7] and Benamor[8]).

"Going dark" in the world wide web

There are innumerable dangers lurking in the internet as a worldwide communications network that connects everyone in virtually all areas of life in real time.

Not even the former Federal Minister of Justice Buschmann disputes that serious crimes are being committed relentlessly via the internet, such as the consumption and distribution of child sexual abuse material. Genuine suffering lies behind the vast majority of criminally relevant images and videos on the internet. Almost every image uploaded online is created offline. In some cases, the production of such image material is even published as a livestream of the abuse. Moreover, the internet is used to obtain opportunities for committing such acts, including so-called cybergrooming. This refers to the targeted contacting of children on the internet with the aim of initiating sexual contacts, in most cases

anonymously or under a false name. Furthermore, the internet is being increasingly used to disseminate hate speech, it is a platform for radicalisation, for exchanging discriminatory materials with like-minded persons and for planning and conducting terror attacks. But even crimes that may be considered less severe are developing extreme dimensions on the internet. For instance, criminals attempt to obtain user login data using all kinds of phishing tactics, with the aim of conducting financial transactions for their own benefit, especially bank account transfers and product orders. Also, ransomware is used for means of digital extortion.

In the anonymity of the Darknet, IP addresses frequently represent the only indicators for investigation activities by the security services (see *La Quadrature du Net I* (C-511/18, C-512/18 and C-520/18), para. 154). To use a figurative comparison, IP addresses are the number plates on the data highways, with the major difference that they are issued dynamically with each time somebody connects to the internet, which means that they can only reveal who is accessing a service as long as the relevant data is stored by the telecommunications provider. If the IP address is no longer stored by the telecommunications provider at the time of the law enforcement agency's request, or cannot be determined due to the lack of any stored port number, investigations usually fail due the absence of further investigative approaches. After the failed Islamist terror attack involving the use of the poisons like ricin and cyanide in January 2023,[9] hardly anyone can seriously doubt that the failure to store IP addresses creates security risks that can put people's lives in danger. It was only the fortunate circumstance that one of the suspects was a customer of a telecommunications provider that stores IP addresses voluntarily for seven days that led the investigators to his home address in Castrop-Rauxel.

"Quick freeze" is not an alternative

The "quick freeze" procedure proposed by the former Federal Minister of Justice is not able to fill the protection gap caused by the omission to store IP addresses. Here, data from the period before the judicial order was issued can only be gathered if it has been stored voluntarily by the provider, for example for commercial purposes. Due to the unavoidable delay until a security service is notified of an offence, the quick freeze procedure is unsuitable, in particular when it comes to combating child sexual abuse. It is also important to note that after a certain period of time, providers are legally obliged by data protection law to irreversibly delete data that they have stored and no longer require. The quick freeze procedure only allows for data to be frozen which is still available at the time of the court's decision. Even in the best cases, providers currently only store IP addresses between four and seven days. Sometimes they store the data only for one day or a few hours, so that the quick freeze procedure is in most cases no longer capable of securing any relevant data.

Proportionality depends on context and time

As with all national security matters, proportionality is a decisive factor when it comes to the question of the legality of storing traffic data. The aim is to create an appropriate balance for the conflicting fundamental rights. This consideration falls within the primary competence of the democratically legitimized legislature. The objectivity of law inevitably reaches a certain limit here, since the question of what is proportionate is always to a certain degree in the eye of the beholder and depends on the latter's values and convictions. In other words, the balancing of the impacts certain

measures have on fundamental rights with the purposes pursued by the law, in particular when they are aiming at protecting citizens' fundamental rights, is at its core a political decision, which is determined by the democratically elected majority. The outcome of this balancing exercise can change when democratic majorities change. For example, a social-liberal government might evaluate the proportionality of a limited retention of IP addresses differently[10] than a Christian-conservative government[11]. The primacy of politics makes it impossible to derive absolute judicial standards from the principle of proportionality that bind the legislature forever.

There is no doubt that one of the great achievements of the rule of law is that independent courts, which, like the ECJ and the Federal Constitutional Court, have the power to review legislation, ensure that the political majority does not lose sight of what is reasonable. However, this does not legitimise any kind of judicial "super legislature". The requirement of judicial self-restraint is to a considerable degree immanent to the test of proportionality. It is not always the case that this is observed as consistently by the courts as it was by the German Constitutional Court during the COVID pandemic. Here, the Court made the following clarification:

> *"When assessing whether a measure is appropriate, too, the legislator in principle has a margin of appreciation [...]. In this respect, the Federal Constitutional Court reviews whether the legislator has taken tenable decisions within its margin of appreciation."*[12]
> (para. 217)

However, the more the judiciary takes the test of proportionality out of the hands of the legislature, the more politicized it becomes.

If every problem had only one proportional solution, the Bundestag would be out of a job by now, after 75 years of vigorous legislation. The fact that this is not the case has one simple reason: the world is in a state of constant change. Not only do some values and convictions change in the course of time but also – and particularly – the political and social framework. This applies above all in "insecure times", when crises and international conflicts render the world in a state of unrest. As a result of this, "there is no 'final word' in a democracy"[13]. With democracy, it is therefore as with communicating vessels: Any change on one side always leads to a change on the other. As a relative principle, proportionality is an inherently unsuitable instrument to develop absolute standards for eternity.

If the threat changes, the proportionality of countermeasures changes accordingly

In terms of security law, a change in the threat situation requires a response by the legislator. It must put the security services in a position that enables them to react adequately to the new threat situation. If a court decision has conducted a proportionality review to a great extent in the place of the legislature, the change in the threat situation can force the court to re-evaluate its assessment. A judgment is always bound to its concrete context and thus limited in its effects, especially when proportionality considerations were at the core of the decision. A different context can and must result in a different decision. This is quite self-evident, and is now perceived with particular clarity in the more decisionistic case law of the ECJ. Such re-evaluations can also be found, however, in the case law of the German Constitutional Court, which is oriented more to-

wards continuity. This is evident in the judgment from 2020 regarding the strategic foreign telecommunications surveillance of the German Federal Intelligence Service (BND): here, the Court on the one hand emphasized the higher intensity of the interference with fundamental rights considering the "disproportionately broader access" compared to its decision from 1999[14], but at the same time, it contrasted it with the "higher potential for danger" that had resulted from the development of communications technology, the tighter cross-border integration of the living conditions in general, and the considerable increase in threats from abroad.[15]

The same principles must apply when it comes to data retention. Since the precedent-setting judgments of the German Constitutional Court in 2010[16] and the ECJ in 2014 (*Digital Rights Ireland*), the security situation in Germany and Europe has changed profoundly. The global political landscape is considerably less stable in the wake of the war in Ukraine and the conflicts in the Middle East, and also due to the impact of climate change and the COVID pandemic. Also domestic security is endangered to a degree that would have been unimaginable only a few years ago. We are being overrun almost daily with cyberattacks and disinformation campaigns by foreign powers, while their espionage and sabotage are meanwhile exceeding Cold War levels. At the same time, global insecurity is fuelling extremist efforts of all kinds, as well as crude conspiracy theories, and anti-democratic propaganda. Unbridled hate and agitation are proliferating, especially on the internet, but also on our streets, where police and rescue services come under attack and are even lured into traps. General acceptance of the fundamental values of a liberal basic democratic order in society is vanishing. The inevitability that liberal democracy could one day mark "the end of history"[17], appears to us today as illusory, even as a

utopia, when we already discuss the question of "How Democracies Die"[18].[19]

The alarming developments in our security situation are calling many certainties from the past into question. This also applies to the idea, inherited from the 1970s, that surveillance inevitably restricts freedom. The dystopian fears for the future that prevailed at that time, which continue to survive to this day in certain circles, are the basis of their fundamental rejection of the temporary retention of IP addresses. I was never convinced by this attitude, since security services that are bound by the rule of law are not a threat but a guarantee of freedom. Today, I consider this self-evident. The "turning point" in the protection of external security announced by the former Chancellor Scholz is equally inevitable in our domestic security policy. This also involves a re-evaluation of traffic data retention. Even after the decisions by the ECJ[20] and Federal Administrative Court[21], I have criticised that the former Federal Minister of Justice is refusing to do his work at the expense of victims of serious crimes like child sexual abuse.[22] After the recent judgment, it is now clear that the compulsory retention of IP addresses would be compatible with Union law, even in the case of far less serious crimes. For which ones exactly remains to be discussed in more detail. The complete failure by the federal legislature is no longer compatible with the protection of victims as demanded by fundamental rights. To protect freedom online, our security services urgently need to be able to access stored IP addresses. The ECJ has correctly recognized this need. Thus, it is not the time to say "Goodbye".

My special thanks go to the staff of the Bavarian State Ministry of the Interior, for Sport and Integration, in particular Ministerialrat Dr. Johannes Unterreitmeier and Oberregierungsrätin Ms. Kathrin Aicher.

References

1. Sabine Leutheusser-Schnarrenberger, 'Goodbye Vorratsdatenspeicherung' (2020) *Verfassungsblog*.
2. Joachim Herrmann, '(Kein) Recht auf Sicherheit im Internet?' in Josef Franz Lindner and Johannes Unterreitmeier (eds.), *Going dark – Signals Intelligence im IT-Zeitalter*, (Mohr Siebeck, 2023), p. 9-10.
3. Lukas Martin Landerer, 'Things That Are Different Are Not the Same' (2024) *Verfassungsblog*.
4. La Quadrature du Net (LQDN), 'Surveillance and Hadopi: EU Court Buries Online Anonymity a Little Further' (30 April 2024), https://www.laquadrature.net/en/2024/04/30/surveillance-and-hadopi-eu-court-buries-online-anonymity-a-little-further/.
5. Markus Reuter, 'EuGH-Urteil zur Vorratsdatenspeicherung: „Traurige Wende beim Schutz der Privatsphäre"' *netzpolitik.org* (30 April 2024), https://netzpolitik.org/2024/eugh-urteil-zur-vorratsdatenspeicherung-traurige-wende-beim-schutz-der-privatsphaere/.
6. German Federal Constitutional Court, *Ökotox-Daten* (2 BvR 206/14), Order of 27 April 2021.
7. Mattias G. Fischer, 'EuGH zur Vorratsdatenspeicherung: Gar nicht zu speichern, ist auch verfassungswidrig' *Frankfurter Allgemeine Zeitung* (28 October 2022), https://www.faz.net/einspruch/eugh-zur-vorratsdatenspeicherung-gar-nicht-zu-speichern-ist-auch-verfassungswidrig-18421290.html.
8. Sofiane Benamor, 'Staatliche Schutzpflichten im Kontext der Vorratsdatenspeicherung' (2022) *Verfassungsblog*.
9. Jan Drebes, 'Ermittler im Glück: Zugriff in Castrop-Rauxel hing offenbar an Speicherfrist für IP-Adresse' *Rheinische Post* (26 January 2023), https://rp-online.de/nrw/panorama/bka-bericht-zugriff-im-fall-castrop-rauxel-hing-an-speicherfrist-fuer-ip-adresse_aid-83718409.
10. Bundestag, 'BT-Drucksache 20/11675' (27 May 2024), p. 33.
11. Bundestag, 'BT-Drucksache 20/11135' (23 April 2024), p. 2.
12. German Federal Constitutional Court, *Bundesnotbremse I* (1 BvR 781/21, 1 BvR 798/21, 1 BvR 805/21, 1 BvR 820/21, 1 BvR 854/21, 1 BvR 860/21, 1 BvR 889/21), Order of 19 November 2021.
13. Oliver Lepsius, 'Kontextualisierung als Aufgabe der Rechtswissenschaft' (2019) 74:17 *JuristenZeitung (JZ)*, p. 801.
14. German Federal Constitutional Court, *Telekommunikationsüberwachung I* (1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95), Judgment of 14 July 1999, para. 220.
15. German Federal Constitutional Court, *Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes* (1 BvR 2835/17), Judgment of 19 May 2020, para. 164.

16. German Federal Constitutional Court, (1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08), Judgment of 2 March 2010.
17. Francis Fukuyama, 'The End of History?' (1989) 16 *The National Interest*.
18. Steven Levitsky and Daniel Ziblatt, *How Democracies Die* (Random House LLC US, 2019).
19. Michael Baurmann, 'Wir haben die Duldung der Demokratie mit ihrer Akzeptanz verwechselt' (2022) *Verfassungsblog*.
20. See CJEU, *SpaceNet AG* (Joined Cases C-793/19 and C-794/19), Judgment of 20 September 2022.
21. German Federal Administrative Court, (6 C 6.22), Judgment of 14 August 2023.
22. Tagesschau, 'Bundesverwaltungsgericht: Anlasslose Vorratsdatenspeicherung ist rechtswidrig' *tagesschau.de* (7 September 2023), https://www.tagesschau.de/inland/gesellschaft/bundesverwaltungsgericht-vorratsdatenspeicherung-rechtswidrig-100.html.

Erik Tuchtfeld

Protecting Victims Without Mass Surveillance

A Response to Joachim Herrmann

Mass data retention is on the rise: on the initiative of Hesse (governed by conservatives and social-democrats), the Bundesrat has called on the Bundestag to introduce a one-month retention period for IP addresses,[1] North Rhine-Westphalia, Schleswig-Holstein and Baden-Württemberg (the coalitions of conservatives and greens in Germany) support a similar initiative,[2] and the (conservative) Bavarian Minister of the Interior, Joachim Herrmann, is also calling for "More protection for victims through data retention"[3]. In the current heyday of security packages in Germany,[4] we are now also seeing a "super grand coalition" in favour of mandatory IP address retention.

Herrmann argues, on behalf of this "coalition of the willing" to store data, that the changes in Germany's and Europe's security are forcing constitutional courts to reconsider the proportionality standards of past decisions and, in particular, to allow the introduction of mass data retention. He paints a dystopian picture of the situation in Germany, a state of hate and violence. What he and his political comrades-in-arms overlook: The investigative capacities of law enforcement authorities have never been better, and the digital data pools that can be analyzed have never been larger.

The never-ending story of mass data retention

Mass data retention to combat internet-related crimes is an evergreen in European security policy. The German Federal Constitutional Court and the European Court of Justice (ECJ) have by now issued (at least) eight different rulings on the permissibility and structure of a preventive obligation to store metadata (such as telephone numbers and times of telephone calls, the connection owner behind an IP address and location data of cell phones, see Article 5

of the Data Retention Directive of 2006 (Directive 2006/24/EC).[5] Herrmann's accusation that "data retention" is a "misleading term" of a certain "political camp" is not very convincing. As the European Directive repealed by the ECJ in 2014 was entitled "Directive [...] on the retention of data [...]", the accusation can basically only be directed self-critically at the (conservative) majority in the Council and Parliament at the time, which adopted the Directive with this name.

Data retention has been the subject of intense political and legal debate for almost two decades now. It was introduced in Germany in 2007,[6] immediately restricted by a temporary injunction from the Federal Constitutional Court,[7] declared unconstitutional in 2010,[8] passed again – in a modified form – by the Bundestag in 2015,[9] declared unlawful under EU law and therefore inapplicable by the OVG Münster in 2017;[10] an assessment that was finally confirmed by the ECJ in *Bundesrepublik Deutschland v SpaceNet AG* (C-793/19) and *Bundesrepublik Deutschland v Telekom Deutschland GmbH* (C-794/19) in 2022. The coalition agreement of the former "traffic light coalition" provided for regulations on data retention to be designed in such a way that they "can be stored in a legally secure manner on a case-by-case basis and by court order".[11] While former (liberal) Minister of Justice Buschmann sees this agreement as a mandate to implement the quick freeze concept (in which metadata is only "frozen" on an ad hoc basis following a criminal offense),[12] the social-democratic Minister of the Interior Faeser – in contradiction to the coalition agreement, but in agreement with the opposition[13] and the Bundesrat – is calling for the introduction of general IP data retention.[14] It shows that the almost 20-year history of data retention in Germany is quite confusing and has been characterized by many agreements, terminations of agreements, judgments and civil society protests.

The problem of anonymity on the internet

Data retention is more controversial than almost any other measure in German domestic policy. The current demands are limited to the introduction of IP data retention. Unlike, for example, the storage of location data, times and participants in telephone calls, this is not about the possibility of retrospectively investigating the life of a known suspect, but about identifying an unknown suspect. Thus, it is primarily a tool for de-anonymization, not for comprehensive profiling. Accordingly, the Federal Constitutional Court already emphasized in its 2010 decision[15] and the ECJ since 2020 in *La Quadrature Du Net I* (C-511/18, C-512/18 and C-520/18; paras. 152-159) that the requirements for IP data retention are lower than for the retention of other metadata.

However, it remains the case, as critics repeatedly emphasize in various places, that the retention of data without reasonable cause puts citizens under general suspicion.[16] From this point of view, anonymity is seen as a danger whose primary function is to provide a cover for crimes. As a result, citizens are generally seen as possible perpetrators who must accept interferences with their fundamental rights in order to be identifiable at the time when the suspicion is realized and a crime is committed. The possibility of identification is not a by-product of other data processing – such as the storage of IP addresses for commercial purposes or maintenance purposes – but the sole purpose of the state's command to store data. This ignores that anonymity – both in virtual as in physical spaces – is a prerequisite for freedom. The mere existence of surveillance increases the pressure to conform and leads to chilling effects for the exercise of freedoms protected by fundamental rights, including stating (supposedly) controversial opinions.

The dependency on context of fundamental rights judgments

Herrmann is right to emphasize that the legal assessment of interferences with fundamental rights depends on the context. For example, new technological developments or alternative investigative procedures could lead to less intrusive, equally effective means to foster a legitimate goal, so that previously permissible interferences with fundamental rights are no longer necessary. In its 2010 decision on data retention, the Federal Constitutional Court also made it clear that the proportionality of an individual surveillance measure must always be assessed in the context of the overall state of state surveillance ("general surveillance account"):

> *"[...] the retention of telecommunications traffic data must not be understood as paving the way for legislation aiming to enable, to the greatest extent possible, the precautionary retention of all data that could potentially be useful for law enforcement or public security purposes. Regardless of how the provisions governing data use were designed, any such legislation would be incompatible with the Constitution from the outset. The retention of telecommunications traffic data without specific grounds will only satisfy constitutional standards if it remains an exception to the rule. It must not be possible to reconstruct practically all activities of citizens even in combination with other existing datasets."*[17] (para. 218)

In order to effectively protect fundamental rights against the possibility to "reconstruct practically all activities of citizens" in today's "Surveillance Capitalism" (Zuboff), a comprehensive analysis of all data collections available to law enforcement authorities

is required. They often complain that the increasing use of encryption technologies makes it more difficult to monitor communication (often referred to as "going dark"[18]). However, in the history of mankind, individuals have never produced as much personal data as they do today. That these data collections, which are held by private companies, are being used for other than their original purposes by law enforcement can be observed intensively in the USA. There, for example, law enforcement authorities have obtained information from Google about which users have used certain search terms or been to certain locations.[19] A striking example of this misappropriation of even the most sensitive data is the well-founded fear that the data stored by female health apps will be accessed in the future to prosecute illegal abortions.[20]

These are all contexts and social conditions that Herrmann seems to overlook. Instead, he emphatically emphasizes that "domestic security is endangered to a degree that would have been unimaginable only a few years ago" and classifies the notion that "surveillance inevitably restricts freedom" as something "inherited from the 1970s". At this point, it should therefore be noted that life in Germany as a whole – despite some problematic developments in recent years – is safer than ever before. In a long-term view, there are fewer homicides,[21] less violence,[22] more rights for women[23] and minorities[24] and less terrorism[25] than in the past. Therefore, labelling the idea of a society free from surveillance as "outdated" by Herrmann is at least not founded in any real-life decrease in security in recent decades in Germany.

IP mass data retention as a panacea

In line with this, Herrmann sketches the image of an internet in which "innumerable dangers" lurk, in which "serious crimes are be-

ing committed relentlessly" and "[u]nbridled hate and agitation are proliferating". This is as (un)true for the internet as it is for physical spaces: where people come together, there is an exchange of knowledge and experience, creativity and inspiration, friendship and solidarity. However, as in any social context, norm violations, including the most serious crimes, are also committed.[26] These must be prevented to a sufficient degree – also due to the state's duty to protect its citizens – and otherwise be sanctioned. However, Herrmann's panorama of cybercrime, from the exchange of child sexual abuse material (CSAM) to ransomware attacks, gives the impression that IP data retention is the only thing standing between a state of rampant violence and lawlessness caused by anonymity on the one hand and a good life in absolute security on the other.

This clearly exceeds the reasonable expectations for IP data retention. Firstly, it is already the case that, in practice, all German telecommunications providers voluntarily store IP addresses for seven days[27] for billing purposes.[28] The Bundesrat's initiative mentioned above also explicitly recognizes this.[29] These seven days are already sufficient to enable the identification of suspects in a good three quarters of all proceedings.[30]

However, there are many reasons why IP addresses often do not bring the desired success: For example, if the identified connection is the operator of a public Wi-Fi hotspot, such as those found in cafés, trains and many other public places, the investigation will come to nothing. Even if a connection is shared in a flat or family, identifying the suspect involves considerable further investigation. IP addresses can also be easily disguised technically, for example by using a virtual private network (VPN) or a proxy. Especially in the field of serious crime, criminals also often use the so-called "Darknet" (it should be noted at this point, however, that the use of the Darknet is essential for human rights activists in authoritarian

regimes). This refers to a part of the internet that is not accessible via conventional browsers, but via the Tor network with the Tor Browser. This network consists of several layers (Tor is an abbreviation for "The Onion Routing") that ensure encrypted and anonymous communication. Contrary to what Herrmann claims, IP addresses are in this context not "the only indicators for investigation activities by the security services"[31], but are useless because they are always obfuscated.

Instead, it is more promising – and in line with the state's duty to protect – to develop targeted solutions for particular criminal phenomena. One promising investigative starting point is the user account, which is used to contact victims and is, thus, a prerequisite for the commission of the crimes. Such an account can provide a variety of clues that can be analyzed by Open Source Intelligence (OSINT) or Social Media Intelligence (SOCMINT) investigations. The ECJ also recognizes this (*La Quadrature du Net II,* C-470/21; paras. 120-121), but emphasizes the particular intensity of the interference of such comprehensive investigations for the person concerned, as further information about their private life is obtained. However, it does not seem to take into account that these interferences are limited to a specific suspect and therefore have significantly less broad effects than the mass retention of the data of all citizens.

User accounts as an investigative approach for serious crime

As the accounts are often used repeatedly, the preventive storage of IP addresses is not necessary in order to use them for investigative purposes. Instead, it would be sufficient to forward the IP address of the user account the next time the account is used after a suspi-

cion of a crime has been confirmed and then immediately resolve it in order to identify the individual behind the IP.[32]

Such an approach is promising even in cases of serious crime, such as the dissemination of CSAM. A large number of these cases only become known due to reports from the US-based NGO NCMEC, which cooperates with social platforms and cloud services that systematically filter the content uploaded to them – both public or private material – for CSAM. Law enforcement authorities emphasize that in these cases, the "IP address is the best investigative approach to identify the perpetrators, in some cases even the only one"[33]. However, all of these constellations involve suspects who have created a user account on the respective service. The recurring use of the account means that the respective company repeatedly obtains knowledge of the user's current IP address – on every single interaction. In these cases, the current IP address can be passed on to the law enforcement authorities (after judicial authorization), and can then be resolved in real time by the telecommunications providers. Consequently, there is no need to store the IP addresses of persons without any connection to a crime.

The same applies to cases of grooming, in which adults approach children and youth with the objective of sexual abuse. This happens mainly on social platforms that are attractive to minors. It is therefore necessary for the perpetrators to have a user account in order to make and maintain contact with the minors. The perpetrators' aim of establishing a basis of trust with them and possibly even creating a relationship of dependency is only possible through the recurring use of the account.

The reasonability of interferences with fundamental rights

Herrmann is right to emphasize that it is primarily the task of policy-makers to balance and reconcile conflicting fundamental rights. To this end, different parties and governing majorities propose different solutions that are in democratic competition with each other. The frame of this democratic competition is defined by the constitution. There is no "primacy of politics" over the law as claimed by Herrmann, but rather an obligation of the legislation to observe the "constitutional order" and fundamental rights "as directly applicable law" (Articles 1 para. 3; 20 para. 3 German Constitution).[34] This limitation of public power by law characterizes the rule of law. It is dangerous to suggest that the judicial prohibition of a certain surveillance measure is tantamount to elevating the judiciary to a "super legislature" in which there is only room for "one proportionate solution". Judgments considering one's own political plans as a violation of fundamental rights may be painful,[35] but should rather encourage a self-critical reflection of the respective political positions than harsh criticism of the courts.

It is still up for debate whether and how IP data retention fits into the political margin defined by the ECJ. In *La Quadrature Du Net II* (C-470/21), the ECJ found that the retention of IP addresses "does not constitute a serious interference". However, the apodictic statement in the judgment that without IP data retention there would be "real risk of systemic impunity" (para. 119) fails to recognize, in my opinion, how extensive the investigative capacities of law enforcement authorities with their access to private data collections already are. The assessment that the retention of additional data benefits the protection of fundamental rights compared to other investigative measures is not very convincing to say the

least (see, however, paras. 120-121). Furthermore, as shown above, the widespread use of user accounts in the commission of criminal offenses due to the architecture of today's internet offers opportunities to identify suspects via their IP address even without preventive data retention.

Moreover, it would be a mistake to interpret the ruling as a blank cheque for IP data retention. The qualification of the interference as not being serious requires "a set of requirements intended to ensure, in essence, a genuinely watertight separation of the different categories of data retained, such that the combination of data belonging to different categories is genuinely ruled out" (para. 103). These high technical requirements for data retention, in particular the "watertight separation" of different data categories to avoid detailed profiles, have led to industry associations from Germany stating publicly that they are in fact no longer allowed to store data and must discontinue the current voluntary retention of IP addresses.[36] It remains unclear how these requirements can be implemented in practice. Therefore, the introduction of laws mandating IP data retention is still associated with a high degree of legal uncertainty. The only thing that seems certain after April 30, 2024 is that data retention will continue to occupy courts throughout Europe.

A Zeitenwende in security policy

People in Germany have a right to be protected by the state. The security policy of recent decades has often sailed on the edge of being unconstitutional – and sometimes even beyond it.[37] Such a policy does not make the country safer. Rather, it leads to unjustified interferences with fundamental rights and legal uncertainty. A lot of time and energy is lost in legislative processes, the product of

which is declared null and void by the highest courts years later. This does not help the victims of violence.

German security policy needs a *Zeitenwende*. Law enforcement authorities should work together with victims of crimes and civil society organization in an open process to develop targeted measures to enhance criminal prosecution without expanding mass surveillance and dismantling legal protection. Only recently, Höffler clearly explained why the best security policy is a social policy that addresses the structural causes of exclusion and violence and, thus, makes the country safer for everyone.[38]

I agree with Herrmann that our democracy is in danger. Freedoms that were long thought to be safe are once again being called into question. The growing right-wing extremism in this country is a danger to our democracy. It is therefore important that our democratic and constitutional institutions are strengthened.[39] This includes, in particular, the separation of powers and effective judicial review mechanisms. We must not allow ourselves to be intimidated by the enemies of freedom, but instead counter them with more openness and more democracy.[40]

References

1. Bundesrat, 'Bundesrat KOMPAKT: Ausgewählte Tagesordnungspunkte der 1047. Sitzung' (27 September 2024), https://www.bundesrat.de/DE/plenum/bundesrat-kompakt/24/1047/13.html.
2. Ministerium der Justiz des Landes Nordrhein-Westfalen, 'Stärkung der Terrorismusbekämpfung und Verbesserungen in der Migrationspolitik: Umsetzung des Maßnahmenpakets zu Sicherheit, Migration, Prävention' (24 September 2024), https://www.justiz.nrw.de/presse/2024-09-24.
3. See the contribution by Joachim Herrmann in this book.
4. Clemens Arzt, 'Die Woche der Sicherheitspakete' (2024) *Verfassungsblog*.
5. See the cases CJEU, *Digital Rights Ireland* (C-293/12 and C-594/12); *Tele2 Sverige and Watson* (C-203/15 and C-698/15); *La Quadrature du Net I* (C-511/18, C-512/18 and C-520/18) and *G.D. v The Commissioner of An Garda Síochána* (C-140/20). See German Federal Constitutional Court, (1 BvR 256/08, 1 BvR 263/08 and 1 BvR 586/08), Judgment of 2 March 2010; (1 BvR 2683/16), Order of 14 February 2023; (1 BvR 2845/16), Order of 14 February 2023; (1 BvR 141/16), Order of 15 February 2023.
6. Dominik Reinle, 'Bundestag beschließt Gesetz zur Vorratsdatenspeicherung' *Westdeutscher Rundfunk* (9 November 2017), https://www1.wdr.de/stichtag/stichtag-bundestag-gesetz-vorratsdatenspeicherung-100.html.
7. German Federal Constitutional Court, (1 BvR 256/08), Order of 11 March 2008.
8. German Federal Constitutional Court, (1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08), Judgment of 2 March 2010.
9. Bundestag, 'Bundestag beschließt neue Vorratsdatenspeicherung' *Archiv Deutscher Bundestag* (16 October 2015), https://www.bundestag.de/webarchiv/textarchiv/2015/kw42_de_vorratsdatenspeicherung-391654.
10. LTO-Redaktion, 'OVG: Vorratsdatenspeicherung verstößt gegen EU-Recht' *Legal Tribune Online* (22 June 2017), https://www.lto.de/recht/nachrichten/n/ovg-nrw-beschluss-13b23817-vorratsdatenspeicherung-telekommunikationsgesetz-verstoss-eu-recht-pauschale-datenspeicherung.
11. Sozialdemokratische Partei Deutschlands (SPD), Bündnis 90/Die Grünen, and Freie Demokratische Partei (FDP), 'Koalitionsvertrag 2021-2025' (24 November 2021), https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf#page=87.
12. Markus Sehl, '"Quick-Freeze"-Vorschlag vom Justizminister' *Legal Tribune Online* (25 October 2022), https://www.lto.de/recht/hintergruende/h/vorratsdatenspeicherung-ueberwachung-bmi-bmj-gesetzentwurf-nach-eugh-urteil.

13. Bundestag, 'Antrag zur IP-Adressen-Speicherung zum Schutz vor Kindesmissbrauch abgelehnt' (18 January 2024), https://www.bundestag.de/dokumente/textarchiv/2024/kw03-de-sexueller-missbrauch-983232.

14. Falk Steiner, 'Faeser fordert nach EuGH-Urteil Vorratsdatenspeicherung' *heise online* (2 May 2024), https://www.heise.de/news/Faeser-fordert-nach-EuGH-Urteil-Vorratsdatenspeicherung-9706221.html.

15. German Federal Constitutional Court, (1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08), Judgment of 2 March 2010, paras. 254-263.

16. Antje Draheim and Harald Baumann-Hasske, 'EuGH: Keine anlasslose Vorratsdatenspeicherung!' *SPD* (21 September 2022), https://www.spd.de/service/pressemitteilungen/detail/news/eugh-keineanlasslose-vorratsdatenspeicherung/21/09/2022; Christian Rath, 'Vorratsdatenspeicherung: Generalverdacht im Netz' *Die Tageszeitung: taz* (15 May 2023), https://taz.de/Vorratsdatenspeicherung/!5931713/; Bundesministerium der Justiz, 'Wir dürfen die Bürger nicht unter Generalverdacht stellen' (15 September 2023), https://www.bmj.de/SharedDocs/Meldungen/DE/2023/0915_Webde.html; Bündnis 90/Die Grünen, 'Unsere Ziele: Digitales' (1 September 2024), https://www.gruene-bundestag.de/unsere-politik/unsere-ziele/digitales/.

17. German Federal Constitutional Court, (1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08), Judgment of 2 March 2010.

18. Tomas Rudl, 'Going Dark: Zivilgesellschaft gibt Kontra' *netzpolitik.org* (21 February 2024), https://netzpolitik.org/2024/going-dark-zivilgesellschaft-gibt-kontra/.

19. Albert Fox Cahn and Amanda Humell, '"Keyword Warrants" Make Every Search A Risk: A Disturbing New Police Tactic Harnesses the Full Tracking Power of "Big Tech"' (2020) *Verfassungsblog*.

20. Carly Page, 'Supreme Court Overturns *Roe v. Wade*: Should You Delete Your Period-Tracking App?' *TechCrunch* (5 May 2022), https://techcrunch.com/2022/05/05/roe-wade-privacy-period-tracking/.

21. United Nations Office on Drugs and Crime, 'Homicide Rate (1990-2022)' *Our World In Data* (30 October 2024), https://ourworldindata.org/grapher/homicide-rate-unodc?tab=chart&country=~DEU.

22. Beate Lakotta, 'Wie sicher ist Deutschland? Daten zur Gewaltkriminalität' *Der Spiegel* (6 May 2018), https://www.spiegel.de/spiegel/gewaltkriminalitaet-wie-sicher-ist-deutschland-a-1206327.html.

23. Jugendnetzwerk Konz e.V., 'Die 15 wichtigsten Meilensteine' https://hundertjahrefrauenwahlrecht.de/meilensteine/.

24. Ulrike Bosse, 'Unter der Regenbogenfahne – Die Anfänge der Schwulenbewegung' *Norddeutscher Rundfunk* (11 January 2023), https://www.ndr.de/geschichte/chronologie/Unter-der-Regenbogenfahne-Die-Anfaenge-der-Schwulenbewegung,schwulenbewegung100.html.

25. Global Terrorism Database, 'Number of Terrorist Attacks (1990-2021)' *Our World In Data* (20 July 2023), https://ourworldindata.org/grapher/terrorist-attacks?tab=chart&country=~DEU.

26. See Philipp Lorenz-Spreen, Lisa Oswald, Stephan Lewandowsky and Ralph Hertwig, 'A Systematic Review of Worldwide Causal and Correlational Evidence on Digital Media and Democracy' (2023) 7 *Nature Human Behaviour* for the complex state of research on the effects of social platforms on democracy.

27. The data for Freenet is somewhat misleading. Freenet is a pure reseller, i.e. it uses the networks of other telecommunications providers, where storage takes place accordingly.

28. Bundeskriminalamt, 'Positionspapier des BKA zu erforderlichen Speicherfristen von IP-Adressen' (21 July 2023), https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/230623_Mindestspeicherfristen_IP-Adressen.html.

29. Bundesrat, 'Drucksache 180/24', (27 September 2024), p. 4 E.2.

30. Bundeskriminalamt, 'Positionspapier des BKA zu erforderlichen Speicherfristen von IP-Adressen' (21 July 2023), https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/230623_Mindestspeicherfristen_IP-Adressen.html.

31. Sabine Vogt, 'Das Darknet: Rauschgift, Waffen, Falschgeld, Ausweise – das digitale „Kaufhaus" der Kriminellen?' (2017) 2 *Die Kriminalpolizei*.

32. D64 Zentrum für Digitalen Fortschritt e.V., 'Die Login-Falle: Strafverfolgung im Internet ohne Massenüberwachung' (14 June 2021), https://d-64.org/login-falle/.

33. Bundeskriminalamt, 'Vorratsdatenspeicherung: Fragen & Antworten' (2023).

34. Till Patrik Holterhus, 'Die Idee der Rechtsstaatlichkeit' (2022) 351/2022 *bpb: Informationen zur politischen Bildung*.

35. German Federal Constitutional Court, *Bayerisches Verfassungsschutzgesetz* (1 BvR 1619/17), Judgment of 26 April 2022 and Irene Esmann, 'Urteil zu Analyse-Software der Polizei: Folgen für Bayern?' *Bayrischer Rundfunk* (16 February 2023), https://www.br.de/nachrichten/deutschland-welt/karlsruhe-beanstandet-regelungen-zu-datenanalyse-bei-der-polizei,TW0Wy8E.

36. Friedhelm Greis, 'EuGH-Urteil zu IP-Adressen: Wie die Provider künftig Vorratsdaten speichern dürfen' *Golem* (8 May 2024), https://www.golem.de/sonstiges/zustimmung/auswahl.html?from=https%3A%2F%2Fwww.golem.de%2Fnews%2Feugh-urteil-zu-ip-adressen-wie-die-provider-kuenftig-vorratsdaten-speichern-duerfen-2405-184919.html.

37. Mark A. Zöller, 'Und (fast) täglich grüßt das Murmeltier: BKA-Produkttest von Gesichtserkennungssoftware offenbart verfassungsrechtliche Fehlverständnisse' (2024) *Verfassungsblog*.

38. Katrin Höffler, 'Solingen 93/24: Menschenrechte als bestes Präventionskonzept' (2024) *Verfassungsblog*.

39. Verfassungsblog, 'Das Thüringen-Projekt' https://verfassungsblog.de/thuringen-projekt/.

40. Helen Pidd and James Meikle, 'Norway Will Not Be Intimidated by Terror Attacks, Vows Prime Minister' *The Guardian* (27 July 2011), https://www.theguardian.com/world/2011/jul/27/norway-terror-attacks-prime-minister.

Lukas Martin Landerer

Data Retention

Between Fundamental Rights and Integration

The most vocally debated and legally intensively examined instrument of mass surveillance is the obligation of telecommunication services providers to retain metadata (such as traffic and location data or IP addresses) of all their users without them being in any way connected to a crime. The central protagonist in this saga of "mass data retention" is the Court of Justice of the European Union (CJEU). In its *Digital Rights Ireland* (C-293/12 and C-594/12) ruling of 2014, the CJEU declared the European Data Retention Directive (Directive 2006/24/EC) (DRD), which universally obliged providers to retain their customer's traffic data, as incompatible with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (EU-CFR). Since then, the CJEU has granted Member States increasingly broad leeway in a series of rulings. Most recently, the Court ruled in *La Quadrature Du Net II* (C-470/21) that the retention of IP addresses is permissible to combat "general criminal offenses".

This development has drawn criticism of the CJEU. Some argue that the Court has taken "one step forward and two steps back"[1]. First, the Court wanted to establish itself as a highly fundamental rights sensible institution in *Digital Rights Ireland*. Then, in a "Copernican revolution"[2], it revised its liberal stance. While I do not want to dismiss this criticism completely, I believe that one should not regard the court's shift as yielding to the political pressure from the Member States. Rather, it is the logical consequence of the expanding European competence on (constitutional) security law. Security law, in this context, refers to the law focusing on the procedures and investigation measures of law enforcement agencies and intelligence services. This traditionally nationally regulated legal field has become increasingly complex. Nowadays, constitutional courts do not strictly prohibit security measures, such as mass surveillance measures, but "proceduralize"[3] them.

The CJEU as both an "engine of integration" and fundamental rights institution?

If one had conducted a survey among lawyers and (other) social scientists in the early 2010s about what guides the CJEU in its decisions, the majority would likely have invoked the image of the "engine of integration"[4]. This phrase was often used – somewhat critically – to suggest that the CJEU tended to interpret European law more expansively than one could have expected by an objective instance. And as the Member States would have appreciated.

With the 2014 *Digital Rights Ireland* ruling, the CJEU assumed a new role, according to many observers. Unlike the German Federal Constitutional Court (BVerfG) four years earlier,[5] the Court ruled that the obligation of private telecommunications providers to retain traffic data universally for six months and to hand it over to state security authorities was disproportionate. This Decision was warmly welcomed in Germany, especially by politicians from the German-speaking world (such as former Justice Minister Sabine Leutheusser-Schnarrenberger[6] and former Pirate Party member Patrick Breyer[7]), who had sharply criticized the data retention obligation for its infringement on telecommunications privacy. According to prevailing opinion, the CJEU had established itself as a "fundamental rights institution"[8] with the Decision. Some even called it a "turning point in European fundamental rights protection"[9].

The ban on data retention and its exceptions

Consequently, the reactions in the German-speaking discourse to the subsequent CJEU rulings on data retention were rather

negative,[10] as these rulings gradually expanded the possibilities for national legislators to introduce data retention regulations.

In *Digital Rights Ireland*, the CJEU had already hinted at the permissibility of a limited data retention obligation. The main condition, according to the Court, was whether the stored data could potentially be used for crime prevention (para. 59). This opened up some flexibility for Member States, which then introduced national data retention laws.

The CJEU first clarified the requirements for proportional data retention in its ruling on the UK's and Sweden's data retention laws (*Tele2 Sverige & Privacy International* (Joined Cases C-203/15 and C-698/15) in 2016). Later, while reviewing the regulations in France, Belgium and Germany (*La Quadrature Du Net I* (C-511/18, C-512/18 and C-520/18) (2020), *SpaceNet* (C-793/19) (2022) and *La Quadrature du Net II* (2024)), it progressively expanded the leeway available to Member States.

Some critics had believed that data retention was "stone dead"[11] after *Tele2 Sverige* because the boundaries set by the CJEU were extremely narrow. This interpretation, however, did not hold: data retention is today as alive as ever.

Since *La Quadrature du Net I*, the CJEU has allowed the universal retention of IP-addresses (yet initially only to combat serious criminal offenses). It has also allowed the retention of traffic data under two exceptions. These are:

1. The universal retention of traffic data on a states' territory for short periods, when the Member State is facing a serious, real, and ongoing or foreseeable threat to national security.
2. A "targeted data retention" in specific, particularly crime-prone areas, even without a national security threat.

Member States have creatively exploited these exceptions. France continues to implement a general data retention obligation nationwide,[12] arguing that the national security threat required by the CJEU is continually present. It imposes a (short-term) data retention obligation on a rotating basis. The French Constitutional Court has essentially approved this practice.[13] It was under significant pressure, since the French government threatened to pursue an *ultra vires* review, if the court decided otherwise.[14]

Belgium bases its national data retention on the "targeted retention" exception. The specific, crime-affected area where the data retention applies (without a national security threat) has, however, the same borders as the Belgian state territory.[15]

The CJEU seems to have underestimated the resistance of some Member States to the ban on data retention. It was probably unaware of how differently security authorities use this instrument. French law enforcement agencies, for example, work much more intensively with traffic data than their German counterparts. According to a survey, French security authorities requested traffic data in over 80% of investigations in 2018-2019.[16] Thus, a data retention ban would particularly affect France.

Security law between integration and fundamental rights

According to Article 4 (2) of the Treaty on the Functioning of the European Union (TFEU), national security remains the sole responsibility of the Member States. The EU only has competence in criminal matters that typically have a cross-border nature. This competence however, primarily concerns the harmonisation of the definitions of criminal offence, not the national law enforcement authorities' investigation measures. Consequently, some argued after the annulment of the DRD that the EU-CFR could no longer

apply to national obligations since there was no EU law requiring data retention anymore.[17]

The competence of the EU institutions over security law arises from the fact that security law today is primarily information law. European institutions use this vehicle to influence national investigative measures.

The CJEU based its authority in *Tele2 Sverige* (paras. 73 ff.) on Article 15 (1) of the ePrivacy Directive (Directive 2002/58/EC). This provision states that the retention of telecommunications traffic data is generally prohibited unless it is necessary and appropriate for national or public security. The impact of this rule on national data retention regimes was questioned, as the ePrivacy Directive does not apply to measures in the area of public security according to Article 1 (3). However, the CJEU argued that Article 15 (1) had no use unless it regulated national data retention regimes. Thereby, it established its competence over the issue. Some have argued that the Union lacks the competence to establish such a fundamental ban for national regulations in the field of security law in the first place.[18] However, the CJEU had already commented on this issue of competence before:

The Commission has consistently argued that the data is not retained by state authorities, but by private companies. Therefore, it can rely on its competence to harmonize the internal market (Article 114 (1) TFEU). In its decision C-317/04 and C-318/04 on the passenger data agreement with the United States in 2006, the CJEU initially rejected the Commission's argument. The data transfer would obviously concern public security and state activities in criminal matters (paras. 57 and 54 ff.). Therefore, it was clear that the agreement did not mean to harmonize the internal market. However, in later decisions on the retention of telecommunications traffic data, the CJEU accepted the Commission's view.[19]

This explains why the CJEU considers Article 15 (1) of the ePrivacy Directive to be a legal basis for a legitimate EU limitation on national data retention regimes. The Commission and the CJEU have expanded the scope of EU law factually to a broad range of security authorities' measures by treating the obligation of private entities to process data in this regard as a matter of market harmonisation. By doing so, the CJEU has put itself in a difficult position. It must harmonize procedures of national security authorities, although it is not originally competent for national security law.

"Proceduralized" security law

The CJEU had to find a way out of this situation. It appears to have aligned its case law to the jurisprudence of the Federal Constitutional Court of Germany (FCC).

Rather than declaring specific security measures as disproportionate, as the CJEU attempted in *Digital Rights Ireland*, the FCC derives specific thresholds and other requirements for surveillance and other security measures from the principle of proportionality. It has developed a broad catalogue of characteristics to define the intensity of any investigation measure. Based on this, the FCC classifies measures on a scale ranging from "insignificant" to "very intense" using a firmly established case-by-case model. The entire system is so complex that it is referred to as an independent "constitutional security law"[20], which no longer has much in common with a proportionality test in the sense of a rationality review.[21] Indeed, some have criticized recent decisions (e.g., the latest on the BKA-Act[22]) as overstepping judicial boundaries by writing "guidelines" for legislation.[23]

The resemblance of the FCC's approach in recent rulings of the CJEU is clear. Thus, I do not regard the recent data retention rulings as signs of a growing authoritarian or "illiberal" jurisprudence. Rather, they are an advancement in terms of complexity and differentiation.[24] The Court has adopted a systematic approach, categorizing security law measures – much like the FCC – according to intensity levels and constituted specific conditions and thresholds for the legal basis of any security measure depending on its intensity.[25] The black or white thinking, which considers mass surveillance and other investigative measures generally as either proportionate or disproportionate, is outdated. Instead, these measures are "proceduralized"[26].

The changing role of the fundamental rights institution

Therefore, one should not accuse the CJEU of abandoning its role as a sensible "fundamental rights institution". Rather, the CJEU has adopted the approach of other courts in the area of (constitutional) security law. As a European court, the CJEU cannot simply ban certain police measures, but must respect the complexity and heterogeneity of national law enforcement agencies. Expanding the Court's competence to prescribe rules concerning national security law would otherwise have led to significant conflicts with the Member States, as evidenced by the French government's open threat of an *ultra vires*-review.[27]

The CJEU's case law therefore does not reflect a shift towards a more fundamental rights-hostile interpretation of the law, but rather rests on the fact that the CJEU had to keep pace with developments in fundamental rights jurisprudence – at least in the area of security law.

References

1. Maria Tzanou and Spyridoula Karyda, '*Privacy International* and *Quadrature du Net*: One Step Forward Two Steps Back in the Data Retention Saga?' (2022) 28:1 *European Public Law*.
2. Philipp Hacker, 'EuGH erlaubt mehr Möglichkeiten zur Vorratsdatenspeicherung' *Science Media Center Germany* (3 May 2024), https://sciencemediacenter.de/angebote/eugh-erlaubt-mehr-moeglichkeiten-zur-vorratsdatenspeicherung-24069.
3. Maria Tzanou and Spyridoula Karyda, '*Privacy International* and *Quadrature du Net*: One Step Forward Two Steps Back in the Data Retention Saga?' (2022) 28:1 *European Public Law*.
4. Mark A. Pollack, 'The Engines of Integration? Supranational Autonomy and Influence in the European Union' *Conference Paper (Fifth Biennial International Conference of the European Communities Studies Association)* (29 May 1997), http://aei.pitt.edu/id/eprint/2706.
5. German Federal Constitutional Court, (1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08), Judgment of 2 March 2010.
6. Interview mit Sabine Leutheusser-Schnarrenberger, '"Der Speicherwahn führt in den Überwachungsstaat"' *Der Spiegel* (16 November 2007), https://www.spiegel.de/netzwelt/web/leutheusser-schnarrenberger-der-speicherwahn-fuehrt-in-den-ueberwachungsstaat-a-517575.html.
7. Patrick Breyer, *Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland* (Rhombos-Verlag, 2005).
8. Allan Rosas, 'The Court of Justice of the European Union: A Human Rights Institution?' (2022) 14:1 *Journal of Human Rights Practice*.
9. Heribert Prantl, 'Ende der Maßlosigkeit' *Süddeutsche Zeitung* (8 April 2014), https://www.sueddeutsche.de/politik/urteil-zur-vorratsdatenspeicherung-ende-der-masslosigkeit-1.1932057.
10. Aqilah Sandhu, 'Die *Tele2*-Entscheidung des EuGH zur Vorratsdatenspeicherung in den Mitgliedstaaten und ihre Auswirkungen auf die Rechtslage in Deutschland und in der Europäischen Union' (2017) 52:3 *Europarecht – EuR*.
11. Nikolaus Marsch, 'Do(n't) Think Twice, It's All Right: der EuGH beerdigt die Vorratsdatenspeicherung' (2016) *Verfassungsblog*.
12. Journal Officiel de la République Française, 'Décret No. 2022-1327', 17 October 2022.
13. La Quadrature du Net (LQDN), 'Le Conseil d'État valide durablement la surveillance de masse' (21 April 2021), https://www.laquadrature.net/2021/04/21/le-conseil-detat-valide-durablement-la-surveillance-de-masse/.

14. Laura Kayali, 'France Seeks to Bypass EU Top Court on Data Retention' *Politico* (3 March 2021), https://www.politico.eu/article/france-data-retention-bypass-eu-top-court/.
15. Patrick Breyer, '"Gezielte" Vorratsdatenspeicherung in Belgien: was unsere Karte zeigt' (8 June 2022), https://www.patrick-breyer.de/gezielte-vorratsdatenspeicherung-in-belgien-was-unsere-karte-zeigt/.
16. European Commission, DG for Migration and Home Affairs, *Study on the Retention of Electronic Communications Non-Content Data for Law Enforcement Purposes* (Publications Office of the European Union, 2020).
17. England and Wales Court of Appeal, *Secretary of State for the Home Department v Tom Watson MP and Others* (C1/2015/2612), Judgment of 20 November 2015, paras. 72 ff.
18. Ferdinand Wollenschläger and Lukas Krönke, 'Telekommunikationsüberwachung und Verkehrsdatenspeicherung – eine Frage des EU-Grundrechtsschutzes?' (2016) 69:13 *Neue Juristische Wochenschau*.
19. Cf. critical remarks by Kai Ambos, 'Anmerkung' (2009) 64:9 *JuristenZeitung (JZ)*.
20. Steffen Tanneberger, *Die Sicherheitsverfassung: Eine systematische Darstellung der Rechtsprechung des Bundesverfassungsgerichts. Zugleich ein Beitrag zu einer induktiven Methodenlehre* (Mohr Siebeck, 2014).
21. Ralf Poscher, '§ 3: Das Grundgesetz als Verfassung des verhältnismäßigen Ausgleichs' in Matthias Herdegen, Johannes Masing, Ralf Poscher, and Klaus Ferdinand Gärditz (eds.), *Handbuch des Verfassungsrechts: Darstellung in transnationaler Perspektive*, (C.H. Beck, 2021).
22. German Federal Constitutional Court, *Bundeskriminalamtgesetz II* (1 BvR 1160/19), Judgment of 1 October 2024.
23. Cf. the Dissenting Opinion of Judge Schluckebier in German Federal Constitutional Court, (1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08), Judgment of 2 March 2010, para. 326.
24. Cf. Sarah Eskens, 'The Ever-Growing Complexity of the Data Retention Discussion in the EU: An In-Depth Review of *La Quadrature du Net and others* and *Privacy International*' (2022) 8:1 *European Data Protection Law Review*.
25. See this overview: Elspeth Guild, Elif Kuskonmaz, Valsamis Mitsilegas, and Niovi Vavoula, 'Data Retention and the Future of Large-Scale Surveillance: The Evolution and Contestation of Judicial Benchmarks' (2021) No. 372/2021 *Queen Mary Law Research Paper* .
26. Maria Tzanou and Spyridoula Karyda, '*Privacy International* and *Quadrature du Net*: One Step Forward Two Steps Back in the Data Retention Saga?' (2022) 28:1 *European Public Law*.
27. Laura Kayali, 'France Seeks to Bypass EU Top Court on Data Retention' *Politico* (3 March 2021), https://www.politico.eu/article/france-data-retention-bypass-eu-top-court/.

Aqilah Sandhu

Squaring the Circle

The CJEU between Fundamental Rights Guardian and Architect of a Security Union

Rarely is the name of a decision so emblematic of the problem that lies behind it. The association La Quadrature du Net has reached yet another landmark judgment on data retention before the Court of Justice of the European Union (CJEU). However, the decision seems like squaring the circle for opponents and proponents of mass surveillance alike. For decades, national law enforcement authorities and interior ministries have complained about a constant lack of investigative capacity for combating online crime. The CJEU is caught between its duty to ensure uniform application of EU law and its claim to have the final say in resolving conflicts affecting fundamental rights. As a matter of fact, the data retention saga is at the core of the judicial dialogue between the EU Court and the national constitutional courts.[1] This contribution aims at contextualizing the *La Quadrature du Net II*-judgment (C-470/21) of 30th April 2024 and questions the flawed methodological approach of the CJEU. Instead of conjuring up a worrisome paradigm shift, the judgment should rather be seen as a wakeup call for the EU legislator, who for decades has failed to establish clear and unambiguous limits for data retention.

Steady retreat

Ever since the *Digital Rights Ireland*-judgment in 2014 (C-293/12 and C-594/12), the CJEU has slowly been watering down its own jurisprudence. In *Tele2 Sverige* (C-203/15) in 2016, it declared "targeted retention of traffic and location data" to be permissible, if it was strictly limited "with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted" for the purpose of fighting serious crime (para. 108). In *La Quadrature du Net I* (C-511/18, C-512/18 and C-520/18) in 2020 the CJEU declared that the object-

ive of safeguarding national security justified the "preventive retention of data of all users of electronic communications systems" if it was limited to a foreseeable period of time (paras. 137 f.). Also, the Court paved the way for the general and indiscriminate data retention of IP addresses as they might be the only means to investigate offences committed online. This possibility was however limited to cases of combating serious crime, preventing serious threats to public security and safeguarding of national security. The retention of IP addresses has since been subject to fewer restrictions than the retention of traffic and location data.

In 2022, upon request for a preliminary ruling by the German Federal Administrative Court (*SpaceNet* (C-793/19 and C-794/19)) and the Supreme Court of Ireland (*Commissioner of An Garda Síochána* (C-140/20)), the CJEU affirmed these limitations, allowing the generalised retention of IP addresses to combat serious crime (para. 102). With the recent *La Quadrature du Net II*-judgment, the Full Court extended this exception to lesser crimes, such as combating infringements of intellectual property rights committed exclusively online. It is important to note that the general and indiscriminate retention of IP addresses in this case was not necessarily considered to constitute "a serious interference" (paras. 78 ff.) with Articles 7, 8 and 11 of the Charter. Given the specific provisions and safeguards in French law, the Court was convinced that the possibility that retention could give rise to serious interferences in the private life of the person concerned could be "genuinely ruled out".

Competence creep vis-à-vis the Member States

Leading court cases do not automatically create universally binding precedents and instead require contextualization, also in the con-

tinental legal system which is primarily based on statutory law.[2] It is the task of legal academia to assess the complex factual context of a decision, the hermeneutics applied by the court as well as the procedural history behind a case. In EU law in particular, the interpretation of the law is increasingly being replaced by the interpretation of court decisions.[3]

The CJEU's preliminary rulings must be interpreted in the light of the questions referred as well as the societal conditions[4] in and the legislative framework of the referring Member State. Given the specific legal framework governing the administrative procedure of Hadopi, an independent public authority tasked with combating copyright infringements committed online, the CJEU was convinced in the recent *La Quadrature du Net II*-judgment that data retention was organised in such a way that the "genuinely watertight separation" of the different categories of data was guaranteed from a technical point of view as well. Bearing this in mind, it is noteworthy that *La Quadrature du Net II* was referred to the CJEU by the French Conseil d'État, the highest administrative court in France – the very same court that back in 2021[5] was asked by the French Government to declare *La Quadrature du Net I* to be an act *ultra vires* as it encroached upon France's national security and undermined its constitutional identity.

The Conseil rejected this claim, thereby refraining from waging "open war"[6] against the CJEU and instead opted for what the Conseil's former vice president called a rough dialogue (*le "dialogue rugueux"*[7]) with the CJEU. Needless to say, the Conseil considered the CJEU to be incapable of guaranteeing adequate protection on the basis that the safeguarding of national security falls exclusively within the competence of the Member States. And, establishing a "securitarian *Solange*"[8] doctrine, the Conseil considered the indiscriminate and general retention of

electronic communication data for a period of one year to be indispensable for the combat of serious crimes and the protection of national security.[9]

Against this backdrop, *La Quadrature du Net II* is neither a "major U-turn in EU case law"[10] nor "the end of online anonymity"[11]. Instead, the judgment is just yet another chapter in the constitutional dialogue between the European courts – it is more a tactical concession to French particularities, a strategy of appeasement, than a really serious departure from the high standards of protection of fundamental rights, as established in the Court's previous case law.

Methodological flaws

When the Court (rightly) annulled the EU Data Retention Directive (Directive 2006/24/EC) in *Digital Rights Ireland* in 2014, it did so primarily because instead of limiting itself to what is strictly necessary, the Directive interfered "with the fundamental rights of practically the entire European population" (para. 56). The CJEU found that the Directive lacked clear and precise rules for limiting the scope and application of data retention measures, giving rise to the possibility of severe interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter.

Ever since the annulment, the CJEU has measured the various data retention laws, mainly enacted by the Member States to implement the Data Retention Directive, against the yardstick of a mere opening clause in the ePrivacy-Directive (Directive 2002/58/EC) read in the light of Articles 7, 8 and 11 of the Charter. Its case law is carved out from Article 15 of the ePrivacy Directive, a "vague and vast disciple", as rightly pointed out by Giulia Formici in this book, because it allows Member States to derogate from the

principle of confidentiality of the communications and the obligation to erase and anonymize personal data where they are no longer needed in the electronic communications sector.[12] In fact, Article 15 para. 1 of the ePrivacy Directive is a classic declaratory opening clause (see F. Wollenschläger[13,14]; Müller/Schwabenbauer[15]; Sandhu, pp. 249 ff.[16]) referring to the Member States' exclusive competence to safeguard national security, defence, public security and the prevention of criminal offences.

Whereas the EU can legislate in the fields of data protection and harmonize the processing of electronic communications data, it lacks the competence to harmonize the powers of national law enforcement authorities under the current primary law framework. Whether or not one considers this a deficit in the EU's competence structure, it is not the task of the CJEU to fix it. As such, national data retention for the purposes defined in the opening clause does not fall within the scope of Union law. The CJEU's case law basically reaches the same conclusion via detours. In essence, the CJEU acknowledges a national security exception allowing for the preventive retention of all users of electronic communications systems in case of "serious threat to national security" (*La Quadrature du Net I*, para. 139).[17] Yet, methodologically, it would have been more consistent to declare such measures as falling outside the scope of Union law in the sense of Article 51 para. 1 of the Charter.

Inter-institutional division of power

It is the CJEU, not the EU legislator, which has erroneously taken on the task of defining the strict safeguards, and the limitations as well as technical requirements for data retention measures. In 2017, the Commission published its proposal for an ePrivacy Regulation, which has since May 2021 been negotiated in the Tri-

logue[18] (Council, Parliament, Commission). As revealed by the Council's negotiation mandate, the Member States are trying to pull the rug out from under the feet of the CJEU. They have proposed including the following recital which would heavily restrict both the scope of Union law and, implicitly at least, any chance of applying of EU fundamental rights on their national data retention laws:

> *"This Regulation does not apply to the protection of fundamental rights and freedoms related to activities which fall outside the scope of Union law, and in any event measures, processing activities and operations concerning national security and defence, regardless of who is carrying out those operations, whether it is a public authority or a private operator acting at the request of a public authority."*[19]

This is a clear attempt to counter the CJEU's extensive interpretation of the opening clause in the ePrivacy-Directive. Its aim is to exclude data retention measures carried out by private telecommunication providers in the state's interest from the scope of Union law. Article 11 of the proposed ePrivacy Regulation on restrictions of the confidentiality of electronic communications data is much broader than the current Article 15 para. 1 ePrivacy Directive which it is meant to replace. The proposed provision also allows restrictions on confidentiality to safeguard the enforcement of civil law claims. Furthermore, the opening clause is not only addressed to the Member States, but also directly to the EU legislator and may thus be a hint for the reintroduction of data retention at EU level. The Full Court's decision in *La Quadrature du Net II* is surprisingly in line with this legislative compromise. It would not be the first time the CJEU anticipates a decision by the EU legislator – the

same happened in 2014, when the court established the right to be forgotten in the *Google Spain* decision (C-131/12) before Article 17 GDPR was enacted by the EU legislator. And the same happened in its recent decision on Meta Platforms[20], when it tacitly applied the obligations for gatekeepers under the Digital Markets Act on a case from 2019.

Time for clarity

Whereas EU Law on data retention is considered to intrude too much on national fundamental rights, especially by liberal Justice Ministers in Germany, it seems like it cannot be intrusive enough[21] for others. It could be argued that the decade old dispute over data retention can be tackled by the EU legislator at least insofar as the internal market and serious cross border as well as online crimes are concerned. Indiscriminate and general data retention does constitute a mass breach of confidentiality. It therefore must be the absolute exception and based on objective evidence to prevent unlawful discrimination. Member States could at least agree on a set of serious crimes, for example by means of non-binding Guidelines. They should however refrain from merely referring to "terrorist activities", which is not a legal term. Otherwise, the Member States' contempt for the CJEU and the constant retreat of the Court risk undermining the supremacy of Union law as well as effective fundamental rights protection in the long term. Whereas the processing and retention of communication data by private actors as well as the access to this data by state authorities fall under the scope of Union law, surveillance activities of the competent state authorities remain excluded from the court's scrutiny. This competence division fails to adequately asses mass surveillance activities, which are the product of a public-private

partnership,[22] with law enforcement authorities making use of private data power.[23] The potential risks arising from mass data retention have only increased over the last decades, as the automated and real-time collection of metadata to predict private actions[24] and the use of AI tools[25] in warfare have shown.

The views expressed in this contribution are entirely personal to the author and do not represent the official position of the Federal Constitutional Court.

References

1. Aqilah Sandhu, 'The Judicial Dialogue in the EU Between Law and Politics' in Phillip Hellwege and Marta Soniewicka (eds.), *Law and Interdisciplinarity* (Mohr Siebeck, 2024), p. 167 ff.
2. Oliver Lepsius, 'Kontextualisierung als Aufgabe der Rechtswissenschaft' (2019) 74:17 *JuristenZeitung (JZ)*.
3. Aqilah Sandhu, 'Arbeitsrecht: Kopftuch/Heilerziehungspflegerin – Anmerkung zu ArbG Hamburg, Vorlage an den EuGH, Beschluss vom 21.11.2018 – 8 Ca 123/18 [Urteilsanmerkung] ' (2019) 18:4 *Zeitschrift für Europäisches Sozial- und Arbeitsrecht (ZESAR)*.
4. See CJEU, *Procura della Repubblica presso il Tribunale di Bolzano* (C-178/22), Judgment of 30 April 2024.
5. Conseil d'État, *La Quadrature du Net, French Data Network and Others* (Décision No. 393099), Decision of 21 April 2021.
6. Jean-Baptiste Jacquin, 'Le Conseil d'Etat autorise la poursuite de la conservation généralisée des données' *Le Monde* (21 April 2021), https://www.lemonde.fr/societe/article/2021/04/21/le-conseil-d-etat-autorise-la-poursuite-de-la-conservation-generalisee-des-donnees_6077560_3224.html.
7. Jean-Baptiste Jacquin, 'Le Conseil d'Etat autorise la poursuite de la conservation généralisée des données' *Le Monde* (21 April 2021), https://www.lemonde.fr/societe/article/2021/04/21/le-conseil-d-etat-autorise-la-poursuite-de-la-conservation-generalisee-des-donnees_6077560_3224.html.
8. Shahin Vallée and Gerard Genevoix, 'A Securitarian *Solange*: France Has Launched a Cluster Bomb on the EU's Legal and Political Order' (2021) *Verfassungsblog*.
9. More detailed on this Maximilian Gerhold, 'Der Conseil d'Etat zur Vorratsdatenspeicherung: Auf Biegen und Brechen des Unionsrechts für die nationale Sicherheit?' (2022) 75:3 *Die öffentliche Verwaltung*.
10. La Quadrature du Net (LQDN), 'Surveillance and Hadopi: EU Court Buries Online Anonymity a Little Further' (30 April 2024), https://www.laquadrature.net/en/2024/04/30/surveillance-and-hadopi-eu-court-buries-online-anonymity-a-little-further/.
11. La Quadrature du Net (LQDN), 'Surveillance and Hadopi: EU Court Buries Online Anonymity a Little Further' (30 April 2024), https://www.laquadrature.net/en/2024/04/30/surveillance-and-hadopi-eu-court-buries-online-anonymity-a-little-further/.
12. See CJEU, *Digital Rights Ireland* (C-293/12), Judgment of 8 April 2014.

13. Ferdinand Wollenschläger, 'Schriftliche Stellungnahme: Öffentliche Anhörung des Ausschusses für Recht und Verbraucherschutz des Deutschen Bundestages zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten' (21 September 2015), https://www.bundestag.de/resource/blob/388296/77e18af13306be0d15e1b9fe9c002d33/wollenschlaeger-data.pdf.
14. Ferdinand Wollenschläger, 'Schriftliche Stellungnahme: Öffentliche Anhörung des Rechtsausschusses des Deutschen Bundestages zum Antrag der Fraktion der CDU/CSU IP-Adressen rechtssicher speichern und Kinder vor sexuellem Missbrauch schützen BT-Drucksache 20/3687' (11 October 2023), https://kripoz.de/wp-content/uploads/2023/10/Stellungnahme-Wollenschlaeger.pdf.
15. Michael W. Müller and Thomas Schwabenbauer, 'Unionsgrundrechte und Datenverarbeitung durch nationale Sicherheitsbehörden' (2021) 29 *Neue Juristische Wochenschau*.
16. Aqilah Sandhu, *Grundrechtsunitarisierung durch Sekundärrecht* (Mohr Siebeck, 2021).
17. Aqilah Sandhu, 'Anmerkung zu EUGH: Datenschutzrecht: Anlassbezogene Vorratsdatenspeicherung nur bei erheblicher Gefahrenlage' (2021) 5 *Europäische Zeitschrift für Wirtschaftsrecht*.
18. Epicenter.works, 'Data Retention, Location Data, Cookie Banners: The ePrivacy Regulation Is Coming' *EDRi* (16 June 2021), https://edri.org/our-work/data-retention-location-data-cookie-banners-the-eprivacy-regulation-is-coming/.
19. European Union, 'Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)', 10 February 2021.
20. Aqilah Sandhu, 'EuGH 04.07.2023 - 252/21: Die Wettbewerbsbehörden als Datenschutzhüter [Urteilsanmerkung] ' (2024) 1:35 *Europäische Zeitschrift für Wirtschaftsrecht*.
21. See the contribution by Joachim Herrmann in this book.
22. Valsamis Mitsilegas, Elspeth Guild, Elif Mendos Kuskonmaz, and Niovi Vavoula, 'Data Retention and the Future of Large-Scale Surveillance: The Evolution and Contestation of Judicial Benchmarks' (2022) 29:1-2 *European Law Journal*.
23. See the contribution by Thomas Christian Bächle in this book.
24. See the contribution by Thomas Christian Bächle in this book.
25. Harry Davies, Bethan McKernan, and Dan Sabbagh, '"The Gospel": How Israel Uses AI to Select Bombing Targets in Gaza' *The Guardian* (1 December 2023), https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets.

Ana Bobić

Prioritising Member States Over Citizens

La Quadrature du Net II and the Growing Space for Member State Preferences

The classic story about the right to privacy and data protection in the EU is one of a high level of protection. According to this narrative, the Court is the champion of privacy and data protection, constraining the Member States' competences in national security.[1] And yet, this original rosy image is increasingly fading away, perhaps most visibly in the *La Quadrature du Net* litigation (now in its second iteration, C-470/21). I will argue that the second judgment is a continuation of two dynamics in EU law. First, the Court is still cleaning up the residual mess that lingers on from the now annulled Data Retention Directive (Directive 2006/24/EC). Second, in so doing, it is incrementally allowing the Member States to inch ever more closely to what the annulled Directive originally empowered them to do: indiscriminately retain personal data. What connects these two outcomes is the Court's shift towards carving out space for Member States' preferences to the detriment of the protection of the individual and her rights. This trend, I argue, is consistent with what is happening in other areas of EU law, pointing to a more general normative change in European integration.

To demonstrate these claims, I will do three things. I begin with presenting the "residual mess" that the annulment of the Data Retention Directive left, which is an important context for understanding the judgment and its novelties. Second, I will briefly present the judgment in *La Quadrature du Net II*, by showing that the judgment joins a now constant jurisprudence, extending the space for data retention by the Member States as well as the justifications they may use when doing so. Lastly, I will place this trend in the wider context of the EU's recent prioritising of the Member States over its citizens.

The residual mess of the Data Retention Directive

The Data Retention Directive saw the light of day as a response to the increased regulation of data retention across the Member States for national security and the fight against terrorism.[2] It imposed an obligation on service providers to retain telecommunication data, making it available for access by competent national authorities to combat "serious crime". The data to be retained was confined to traffic data, location data, and data necessary to identify the user, to the exclusion of the content of communications. The procedure for access itself was left to the discretion of the Member States and was outside the scope of the Directive, subject to the principles of proportionality and necessity.

Although the Directive initially survived the competence challenge (C-301/06), its national implementing measures were subject to a number of actions before national courts,[3] and ultimately reached the Court of Justice via the preliminary reference procedure, where it was annulled (*Digital Rights Ireland*, Joined Cases C-293/12 and C-594/12). Without the Directive, some Member States simply retained their data retention legislation as a matter of national competence, which led to further litigation before the Court of Justice. In *Tele2 Sverige and Watson* (Joined Cases C-203/15 and C-698/15), the Court of Justice brought the matter back within EU law, with the ePrivacy Directive (Directive 2002/58/EC) (and most prominently its Article 15 (1)), now doing all the heavy lifting. Accordingly, if the Member States want to order telecommunication service providers to retain data, they must do so in line with the ePrivacy Directive and the Charter. In that sense, the confidentiality of private communications is the rule, and data retention the exception. Any indiscriminate data retention may be ordered solely for the purpose of fighting serious crime, be subject

to prior review by a court or an independent administrative authority, and be retained within the EU.

With Member States eager to carve out as many exceptions as possible under Article 15 (1) of the ePrivacy Directive, national courts pursued further preliminary references. This bring us to the first *La Quadrature du Net* judgment (Joined Cases C-511/18, C-512/18 and C-520/18), where the Court expanded the possibility of indiscriminate data retention: "the objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives" (para. 136). Using the Court's finding, the referring court (the French Conseil d'État), found that preventing breaches of public order, tracking down the perpetrators of criminal offences and combating terrorism are of constitutional value, safeguarding the fundamental interests of the nation.[4]

The judgment may be used to summarise the standard set of rules for data retention: Indiscriminate data retention is allowed for the protection of national security or combating serious crime. Conversely, combating ordinary crime may only justify discriminate data retention (para. 141). The degree of interference with fundamental rights must have a correspondingly proportionate limitation, and any indiscriminate retention must be subject to prior review by either a court or an independent administrative body whose decisions are binding (para. 139). The wisdom was repeated in *Prokuratuur* (Case C-746/18) and *Commissioner of An Garda Síochána* (C-140/20). This is the crucial context for understanding *La Quadrature du Net II*.

La Quadrature du Net II: normalising data retention

The French "Hadopi law" aimed to prevent internet users from sharing copyrighted works without the permission of the copyright holders.[5] The law's namesake agency was empowered with a "graduated response" to copyright infringements: 1) sending "recommendations", which are similar to warnings; 2) within a period of one year following the sending of a second recommendation, in respect of conduct that may constitute a repetition of the offending conduct detected, the subscriber is notified that the conduct may constitute the offence of gross negligence, which is a minor offence; 3) the referral to the public prosecution service of conduct that may constitute such a minor offence or, as the case may be, the offence of counterfeiting (para. 57). To carry out its work, Hadopi is able to order service providers to retain IP addresses and personal data and information relating to their holders, concerning their civil identity. No prior judicial or independent administrative review is necessary for Hadopi to make such requests.

In sum, at stake here is a national law allowing for indiscriminate data retention, for the purposes of preventing and prosecuting crime, without prior review. Originally hearing the case in grand chamber, the Advocate General proposed a change in the case law for offences conducted exclusively online, dispensing with the need for a prior review. The case was reopened for a second hearing, this time before the full court. The Court made great efforts (see in particular paras. 77-84) to maintain that it is, in fact, not at all changing its previous case law, but it just so happens that this case may be distinguished on facts.

Why it was necessary to then do so in full court is puzzling to say the least, given the magnitude of other recent cases decided in that composition (for example, the validity of the Rule of Law Con-

ditionality Regulation (C-156/21) and the validity of a treaty change in *Pringle* (C-370/12)). This is all the more curious when looking at the fact that Advocate General Szpunar called his proposal in his First Opinion a "readjustment" of the case law on data retention (section IV.4 of the Opinion),[6] but in his Second Opinion insisted that "the solution which I propose aims not to call in question the existing case law, but, with a view to a certain pragmatism, to enable that case law to be adapted in particular and very narrowly defined circumstances" (para. 30).[7]

Regardless of semantics, the Court found that in the present case, regardless of the large scale of indiscriminate retention (most strikingly, compare this to para. 100 of *Space Net* (Joined Cases C-793/19 and C-794/19) as well as paras. 139 and 141 of the first *La Quadrature du Net*), the interference with fundamental rights is less serious than in previous cases. The Court stated that "in relation to email and internet telephony, provided that only the IP addresses of the source of the communication are retained and not the IP addresses of the recipient of the communication, those addresses do not, as such, disclose any information about third parties who were in contact with the person who made the communication. To that extent, that category of data is less sensitive than other traffic data" (para. 76). Since the intrusion is (allegedly) less serious, the margin for authorities to intervene increased, warranting a relaxed set of criteria, most crucially omitting prior review.

Thus, policing copyright infringement on a large scale in the eyes of the Court does not meet the standard of serious interference. Two criticisms may be directed to this conclusion. First, by using the method of distinguishing (although it is a matter of course that every single case is different), the Court signalled to national courts to continue asking about every measure involving data retention, without providing a more general rule. Put differ-

ently, national courts cannot be certain that *La Quadrature du Net II* provides a general rule for online offences, or whether its findings will later be confined to the French Hadopi law. Perhaps this is what the Court wants to achieve.

The second criticism concerns the departure from the way in which exceptions contained in Article 15 (1) of the ePrivacy Directive were previously interpreted: As exhaustive, among which the prevention and prosecution of ordinary crime did not feature among those justifications for which indiscriminate retention of data was allowed (and this specifically concerning IP addresses in the abovementioned *Space Net* judgment). Copyright infringements are far from being the only crimes committed (exclusively) online, and therefore the Member States may see this as a green light to expand the list of crimes for which indiscriminate data retention may be ordered. And all this without prior judicial or administrative review.

The rule, not an exception

Beyond the protection of privacy and personal data, I see the judgment as part of a broader trend of the EU's normative orientation. When the EU is presented with the choice of individual rights versus Member States' regulatory powers, it increasingly chooses the latter. That was the case in the Euro crisis, where the principle of equality of Member States was the main and guiding rationale for endorsing measures based on the logic of strict conditionality, disregarding the rights of citizens affected by austerity measures. Specifically, conditionality is, at its core, an insurance that the Member States receiving assistance will continue to pursue a sound budgetary policy. This in turn means that it would not become necessary for Member States to cover the liabilities of others in con-

travention of the prohibition of monetary financing under Article 125 TFEU. This resulted in a disregard of the major re-distributive effects of such decisions for citizens across different Member States and different socioeconomic groups across the EU.

The same applies to the principle of solidarity, which is mentioned in the Treaties concerning both the relations between citizens and those between the Member States. The Court of Justice, however, endorsed it as a general principle only when applied between the Member States (concerning the fair sharing of burden in asylum (Joined Cases C-643/15 and C-647/15) and energy (C-848/19 P)). In addition, the new Migration and Asylum Pact follows this trend by allowing the Member States wide powers to the detriment of individual rights of asylum seekers,[8] including opening up space for their surveillance.[9]

The narrative of the Court as the institution protecting the individual and her rights is thus at risk, and the judgment in *La Quadrature du Net II* did little to change this.

References

1. Marcin Rojszczak, 'Data Retention in the Light of Copyright Infringements: Protecting the Status Quo or Seeking a Third Way? (Case C-470/21, *La Quadrature du Net II*)' (2024) 31:4 *Maastricht Journal of European and Comparative Law*; Monika Zalnieriute, 'A Struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of European Union' 85:1 *The Modern Law Review*; Liv McMahon, 'Meta Must Limit Data for Personalised Ads – EU Court' *BBC* (4 October 2024), https://www.bbc.com/news/articles/c4gr4r5ln03o.
2. European Union, 'Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC {SEC(2005) 1131}', 21 September 2005.
3. Ana Bobić, 'Fundamental Rights Review' in *The Jurisprudence of Constitutional Conflict in the European Union*, (Oxford University Press, 2022).
4. Conseil d'État, *La Quadrature du Net, French Data Network and Others* (Décision No. 393099), Decision of 21 April 2021.
5. Wikipedia, 'HADOPI law' https://en.wikipedia.org/w/index.php?title=HADOPI_law&oldid=1255984801.
6. CJEU, Opinion of Advocate General Szpunar, *La Quadrature du Net* (C-470/21), Opinion of 27 October 2022.
7. CJEU, Opinion of Advocate General Szpunar, *La Quadrature du Net II* (C-470/21), Opinion of 28 September 2023.
8. Amnesty International, 'EU: Migration and Asylum Pact Reforms Will Put People at Heightened Risk of Human Rights Violations Migration and Asylum Pact Reforms Will Put People at Heightened Risk of Human Rights Violations' (4 April 2024), https://www.amnesty.org/en/latest/news/2024/04/eu-migration-asylum-pact-put-people-at-risk-human-rights-violations/.
9. PICUM, 'The EU Migration Pact: A Dangerous Regime of Migrant Surveillance' (11 April 2024), https://picum.org/blog/the-eu-migration-pact-a-dangerous-regime-of-migrant-surveillance/.

Guido Westkamp

Anonymity and Surveillance, Creativity and Copyright

Disrupting the Balance Between Users, Authors, Exploiters, and Platforms

It is almost too trite to state that the emergence of digital networks over the past decades has presented a problem for copyright exploiters. Enforcement of copyright against intermediaries was and is arduous. The legal landscape remains complex due to different rules on liability in national laws and the existence of safe harbour provisions. Copyright exploiters thus resorted to adopting strategic enforcement targeting individual users. These, however, would often remain anonymous due to the lack of access to traffic data revealing their identity. Things changed in 2019 with the coming into force of Article 17 of the Directive on Copyright in the Digital Single Market (DSMD), which imposes certain obligations on platforms to remove infringing content and to employ filtering technologies for certain larger platforms. Article 17 DSMD – a fervently debated provision – requires certain large platforms to remove content infringing copyright under certain circumstances by using upload filters. That legislative move clashes with communicative freedoms because it cannot be said for certain at the very moment of the upload whether content that makes use of other works (memes, remixes etc) is infringing, or whether such use is covered by an exception to copyright. In Germany, the clear legislative objective under the (complex) new "Urheberrechts-Diensteanbieter-Gesetz" (UrhDAG), which transposes Article 17 DSMD, was to safeguard the collective expectation to communicative freedoms and to maintain creativity on platforms. But the decision in *La Quadrature du Net II* (C-470/21) – broadly permitting retention of traffic data for minor offences and their disclosure for the purpose of litigation – has the adverse effect: it incentivises and reinforces broad enforcement strategies targeting users and requiring platforms to hand over such data. Evidently, no user would risk becoming the subject of litigation instigated by powerful copyright exploiters.

The Matrix Reloaded

The decision in *La Quadrature du Net II* is a disfavor to creativity. It permits a renaissance of strategic copyright enforcement that is at odds with the specific German transposition of the Copyright Directive (Article 17 DSMD) in the UrhDAG and is hardly in line with the requirements under the EU Charter of Fundamental Rights.

In Germany, the legislator opted for a model that does not require immediate removal of potentially infringing content but allows users to "flag" transformative or referential uses as falling under the caricature, parody and pastiche exception. Authors (not exploiters) will receive fair compensation for such uses and, in consequence, the content "stays up". The copyright owner can then make a complaint to the platform seeking removal or pursue litigation.

The approach differs very much from solutions that are simply based on requiring platforms to install upload filters that immediately remove any content that could potentially be infringing. Indeed, from a fundamental rights perspective, the German transposition focussed on balancing the interests of authors and (usually anonymous) users and their respective claims to freedom of communication and art, rather than pitting the commercial interests of the copyright and the platform industries (in particular, their respective claims to property and freedom of business) against each other. The decision in *La Quadrature du Net II* likely has the opposite effect: the copyright industries will have access to traffic data, which in turn allows fortified strategic enforcement and litigation against users. That effect is inconsistent with the EU Charter and the very jurisprudence of the Court of Justice concerning user rights under copyright and fundamental rights law.

Copyright enforcement and anonymity

The Court of Justice confirmed that data retention is permissible even though the crime in question is not serious. The decision centrally concerns copyright law. A critical effect of the decision is that platform or social media users relying on copyright exceptions and therefore exercising their rights may lose anonymity. Now, the copyright industries can enforce the right to obtain user data based on traffic data much more easily.

The decision is arguably inconsistent with previous case law on data retention and causes frictions with the overall balance that has been achieved in copyright law over the last decade. This applies at the EU level, but to a much more critical degree to Germany.

The Court of Justice has early on affirmed in its *Promusicae* (C-275/06) decision that copyright enforcement – which today rests upon Article 8 of the Enforcement Directive[1] – is subject to balancing with privacy and data protection concerns under the EU Charter. Later, the Court of Justice (in *Funke Medien* (C-469/17) and *Spiegel Online* (C-516/17)) conceded that written copyright exceptions (such as for purposes of quotation or media uses) must be construed in light of the EU Charter – and that, importantly, these exceptions give users rights rather than mere privileges. This was a compromise between secondary EU copyright law (Article 5 of the InfoSoc Directive (ISD), Directive 2001/29/EC), and the position taken by the German Constitutional Court in the *Pelham* case[2], according to which freedom of art should be recognised as a balancing factor under the pre-existing "free use" clause (previously § 24 (1) of the Authors Rights Act, now repealed and replaced in § 51a UrhG with the "caricature, parody and pastiche" exception in Article 5(3)(k) ISD). In *Pelham* (C-476/17), the Court of Justice indeed

refused to allow domestic law to apply fundamental rights as external limitations to copyright infringement, unless a written exception is in place.

The copyright industry would usually claim that any use in such way *prima facie* constitutes an infringement. For example, an alleged pastiche may constitute, following conventional copyright doctrine, a criminal offence if found to be, in fact, a reproduction. But the assessment is utterly convoluted. Opinions on what constitutes pastiche vary considerably. "Pastiche" (in the sense of some transformative or referential use) also comes close not only to notions of non-literal reproductions, but also to the distinction between idea and expression, to the minimum requirement that a substantial part of the author's expression has been taken, and to the dividing line to be set between reproduction and adaptation, to name but a few.

The matrix of interests

The presence of surveillance and the potential loss of anonymity now following from the *La Quadrature du Net II* decision has the capacity to render the right to pastiche (and communicative freedoms by and large) obsolete. Anonymity is an indispensable condition to exercise fundamental rights including the right to freedom of expression and art on social media and sharing platforms. Unavoidably – and especially concerning large platforms such as Google's YouTube service – copyright exploiters consider the presence of such platforms as a threat to their market and irritating competition. That collision between big platforms and the copyright industry has ultimately led to Article 17 DSMD (previously (draft) Article 13). On the one hand, Article 17 imposes extended direct liability standards for platform operators for any-

thing potentially infringing uploaded content by users. On the other hand (and after much tribals and tribulations in the legislative process), it is introducing a mandatory provision: Member States must ensure that users can effectively exercise their fundamental rights and rely, in particular, on pastiche. But how?

The matrix of interests that national legislators face when transposing these conflicting principles is multifarious. Platforms may rely on the freedom to conduct their business. Exploiters would point out that they enjoy property rights and benefit from a principle of a high level of protection under secondary law. Users engaging in memes and mashups will refer to communicative freedoms and, additionally, may rely on the rights to data protection and privacy should they be targeted by the industry.

Authors versus exploiters

And authors? Authors can indeed claim rather diverse legitimate interests that legislators must recognise. Of course, authors would like to see fair remuneration (not necessarily derived from agreements with their exploiters, as the case may be, but also via a new statutory licensing scheme), but also, and more importantly, need rights of access to preexisting works if the purpose of copyright is indeed to foster creativity. To complicate things, many authors will be platform users – and, of course, vice versa.

For exploiters, the legal landscape that should, ideally, be unfolding appears straightforward. To them, necessarily, the proliferation of sharing platforms constitutes direct competition with their own business models, i.e. streaming or download services. Of course, any content resembling a work or a producer right (even snippets taken from a broadcast or sound recording) constitutes, *prima facie*, an infringement, a position fully aligned with copyright

doctrine. Hence, platforms must immediately remove any protectable content – it is their obligation to install upload filters. Users would still have a right to rely on pastiche, but must enforce it against the platform after their content had been taken down. Indeed, this may also be the preferred solution from the perspective of the platform operator. Technical solutions mean less expenditure compared to laborious and elaborate content moderation schemes.

And even if such moderation scheme is in place, exploiters may still employ a strategy to dissuade users from transformative uses. The threat of costly litigation to the individual user is real (and a protected right under Article 47 EU Charter) – provided, of course, the platform has information on the offending user's identity. This may be so or not. Whether a duty to disclose such data to the potential claimant exists is, first and foremost, a matter of secondary law and may depend on further conditions such as a court order. The effect is, overall, to disincentive creative expression that may potentially be covered by freedom of art.

From a constitutional perspective, the "stay down" scheme follows from a particular framing of the legislative proportionality exercise. The assessment is essentially based on balancing economic interests – the right to property enjoyed by copyright exploiters versus the right to business enjoyed by platform operators. It is no coincidence that, around 2018, when lobbying for direct liability began, the main and most prominent argument put forward by copyright exploiters was the alleged "value gap". In essence, they claimed numerous instances of unjust enrichment at the expense of both traditional and modern markets, including streaming and download services.

The Court of Justice subsequently noted, in the *Poland* decision (C-401/19) (following the opinion by AG Saugmandsgaard Øe), that

the use of upload filters is compliant with the EU Charter only in case of "manifest infringements", though it did not define that term. However, the Court also clearly conceded the need for user creativity. There is one example that may be used to illustrate an approach that manages to reduce complexity convincingly, much in line with the assertions in the *Poland* decision: The German UrhDAG transposes Article 17 DSMD in certainly a unique manner. The German government had made it clear, immediately following the adoption of the DSMD, that it would not accept widespread filtering in the interests of communicative freedom. The central mechanism is, in short, that users may flag uploaded content as pastiche or parody, and if so, the platform must not remove that content unless the right holder objects and refers the matter to content moderation, or indeed to a court. Yet the real "trick" is that the new law employs a mechanism not known in any other jurisdiction. Authors receive, for every flagged use, remuneration from the platform and thereby have, mostly, no incentive to prevent or object to such uses. Because of that prospect of a new source of income, the new law also absolves the operator from making decisions concerning the meaning of the notoriously opaque terms of pastiche or parody – and therefore also, on balance, averting the thorny problem of platform staff elaborating on the scope of fundamental rights. The mechanism adopted may, as a more distant yet powerful effect, also incentivise more established artists to welcome platform uses in general – and thus to exert pressure on exploiters to license any platform use (to ensure that income is generated for their benefit to achieve the ultimate objective underpinning the new law).

In consequence, the "medium of money" ensures creative freedom. In a subtle and almost perfidious way, the German legislator (unconsciously, probably) marginalised the respective economic

rights and interests of both platforms and exploiters, turning the rights to property and business into what may be termed as trans-subjective rights to be exercised in the interest of authors and users much in the sense of an "agency" right.

Exploiters therefore lose out twice: they cannot fully control relevant flagged uses, and in the future, new statutory licensing models might emerge, requiring platforms to make payments to authors. This marginalisation of exploiter interests creates further issues – that is, to strategically target individual users, a prospect that the decision in *La Quadrature du Net II* now reinforces by giving access to traffic data held by providers. It is easy to see why: a user flags their content as pastiche, the content stays up, which results in a payment to the author. The marginalised exploiter, however, either as a licensee or as an owner of a neighbouring right, may well wish to instigate a complaint with the platform, or indeed take immediate legal action through courts. User knowledge on such strategy will spread fast. In addition, adopting such strategies will work against the interests of authors – no payment is due where the work in question is ultimately removed.

Yet, the UrhDAG is silent on user anonymity. The traditional right to information (§ 101 UrhG) still applies, a right that has been construed by German courts in a manner very favorably to right owners. Data protection laws play no role in such scenario, as I have outlined elsewhere in more detail.[3]

Takeaway

At this juncture, the *La Quadrature du Net II* decision creates an enormous friction between the delicate balance achieved under the UrhDAG and the broad permission for data retention following from the ruling. In fact, following an economic logic, strategic en-

forcement targeting individual users is now the only means for the copyright industries to protect their own existing or future markets and thus to avoid unwanted competition. It is easy to imagine how such strategy could be rolled out. A user flags, and money is paid to the author. But the right owner can always instigate legal proceedings, and for that they will need to know the personal details of the alleged offender. Previously, this was restricted to static data, and a claim to disclose such data, of course, depends on whether the operator held such data in the first palace. Now, exploiters can effectively instil fear of litigation on the platform through access to traffic data, making widespread litigation much more effortless. At the EU level, such effect obviously collides with the relevance of pastiche as asserted in the decision in the *Poland* case. For Germany, the decision – more critically – eradicates the incentive for the industry to licenses uses on platforms in general. To put it bluntly: the decision, primarily concerning copyright, disrupts the legislative decision in a Member State that adopted a solution centrally emphasising creativity.

What is most mischievous is that the Court of Justice saw itself unable to cast an eye on its own decision in *Poland* and accordingly to elaborate on its own stance which places emphasis on user creativity. It did not consider the effects the ruling will have on user anonymity as a central condition for the exercise of fundamental rights under the DSMD. It can easily be predicted that the matter will become another bone of contention yet again between the German Constitutional Court and the Court of Justice on the relevance and status of communicative freedoms in a copyright context – and, ultimately, whether it is the former who will have the last word on such constitutional matters. It is certainly not a coincidence that German courts in 2007 asked the Court of Justice what is the appropriate methodological approach to construing commu-

nicative freedoms protected under constitutional law in copyright matters. As mentioned, the Court of Justice had – very likely to avoid frictions with the German Constitutional Court – to make concessions. It had to abandon the conventional principle that copyright exceptions must be "interpreted narrowly" in the interest of rights holders and also had to broadly relativize the "high level of protection" tenet under secondary law. The *La Quadrature du Net II* decision now gives the copyright industry leverage to undermine the delicate balance of interests, particularly in the German UrhD-AG. A disservice indeed.

References

1. Official Journal of the European Union, 'Corrigendum to Directive 2004/48/EC on the Enforcement of Intellectual Property Rights' (OJ L 157), 30 April 2004.
2. Neil Conley and Tom H. Braegelmann, 'English Translation: Metall auf Metall (Kraftwerk, et al. v. Moses Pelham, et al.), Decision of the German Federal Supreme Court no. I ZR 112/06, dated November 20, 2008' (2009) 56 *Journal of the Copyright Society*.
3. Guido Westkamp, 'Digital Copyright Enforcement after Article 17 DSMD' (2023) 14:4 *Zeitschrift für geistiges Eigentum*.

Marcin Rojszczak

Data Retention Laws and La Quadrature du Net II

A Necessary Adjustment to a Timely Problem

Data retention laws are not a shield for online abusers or a means of ensuring impunity. While new forms of data processing pose privacy risks, they also enable the implementation of data retention regimes to combat abuse without going beyond what can be considered necessary in a democracy.

When the CJEU handed down its judgment in *La Quadrature Du Net I* (C-511/18, C-512/18 and C-520/18) (and *Privacy International* (C-623/17)) in 2020, it seemed that the saga of retention cases was coming to an end. The Court – in its eighth consecutive ruling – clarified (what appeared to be) the final aspects of the application of data retention legislation, which were largely focused on the use of such information in the area of state security.[1]

However, this did not happen. The following years saw the equally significant cases of *Graham Dwyer* (C-140/20) and *SpaceNet* (Joined Cases C-793/19 and C-794/19). And when, once again, it seemed that the issue of general data retention, encompassing traffic and location data, was ultimately closed (in *SpaceNet*, the CJEU clearly and unequivocally indicated its impermissibility in criminal proceedings), the problem of retention rules began to be examined from a new, equally important perspective. As a result of a request for a preliminary ruling from the Conseil d'État,[2] the Court had to clarify again whether the general retention of IP addresses can be used as a mechanism to counter online copyright infringement.

The *La Quadrature Du Net II* (C-470/21) case – especially the AG's opinion accepting the possibility of using such a measure[3] – sparked a discussion on the possibility of revising the CJEU's retention jurisprudence to date.[4] However, I do not believe that the CJEU's judgment actually heralds a "Copernican revolution"[5] or is a "Pandora's box"[6]. It rather complements the existing line of juris-

prudence. Like a cliffhanger in a TV series, it foreshadows that the story is not yet over.

Retention of telecommunications data in the CJEU case law

The Court of Justice's position on generalised forms of retention has always referred to the principle of proportionality, according to which a serious interference with an individual's rights can only be justified by the pursuit of objectives that can also be considered serious. In the Court's view, processing of all retained data makes it possible to reconstruct a digital profile of an individual, revealing detailed information about them – including their worldview, health status, political beliefs etc. Thus, such serious interference can only be justified by the fight against serious crime and national security objectives. Again, however, this measure cannot be applied in a generalised manner, as its application would then not be linked to a concrete and real threat to an important public interest. Rather, it would become a tool for collecting redundant data.

The examination of national retention laws should therefore be carried out in two dimensions: qualitative and quantitative. The former serves to assess the degree of interference with individual rights. Serious interference (collecting the totality of electronic communications metadata) should be limited to cases in which serious objectives are pursued and should require special legal safeguards, such as judicial oversight. When examining retention laws, attention should thus first be paid to the quality of the data collected, which reveals the degree of interference with individual rights.

Importantly, however, the CJEU has not predetermined the absolute impermissibility of all untargeted forms of data retention in its case law to date.[7] The cases examined by the Court concerned

the retention of high-quality data, most often the entirety of metadata from electronic communications, such a location data, date and time of communication, and the communication partners involved (allowing profound interference with individual rights). Consequently, the Court's interpretation concerned the collection and processing of this type of information. It was only in *La Quadrature du Net II* that the CJEU was confronted with the permissibility of applying untargeted retention of a certain category of information, the collection and processing of which, within a limited scope and for a specific purpose, does not seem to seriously interfere with individual rights.

The problem of IP address retention

The background of *La Quadrature du Net II* was the permissibility of a special legal procedure, the so-called graduated response procedure,[8] which was established in French law for cases of counteracting copyright infringement.[9] Its essential part is sending notifications to users (subscribers of an internet service provider) about the use of their network termination to share files on a P2P network in a way that infringes copyright. A graduated response procedure is carried out by an administrative body (Arcom[10], formerly Hadopi) and, in principle, does not involve the imposition of criminal sanctions on users. Only in the case of repeated copyright infringement does the procedure provide for the possibility of notifying a public prosecutor of the infringement.

On the technical side, the procedure is implemented when copyright holders transmit aggregated information about files being shared on P2P networks, along with the IP addresses of the users sharing these files. Arcom combines this information with data from telecoms operators, thus establishing the identity of the

subscriber to be notified of the infringement detected. It was in fact this last element of the mechanism that was at the heart of the dispute in *La Quadrature du Net II* – namely, whether telecommunications operators can be ordered to pre-emptively collect information on the IP addresses of all users simply because these data may (and in some cases will) prove necessary for the purposes of detecting copyright infringements.

A positive answer, it seems, would lead to a situation in which it would be permissible to retain a particular type of metadata (source IP addresses) in an untargeted manner and without any concrete link to a crime. According to critics of such a solution, this would lead to the Court accepting the use of an intrusive measure (generalised data retention) for less important public tasks whilst simultaneously rejecting its use for the purposes of fighting serious crime.

However, a negative answer – upholding the prohibition of IP data retention in an untargeted manner for the use of combating general crime – would make it significantly more difficult to investigate online copyright infringements. In the Court's view, it would in fact not so much hinder such a fight as make it impossible, creating the risk of systemic impunity for perpetrators (para. 119).

In my view, such a polarised framing of the problem presented in *La Quadrature du Net II* is flawed and leads to oversimplification. On the one hand, the need for effective prosecution of online infringements is real. On the other hand, the measure needed to provide this protection – albeit using untargeted data retention – is not the same as the measure referred to in the earlier CJEU case law. Not every data retention procedure is conducted in an untargeted manner, but neither does every case of data retention affect the rights of the data subject in the same way. By skipping the

qualitative assessment and focussing solely on the quantitative assessment of data collection principles, one loses sight of the actual surveillance potential of the entire process. The Court aptly recognised this problem, addressing it in detail in its judgment.

A readjustment or a u-turn?

In *La Quadrature du Net II*, the Court confirmed in principle that imposing an obligation on telecommunication providers to retain the IP addresses of the source of a connection does not infringe EU law, provided that additional and specific legal safeguards are established. Once again, it based its interpretation on the principle of proportionality, examining whether the bulk collection of IP addresses constitutes a serious interference with individual rights. In this regard, the Court considered that IP addresses, as long as they are not combined with other information (e.g. sites visited, information searched, content viewed etc.), do not enable the establishment of detailed information about an individual. Therefore, their processing does not lead to a serious interference and, thus, should not be limited solely to the pursuit of purposes that can be described as serious. The Court's reasoning was based on two assumptions: (1) IP addresses do not reveal detailed information about an individual (para. 76) and (2) the processing of such data on a case-by-case (individualised) basis does not lead to the profiling of data subjects ("watertight separation", paras. 83, and 87-89).

IP addresses as less sensitive data

The above leads to questions about the actual impact of *La Quadrature du Net II* on the application of retention rules in Member States. On the one hand, many point to the risk of lowering the

restrictive standards[11] set by the CJEU in its earlier case law, which were summarised in the *SpaceNet* case. *La Quadrature du Net II* can also be read as a narrow exception to the general prohibition of untargeted data collection established in former case law. It permits such untargeted data collection only if it takes place in a strictly controlled environment. Furthermore, it remains to be seen whether the judgment initiates a discussion on untargeted retention in relation to other categories of traffic and location data.

In the Court's view, the essential reasoning in *La Quadrature du Net II* remains consistent with – and even reinforces – the earlier case law. Indeed, the qualification of IP addresses as less sensitive data has made it possible not only to put forward a different set of legal safeguards for its processing, but also to dispense with the mandatory prior oversight – which, according to earlier case law, should be applied in cases where retained telecommunications data are accessed.

Although the Court's reasoning is consistent, it is based on the assumption that IP addresses can indeed be categorised as low-sensitivity data. The question is whether this is always the case – all the more so as the experience of recent years shows that groups of information initially classified as not very sensitive[12] (e.g. geolocation data) have in subsequent years been classified by the same Court as requiring the identical protection[13] as the communications themselves. Similar doubts are already present today with regard to IP address data. For example, can information about users of the Tor network – in particular, data recorded at the originating and terminating nodes – really be classified as low-sensitivity data in every case? It should be noted that the collection of IP addresses at entry and exit nodes is a key technique for de-anonymizing Tor traffic and identifying users – a

method successfully employed by security and intelligence agencies worldwide.

More data retention to come?

More controversy surrounds the link between data collection rules and the permissible scope of data processing. In particular, attention is drawn to the risk that implementing the safeguards model described in *La Quadrature du Net II* will only create the illusion of control. If state authorities are able to require telecommunication operators to collect large databases of user information, these data will – sooner or later – also be used for other public purposes. I call this phenomenon "the proliferation of electronic surveillance measures", and it has, in fact, been observed for years.[14]

In the light of the existing case law, there appears to be no obstacle to IP address retention data being used by secret services in the area of state security. Such data may also be helpful in identifying perpetrators of other (more serious) crimes. The question of the required legal safeguards restricting the use of this information may be secondary in a situation where the data have already been collected. This leads to the conclusion that in *La Quadrature du Net II*, the Court – consciously or not – permitted the implementation of a model awaited by many governments, whereby states will be able to legally retain (some) electronic communications data, with the obligation to demonstrate that the necessity criterion is met only at the stage of accessing the data.

A difficult balance to strike

La Quadrature du Net II has been met with mixed reactions, with mainly critical arguments pointing to the departure from the previ-

ous clear interpretation regarding the prohibition of generalised metadata retention measures.[15] These voices should not be ignored, as they express legitimate concerns about the possibility of the judgment introducing solutions which are *de facto* identical in terms of intrusiveness to those previously challenged by the CJEU. At the same time, however, it is important not to lose sight of the fact that law – including data retention rules – must not become a mechanism for protecting criminals. The scale and mass nature of online rights violations are a real problem. P2P networks are not only a threat to copyright protection, but also an environment for the distribution of content related to serious crime (e.g. extremist speech or child abuse materials[16]). It is therefore necessary to strike a balance between the two rationales and to propose solutions that adequately protect users by not guaranteeing impunity for criminals.

La Quadrature du Net II fits into this need but, at the same time, does not seem to explain in sufficient depth the relationship between the collection and processing of low-sensitivity data and their subsequent use by state authorities. Addressing this issue more clearly would help to clarify many controversies and answer questions about the future of retention laws in Member States.

References

1. Marcin Rojszczak, 'National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts' (2021) 17:4 *European Constitutional Law Review*.
2. CJEU, 'Request for a Preliminary Ruling from the Conseil d'État: *La Quadrature du Net, French Data Network and Others v Premier Ministre, Ministère de la Culture* (C-470/21), 30 July 2021.
3. CJEU, Opinion of Advocate General Szpunar, *La Quadrature du Net* (C-470/21), Opinion of 27 October 2022.
4. Oreste Pollicino and Pietro Dunn, 'Op-Ed: "Carving a Third Way? The Opinion of AG Szpunar in *La Quadrature du Net* (C-470/21)"' *EU Law Live* (22 November 2023), https://eulawlive.com/op-ed-carving-a-third-way-the-opinion-of-ag-szpunar-in-la-quadrature-du-net-c-470-21-by-oreste-pollicino-and-pietro-dunn/.
5. Stefan Krempl, 'Vorratsdatenspeicherung: Forscher erkennen "kopernikanische Wende" beim EuGH' *heise online* (5 May 2024), https://www.heise.de/news/Vorratsdatenspeicherung-Forscher-erkennen-kopernikanische-Wende-beim-EuGH-9708717.html.
6. Theresa Bosl, 'Not You Again!: Mass Surveillance Before the CJEU and Why "Hadopi" Could Be a Game-Changer for the Right to Privacy' (2023) *Völkerrechtsblog*.
7. Edoardo Celeste, 'The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios' (2019) 15:1 *European Constitutional Law Review*.
8. Primavera De Filippi and Danièle Bourcier, '"Three-Strikes" Response to Copyright Infringement: The Case of HADOPI' in Francesca Musiani, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson (eds.), *The Turn to Infrastructure in Internet Governance*, (Palgrave Macmillan, 2016).
9. Journal Officiel de la République Française, 'Loi No. 2021-1382 relative à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique (1)', 25 October 2021.
10. Brad Spitz, 'France: ARCOM, A New Regulatory Authority to Fight Online Copyright Infringement' *Kluwer Copyright Blog* (6 January 2022), https://copyrightblog.kluweriplaw.com/2022/01/06/france-arcom-a-new-regulatory-authority-to-fight-online-copyright-infringement/.
11. Marco Mauer, 'The Unbearable Lightness of Interfering with the Right to Privacy' (2024) *Verfassungsblog*.
12. European Court of Human Rights, *Uzun v. Germany* (Appl. No. 35623/05), Judgment of 2 September 2010.
13. European Court of Human Rights, *Ekimdzhiev and Others v. Bulgaria* (Appl. No. 70078/12), Judgment of 11 January 2022.

14. David Lyon, *The Electronic Eye: The Rise of Surveillance Society* (University of Minnesota Press, 1994).
15. EDRi, 'A Complete U-Turn in Jurisprudence: Hadopi and the Future of the Court of Justice of the European Union's Authority' *European Digital Rights* (7 February 2024), https://edri.org/our-work/a-complete-u-turn-in-jurisprudence-hadopi-and-the-future-of-the-cjeus-authority/.
16. Matthieu Latapy, Clémence Magnien, and Raphaël Fournier, 'Quantifying Paedophile Activity in a Large P2P System' (2013) 49:1 *Information Processing & Management*.

Valentina Lana, Aziz Z. Huq

Spillovers and Unexpected Interactions

Reading the La Quadrature du Net II Decision in Context

For more than a decade now, the Court of Justice of the European Union (CJEU) has struggled with the legality of various bulk surveillance mandates imposed under European and national law. Since its 2014 judgment in *Digital Rights Ireland* (C-293/12 and C-594/12), the CJEU has been unequivocal about the need for non-trivial legal constraints on data collection (in that case, under Articles 7, 8 and 11 of the Charter of Fundamental Rights). In the 2016 cases of *Tele2 Sverige* and *Privacy International* (Joined Cases C-203/15 and C-698/15), and subsequent rulings, the Court crafted a reticulated, multi-tiered framework matching different objectives with different regimes for bulk data collection and retention.

Its April 2024 judgment in *La Quadrature du Net II* (C-470/21) extends this proportionality-oriented framework to the retention and sharing of IP address with Hadopi, a French public authority that "protect[s] works and subject matter covered by copyright or related rights against infringement" (para. 52). Hadopi used that data to identify the transmission of unlicensed material. The Court declined to find that a Charter violation in Hadopi's authorized access to, or use of, internet protocol (IP) addresses provided, *inter alia*, that such data was strictly partitioned from other bodies of data (including information about the work downloaded) that could be used to reveal sensitive personal information (e.g., "sexual orientation, political opinions, religious, philosophical, societal, or other beliefs", the so-called "special categories of personal data" of Article 9 of the EU General Data Protection Regulation (para. 110)).

To our eyes, the *La Quadrature du Net II* decision does not mark a sea-change in the CJEU's approach. The Court applied again a general principle that the intensity of the limitation of personal rights and freedoms has to mirror the seriousness of the interest put at risk, and the identification and categorization of what is "in-

tense". What is "serious" now has to be determined by the courts. Both the direct and the indirect impacts of this decision for privacy, we argue here, arise from interactions with other bodies of law and commercial practice related to data.

Assessing the marginal impact of mandatory disclosure

The effect of a novel mandatory retention and official access regime depends on the other ways in which covered entities already come into contact, and share data, with officials. Where those firms are already sharing user data (including perhaps IP addresses) with officials – whether voluntarily or pursuant to a legal mandate – the effect of such retention and sharing mandates will be diminished.

The French law at issue in *La Quadrature du Net II* was the Intellectual Property Code (or CPI). It applied to "[e]lectronic communications providers … and service providers". This covers firms that provide access to the internet for individual private consumers. The CJEU did not ask whether such entities are subject to any other legal regimes that might lead to the sharing of IP addresses with agents of a European state. The gap is puzzling. A proportionality analysis should logically take account of the way in which extant law already gives a (potentially bad intentioned) state actor a path to access such data.

In this regard, consider the effect of the 2024 Digital Services Act (DSA), which came into force on February 17, 2024 (i.e., two months before *La Quadrature du Net II*), upon the electronic communications providers covered by the CPI. The DSA's most well-known provisions concern its implications for very large online platforms. But these are not the only entities reached by that extensive and intricate legal measure.[1] Chapters II and III of the DSA impose new rules for many entities that likely rank also as

electronic communications providers. For instance, Article 18 requires hosting services to "promptly inform" the state of certain suspected criminal activities. The DSA also requires certain intermediaries to trace sellers on online marketplaces as a means to protect purchasers.[2]

While the exact scope and implementation of the DSA are a work in progress, it is hardly far-fetched to posit that the DSA's obligations will fall on some of the firms covered by the CPI, and that firms under the DSA will finds themselves in close and frequent contact with regulators. Article 18, for instance, envisages information sharing on an ongoing basis. Verifying compliance with the DSA regulators will also need top peer inside communications systems. Whatever the formal terms of the law, it would be very surprising if, in practice, this did not lead to *any* leakage from firms to officials, and did not lead to private-public relationships that could serve as effective springboards for informal cooperation.

If officials (especially bad intentioned ones) already have a way of accessing IP addresses and other data, are the CJEU's new constraints doing no work? The effect of the DSA on privacy is not necessarily a negative one, so there is no easy answer to this question. After all, perhaps officials' familiarity with how electronic communications providers structure and preserve their data creates a new or additional interest in finding ways to get data lawfully. That is, it may stimulate the problem to which the CJEU responded. But the interaction does underscore the oddity of evaluating risks to privacy in a vacuum.

There is a second way in which existing electronic communications practices interact with the privacy risks of the CPI. When packets of data are moved across the physical infrastructure of the internet, they are generally labeled with both the source and the recipient IP address.[3] According to Vadim Nikitin, some 70 percent

of this traffic flows through physical switches and data centers in the United States.[4] And, as Henry Farrell and Abraham Newman document, the U.S. has long taken advantage of its unique access to the physical infrastructure of the internet to access data without the permission of other sovereigns.[5] To our knowledge, such access is not constrained by the rules promulgated by the European Data Protection Board.[6] In practical effect, the security of IP addresses, which was the specific kind of data at issue in *La Quadrature du Net II*, turns on the nature of the relationship between a given European country and the U.S. national security apparatus. While it might seem that mere access to source and recipient IP addresses does not reveal a person's civil identity, we suspect that application of data-intensive AI analytic will often (perhaps almost always) allow accurate inferences about individuals.

Again, the reason to highlight this is not to undercut the CJEU's legal conclusions, but to point out how they might be enriched and complicated through contextualization. This underscores the threshold need for the CJEU to produce decisions that are more and more specific and provide some guidance.

The hidden regulatory ambition of the CJEU

Our observations so far have raised questions about the efficacy of the *La Quadrature du Net II* decision as a protection of privacy. In another respect, however, the decision has an unanticipated, even hidden force: It engenders a right against automated, machine decisions far beyond the scope of the extant European law concerning that right.

Explaining why requires some backtracking: One of the questions discussed by the CJEU was whether the CPI's retention mandates triggered a demand for "prior review" by a court or an inde-

pendent administrative body (para. 123). The Court's ruling on this point is complex. Not all applications of the CPI, it explained, involved serious violations of fundamental rights. Where they did, however, the CJEU held that prior review was required. In response to this threatened ruling, the French authorities had suggested that such review could be "entirely automated" because of the sheer volume of such instances (para. 147). The CJEU baulked at this suggestion. It directed instead that "in no case" could prior review be "entirely automated", since this would make it impossible to strike a "fair balance" in an individual case (para. 148). Eventually, the data subject has a right against a fully automated decision by the French government and a parallel right to a fair assessment from a human mind, able to contextualize and understand the full picture as a prerequisite to a balanced decision.

This ruling is striking because European law elsewhere considers the scope of such a right to a human decision (as it might be paraphrased), and does not extend it to these circumstances. Article 22 of the General Data Protection Regulation creates an individual "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". It explicitly limits that right, though, in several ways. One limit concerns instances in which a fully automated decision 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". That could include the CPI. If it does, the CJEU seems to have extended the Article 22 right to a human decision considerably further than its legislative specification. As such, it may be innovating beyond the available legislated materials in unexpected ways.

One of us has argued elsewhere that the Article 22 right to a human decision does not have sturdy normative foundations.[7] But that is beside the point here: More simply, the important observation is that in crafting new rules for privacy protection in the bulk retention and surveillance contexts, the CJEU may be engaging in legal innovations that run far beyond what written law imagines. Perhaps this is desirable, perhaps not. But the spillover effects of its *La Quadrature du Net II* are more complex than commonly appreciated – and require some contextual analysis in order to be excavated. Paradoxically, what seemed an innovation or a step back to those who only looked at the decision, can be analyzed as the specification of existing principles. What is really innovative are the subtle implications resulting from a *mise en perspective*, which is the interaction of the decision with other principles and bodies of law.

Another question is worth asking: if we consider the previously mentioned "intensity" of the limitation of personal rights and freedoms, how "intense" is sharing an IP address? More explicitly, how much does an IP address say about an individual? In this debate, it seems crucial to recall that not all personal data are equal. Some data, in fact, do not say much about the person. It does not allow immediate identification by the general public. We hence think it desirable that a clearer analysis be conducted of what, practically speaking, can be considered as "telling" personal data, seriously damaging one's freedom and reputation in case of disclosure. There certainly is a variability in the significance of personal data that alters the practical effects of disclosure and the possibility of identifying – and potentially damaging – an individual. The GDPR seems to hint to this gradual approach by referring to indirect identification (Article 4) and sensitive data (or special categories of personal data – Article 9). Furthermore, the safeguards

surrounding interfering measures (e.g. confidentiality obligations imposed on public agents) have to be weighed in when assessing how much an individual is in reality impacted.

Conclusion

We understand decisions such as *La Quadrature du Net II* best by locating them in a legal and socioeconomic context, considering how data protection rules exist and are applied in very practical contexts and how they should exist to protect individual rights, without ever sacrificing general interests. We have tried to show how this might be done, and how it could yield analytic payoffs and a better understanding of implications that, without appearing as immediate consequences, are powerful in their effects. We hope that these methods can be used elsewhere in respect to other important questions of European data privacy law. What seems much needed in our time is a constant contextualization and an ability to put things in perspective and in communication, without ever adhering to data protection orthodoxies that could, in the end, damage in far more serious ways the individuals whose privacy we want to protect.

References

1. European Commission – Press Release, 'Questions and Answers on the Digital Services Act' (23 February 2024), https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2348.
2. Moody's, 'Know Your Business – 5 Obligations Relating to the Digital Services Act' (23 February 2024), https://www.moodys.com/web/en/us/kyc/resources/insights/know-your-business-5-obligations-relating-digital-services-act.html.
3. OLCreate, 'Data Networks and IP Addresses ' https://www.open.edu/openlearncreate/mod/oucontent/view.php?id=129584&printable=1#:~:text=7%20Data%20networks%20and%20packet%20switching.%20You,webpage%20(without%20considering%20the%20action%20of%20NAT)..
4. Vadim Nikitin, 'Dadada' *London Review of Books* (21 November 2024), https://www.lrb.co.uk/the-paper/v46/n22/vadim-nikitin/dadada.
5. Henry Farrell and Abraham Newman, *Underground Empire. How America Weaponized the World Economy* (Macmillan, 2023).
6. European Data Protection Board, 'EDPB Clarifies Rules for Data Sharing with Third Country Authorities and Approves EU Data Protection Seal Certification' (3 December 2024), https://www.edpb.europa.eu/news/news/2024/edpb-clarifies-rules-data-sharing-third-country-authorities-and-approves-eu-data_en.
7. Aziz Z. Huq, 'A Right to a Human Decision' (2019) 105 *Virginia Law Review*.

Elif Mendos Kuşkonmaz

Of Minor Benefits and Major Costs

Reformulating the Fundamental Rights Question of the Privatisation of Surveillance in La Quadrature du Net II

Is general and indiscriminate data retention permissible under the EU fundamental rights framework? A decade has passed since the Court of Justice of the European Union (CJEU) was asked this somewhat oversimplified legal question. For a decade, different iterations of this legal question, be it about the various forms of data in question or the purposes for which data are retained, e.g. counter-terrorism, national security, or criminal investigations, have reached the CJEU repeatedly. Each iteration of a similar question revealed the increasing role of the private sector in law enforcement and the national security domain at the expense of protecting individuals' fundamental rights. The *La Quadrature Du Net II* (C-470/21) case adds a new formulation to the question: To what extent internet service providers can retain their users' IP addresses so that HADOPI (*Haute Autorité pour la Diffusion des Œuvres et la Protection des droits d'auteur sur Internet*) – the French administrative authority for copyright protection, can access the civil identity data linked to those addresses to issue sanctions? In answering this question, the Court tilts the metaphorical proportionality scale towards the interest of criminal investigations. The case outcome could contribute to the enlargement of privatised surveillance that rests on a generalised pre-emptive data retention scheme. The Court's findings could cement intrusive practices emerging from the counter-terrorism narrative to regular state practice at the expense of fundamental rights protection.

From hopeful beginnings to a cautionary future

Law enforcement authorities and security agencies praise communications data analysis as critical in criminal investigations and national security matters – so much so that states have tasked the electronic communication service providers, which hold the key to

the unsurmountable amount of data extracted from their users, with data retention obligations to ensure that the data will not be deleted when needed. The result is the collaboration between private sector actors and law enforcement authorities to prevent, detect, investigate, and prosecute crimes in a pre-emptive action model. Lines are thus blurred regarding accountability and oversight of data retention schemes resting on this collaboration.[1]

A decade ago, the CJEU's *Digital Rights Ireland* (C-293/12 and C-594/12) judgment and its following findings in *Tele2 Sverige* (C-203/15) were a ray of hope for strengthening fundamental rights against the pre-emptive and generalised data retention schemes. The Court was critical of the serious interference that such schemes cause to individuals' enjoyment of the rights to privacy and data protection as prescribed under the EU Charter – to the point that they served as the precedent to argue that the indiscriminate data retention schemes were precluded under EU law, for they lead to disproportionate interferences with those Charter rights.[2]

This tide around a robust fundamental rights discourse from the CJEU started to turn with its 2020 *La Quadrature Du Net I* (C-511/18, C-512/18 and C-520/18) and *Privacy International* (C-623/17) decisions, where it began to peel out the security objectives for which Member States may mandate retention of different types of data from communications service providers. A common legal issue in both cases was the applicability of EU law to the disputed national data retention legislation, which the French and the UK governments argued to be based on the national security carve out found in the EU Treaty (i.e. Article 4 (2) TEU) and specific EU legislation covering the data processing obligations of the providers of electronic communications services (i.e. the ePrivacy Directive, Directive 2002/58/EC). Had the Court concurred that the relevant national data retention legislation was outside the scope

of EU law, the duties of those service providers would have escaped its scrutiny, only to be subjected to national constitutional law and the European Convention on Human Rights (*La Quadrature Du Net I*, para. 103).

However, the legislation in question rested on the national security derogation under Article 15 (1) of the ePrivacy Directive, allowing the Member States to mandate that service providers retain communications data (including IP addresses) longer than the period required in the provision of their services (paras. 95-96 and 101). Obliging service providers to retain data by law interfered with the service users' rights to privacy and data protection (paras. 114-115). This legal mandate had to be proportionate to the aim it set out to achieve – protecting national security and combating serious crime (paras. 121-122).

The retention of IP addresses as a serious interference with the right to privacy

Even though this could have partially addressed the legal accountability issues surrounding statutory privatisation, where private sector actors are mandated by law to act in the interest of states' security objectives,[3] the criticisms focused on the proportionality analysis of different retention mandates and categories of communication data.[4] This retention mandate had to be proportionate to the interference it caused to the enjoyment of those rights. With its proportionality assessment, the Court dived into the different public security-related retention purposes, from the most serious one being national security interests to fighting serious crimes. The more intrusive a retention measure is, the more serious the public security purpose ought to be. The IP address, however, did not re-

veal the private lives of individuals as much as the other types of traffic data, only showing the owner of the terminal equipment (*La Quadrature Du Net I*, para. 152). Revealing the owner could be the only way to investigate the perpetrator of an online offence (para. 154), incentivising the legislator to mandate general and indiscriminate data retention to the internet service providers so that the information would be available beyond the period for which it is necessary for billing purposes (para. 155). Still, the IP address could be used to profile users' online activities (para. 153). To mitigate this possibility, legislation imposing a data retention obligation had to comply with certain conditions, primarily the aim to combat serious crime, prevent threats to public security, and safeguard national security (para. 156). A reverse reading of this finding would be that an objective of investigating non-serious crime does not justify the general and indiscriminate retention of IP addresses because of the disproportionate interference it causes with privacy and data protection rights.

In *La Quadrature Du Net II*, the CJEU did not concur with this potential reverse reading. It distinguished the disputed legislation based on its assessment that HADOPI had limited access to the retained data – it could only access the civil identity of the holder of the IP address. If, as the Court argued, there was no possibility to conduct profiling based on the retained IP addresses, the interference arising from the general and indiscriminate data retention could not be deemed "serious". With this lower threshold for rights interference, the Court was satisfied that the internet service providers could be mandated to retain all the IP addresses of their service users to combat "criminal offences in general" (para. 82), however minor they might be. This generalised statutory privatisation had to meet specific standards – but as welcome as the Court's attempt at limiting this indiscriminate surveillance was, the

standards it laid out seem to fall short of addressing the underlying logic behind it.

Oh, the principle of proportionality. Where are you?

Ultimately, those standards were geared towards ensuring that the interference will not be serious by preventing online profiling (paras. 86-90). Without that profiling, the cost to individuals' fundamental rights could be balanced against the benefit of data retention for investigating ordinary crimes. This approach, however, captures only a limited aspect of the impacts of the privatisation of surveillance in question.

The issue here is that this pre-emptive action does not consider the individual circumstances of each case, as the counter-terrorism and national security interests are purported to be driven by a zero-risk imperative. A generalised IP address retention scheme does not target specific people based on their involvement in alleged criminal behaviour. It covers everyone who uses the internet, notwithstanding their online behaviour. This leads to treating everyone as the perpetrator of a criminal offence – the access regime, despite the CJEU's findings on the contrary, does not yield as much protection without independent oversight. As for the proportionality test, on one side of the balancing scale is (even minor) crime prevention. On the other side are categories of interests other than freedom from online profiling, such as presumption of innocence and reasonable expectation of online anonymity. The Court, however, did not explore those interests and focused solely on online profiling. Different interests might require different levels of protection. Without this analysis, the retention of IP addresses was framed as a minor cost, while investigating ordinary crimes was deemed a significant benefit. A pre-emption logic found

in the counterterrorism and national security rhetoric seeped into ordinary crime prevention to the detriment of fundamental rights.

Moreover, this lowering of the protection of fundamental rights within the EU framework could also impact the protection of data transferred from the EU to third countries. In *Schrems I* (C-362/14) and *Schrems II* (C-311/18) the CJEU adopted a strict reading of the adequacy level the receiving country must afford for the incoming data, criticising its indiscriminate data retention schemes. Its findings in the *Schrems*-saga are more protective of personal data than its recent case law, the last of which is *La Quadrature Du Net II*. The CJEU's recent stance on the issue could potentially serve as leverage to turn down the concerns over the expansive surveillance powers of law enforcement and intelligence authorities in the UK when the European Commission reconsiders its adequacy decisions for UK laws protecting personal data in June 2025.[5] The compatibility of UK surveillance laws with the EU fundamental rights framework continues to be a live issue. As much as *La Quadrature Du Net II* might indicate that the CJEU case law on data retention keeps on evolving towards undoing the Court's former restrictive reading of permissible data retention, further issues linger as the UK plans to amend its data protection legislation. Human rights compatibility of UK surveillance laws are among many other problems that need to be reconsidered in evaluating the UK's adequacy status. Just like the CJEU's case law, nothing is settled.

References

1. Valsamis Mitsilegas, 'The Transformation of Privacy in an Era of Pre-Emptive Surveillance' (2015) 20:1 *Tilburg Law Review*.
2. For an analysis of the decisions see Edoardo Celeste, 'The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios' (2019) 15:1 *European Constitutional Law Review*.
3. For de Londras's concept of statutory privatisation see Fiona de Londras, 'Privatized Counter-Terrorist Surveillance: Constitutionalism Undermined' in Fergal Davis, Nicola McGarrity, and George Williams (eds.), *Surveillance, Counter-Terrorism and Comparative Constitutionalism*, (Routledge, 2013).
4. Valsamis Mitsilegas, Elspeth Guild, Elif Mendos Kuskonmaz, and Niovi Vavoula, 'Data Retention and the Future of Large-Scale Surveillance: The Evolution and Contestation of Judicial Benchmarks' (2022) 29:1-2 *European Law Journal*.
5. Maria Tzanou and Spyridoula Karyda, '*Privacy International* and *Quadrature du Net*: One Step Forward Two Steps Back in the Data Retention Saga?' (2022) 28:1 *European Public Law*.

Giulia Formici

The Long and Winding Road

The Data Retention Discipline in the European Union Between Judicial Intervention and Legislative Resistance

The April 30, 2024 judgments of the Court of Justice of the EU (CJEU) mark another key moment in the complex and long-lasting legal debate on mass data retention in the European Union. Starting from the analysis of these decisions, in this contribution I will show that, notwithstanding the CJEU's constant intervention and its efforts to map out a clear path towards a balance point between security needs and fundamental rights protection, the direction still appears confused. Moreover, the fragmented roads taken by Member States do not seem to converge to a final common destination. In this context, the Italian case represents a paradigmatic example of a persistent misalignment among the principles and requirements established by the CJEU case law on data retention and the legislative solutions adopted at the national level. This ultimately demonstrates the need for a decisive EU legislators' intervention, able to draw the future path of data retention regimes.

In fact, after the turning point determined by the CJEU's *Digital Rights Ireland* (C-293/12 and C-594/12) decision invalidating the 2006 Data Retention Directive (Directive 2006/24/EC), the only EU law provision addressing retention and access to metadata is represented by Article 15 of the ePrivacy Directive (Directive 2002/58/EC). This vague and vast discipline allows Member States to implement national legislations imposing the retention – for a specific time-period – of communications data. This exception to the general obligation to delete or anonymize metadata is allowed when it constitutes a "necessary, appropriate and proportionate measure within a democratic society" to safeguard national and public security, including the investigation and prosecution of criminal offenses.

Adapting the words of a splendid and melancholic The Beatles' song referred to in the headline, the cited provision and its interpretation in national contexts paved the way for the long and wind-

ing road of the data retention regime, that always led Member States to the door of the CJEU.

The CJEU road: the direction set by the case La Quadrature du Net II

The April 30, 2024 decision in the so called *La Quadrature Du Net II* (C-470/21) case dealt, once again, with a preliminary ruling actioned by the French Conseil d'État. It concerned, in particular, the interpretation of Article 15 ePrivacy Directive, read in the light of the EU Charter of Fundamental Rights, regarding a peculiar category of metadata deriving from electronic communications: IP addresses and civil identity data of users. Reaffirming its previous case law, in particular in *La Quadrature Du Net I* (C-511/18, C-512/18 and C-520/18) and *HK v. Prokuratuur* (C-746/18), the CJEU emphasized that the more serious the interference in fundamental rights of a data retention measure is, the more important the pursued aims must be, specifically national security or the combat against serious crimes. The Court went even further and outlined its requirements in detail. Depending on the category of data concerned as well as on the retention arrangements, the interference could be classified as limited and, thus, not require a serious purpose for its justification. This is the most innovative part of the decision: the judges entered not only in legal but also in IT technicalities by demanding national rules to ensure that IP addresses and civil identity data are kept "watertight", separated "by means of a secure and reliable computer system" (para. 87) as well as a regular review by a third-party authority (para. 126). Having these safeguards in place, a general and indiscriminate retention of these specific data categories does not allow precise conclusions to

be drawn about the private life of the persons in question (para. 92): Not constituting a serious interference, the bulk retention of IP addresses could therefore be imposed also for the purpose of combating criminal offences in general.

This interpretation seems to dampen the strong reject for bulk data retention expressed in the 2014 groundbreaking *Digital Rights Ireland* decision. Nonetheless, a closer look could reveal not a backtrack but, rather, a new step in a continuous process of refining the route, detailing the balancing exercise. The precise preliminary rulings' questions actioned by Member States allowed the Court to apply the necessity and proportionality principles to heterogeneous contexts and to better explain the initial jurisprudence. This seems to be confirmed by the more and more in-depth differentiations the CJEU proposed in its recent case law between national security and public security purposes, but also between targeted and bulk retention; quick freeze and general and indiscriminate retention; location data and IP addresses; serious and general criminal offenses.

The described approach can be identified also in another decision, released the same day of the *La Quadrature Du Net II* decision and focused more on the procedural guarantees concerning access to metadata: the *Procura della Repubblica presso il Tribunale di Bolzano* (C-178/22) case. This judgment is based on the request for preliminary ruling from the Tribunal of Bolzano – the first one concerning data retention coming from Italy and concluding with a CJEU decision – here, the Court reaffirms that, considering the allocation of competences, the definition of crimes' "seriousness" is in principle left to Member States. However, while they can consider social realities and specificities, the perimeter of "serious offenses" must comply with Article 15 ePrivacy Directive (read in light of the Charter). This provision cannot thus be distor-

ted by rendering the seriousness requirement "largely meaningless", so that "access to data becomes the rule rather than the exception". This important safeguard is confirmed by an additional guarantee: the prior review by a court or an independent administrative body. In fact, these authorities should maintain the power to refuse access to data if, in fact and notwithstanding the definition established by national law, the offence is manifestly not serious. This discretionary power ensures a more effective prior review, which could take into account the specific case and "the societal conditions prevailing in the Member States".

These two judgments enter in what can be defined a gradual "constitutionalization" path of mass surveillance elaborated by the CJEU.[1] This path aims at translating core constitutional principles into the data retention discipline and at introducing limits and safeguards. Nonetheless, the outlined road is not immune to criticism: the Court decisions suffer the specificities of the single case evaluated and the questions referred by national courts, as well as the vagueness – and the possible different interpretations – of some affirmations and requirements (e.g. how can we determine if the guarantees ensured make it "excessively difficult to identify effectively the perpetrator of a criminal offence", as the judges said?). Moreover, the very fragmented responses adopted by Member States[2] to the CJEU case law could concretely impinge on the effectiveness of the Court's efforts. The Italian example represents an interesting case study.

The Italian road: an inevitable shortcut?

The CJEU jurisprudence opened a reform debate[3] in several Member States[4] (*inter alia* Belgium, Germany and the UK[5] – before the Brexit), leading to the rediscussion of national data retention and

access regimes. Nonetheless, in Italy the political and judicial dialogue was almost non-existent. Italian courts mainly adopted "reassuring" interpretations of the supranational jurisprudence,[6] with the purpose of preserving the admissibility of relevant evidence in criminal proceedings. Only in recent times, particularly after the *HK v. Prokuratuur* decision, the legislative and judicial attention to national provisions' compliance with EU law – and particularly with CJEU principles – finally took off. In 2021, the Parliament approved significant modifications to Article 132 of the Privacy Code.[7] This controversial Article disciplines the retention obligation imposed on service providers as well as the access to metadata for security and investigative purposes. The 2021 reform introduced for the first time the judge's prior authorization for accessing metadata and the definition of serious crimes legitimizing the access by law enforcement authorities – offences punishable under national law by a maximum term of imprisonment of at least three years. Notwithstanding the introduction of more profound and unprecedented safeguards, the Bolzano Tribunal raised doubts on the compatibility of such provisions with the EU law, considering: i) that the threshold of "seriousness" covered also offences causing limited social disturbance; ii) that courts lack margin of discretion to refuse the authorization on the basis of an actual evaluation of the offence under investigation. The derived preliminary ruling, the above-analysed *Procura della Repubblica presso il Tribunale di Bolzano* CJEU decision, could lead to reinterpreting the current metadata acquisition discipline in Italy.

While belated guarantees have been introduced on the access side, it's worth underlining that the data retention regime remains still completely uncovered by legislative and judicial considerations. Notwithstanding the objections raised by the Italian Data Protection Authority[8] and several scholars[9], the current legislation

maintains a generalized and indiscriminate retention period of 72 months(!). In fact, Article 132 Privacy Code establishes a 24 months retention for telephone metadata and 12 months for internet metadata; however, the so called Legge Europea 2017[10] extended, in the aftermath of terroristic attacks in the EU, the retention period only with reference to the fight of specific serious crimes (i.e. terrorism, organized crime such as mafia). Since service providers cannot know in advance for what kind of offences law enforcement authorities would request access to data, they are *de facto* obliged to retain metadata for the longest time period of 72 months, thus transforming the exception into general rule.

Moreover, the data retention provision does not establish any form of targeted retention – i.e. geographic areas limitations – for the purpose of combating serious crimes and preventing serious threats to public security. This limitation could reveal inadequate to tackle crimes – such as mafia – not characterized by a limited area of intervention. Nonetheless, the Italian legislators and courts always avoided questioning the legitimacy of the bulk retention regime: this demonstrates a sort of reluctance towards the principles established by the CJEU and confirmed also in the *Spetsializirana prokuratura* (C-350/21) case. Such an approach seems to be based on the belief that solid safeguards concerning the access phase are sufficient to protect fundamental rights from unlawful and disproportionate acquisition of personal information, without considering the bulk retention as a per se severe intrusion in the private sphere.

A journey with a blurred destination?

During the last decade, the CJEU put significant efforts in determining the limits of mass data retention and access to

metadata. Nevertheless, the step by step – or case by case – path outlined by the Court does not yet reveal a clear destination. It is undeniable that the CJEU judgments prompted several Member States to adopt more rights-oriented legislative reforms, introducing new relevant safeguards. At the same time, attributing to EU judges alone the delicate task of mapping out the road towards a "constitutionalization" of mass surveillance practices does not represent a long-term and effective strategy.

The inevitable margin of interpretation and definitory powers left to Member States – also due to the peculiar EU institutional architecture – allowed the creation of a fragmented regulatory scenario: national solutions adapted only slowly, partially and reluctantly to the standards and requirements fixed by the supranational case law. The continuous dialogue between Member States and the CJEU, as well as national courts and supranational judges, often produced legal tensions, exacerbated by the clash between pro-security approaches (by law enforcement authorities) and data protection activists.[11]

In this context, the EU legislators cannot stay silent: On the contrary, they should come into play, promoting a serious regulatory debate and de-escalating dangerous polarizations. The divergent roads established by national policymakers should not necessarily converge. However, a harmonization in terms of shared basic principles and safeguards could finally help Member States navigating the layered CJEU case law as well as identifying viable concrete regulatory disciplines. Undoubtedly, attaining a political compromise able to comply with the high standards set by Court's decisions and, at the same time, to be accepted at the national level is, at this point, quite a hard task. And the recent advancements are not encouraging: on the one hand the debate on a new ePrivacy Regulation seems to be in a deadlock.[12] On the other hand, the ser-

ious concerns expressed by the EDPB on the last available Regulation's draft show the attempt of several States to water down and rediscuss the CJEU case law's principles.[13] A trend that seems to be confirmed by the affirmation of the EU High-Level Group on access to data for effective law enforcement.[14]

In this scenario, the long and winding data retention road that leads Member States to the CJEU door will probably never disappear, taking up once again The Beatles' song. And the stakes are high, especially in a context characterized by technological advancements that made reality the creation of biometric data scraping on the web, social scoring systems and emotion recognition based on vast retention and processing of personal data. As Rodotà strongly highlighted, "we may believe that we are only discussing data protection; in fact we are dealing with the destiny of our social organisations, their present and – above all – their future".[15]

References

1. Edoardo Celeste and Guilia Formici, 'Constitutionalizing Mass Surveillance in the EU: Civil Society Demands, Judicial Activism, and Legislative Inertia' (2024) 25:3 *German Law Journal*.
2. Eleni Kosta and Irene Kamara (eds.), *Data Retention in Europe and Beyond: Law and Policy in the Aftermath of an Invalidated Directive* (Oxford University Press, 2025).
3. Marek Zubik, Jan Podkowik, and Robert Rybski, *European Constitutional Courts Towards Data Retention Laws* (Springer, 2021).
4. Valsamis Mitsilegas, Elspeth Guild, Elif Mendos Kuskonmaz, and Niovi Vavoula, 'Data Retention and the Future of Large-Scale Surveillance: The Evolution and Contestation of Judicial Benchmarks' (2022) 29:1-2 *European Law Journal*.
5. Matthew White, *Surveillance Law, Data Retention and Human Rights A Risk to Democracy* (Routledge, 2024).
6. Luca Lupária, 'Data retention e processo penale: un'occasione mancata per prendere i diritti davvero sul serio' (2019) 4 *Diritto di Internet*.
7. Gazzetta Ufficiale della Repubblica Italiana, 'Codice in materia di protezione dei dati personali' (No. 196), 30 June 2003.
8. Garante per la protezione dei dati personali (GPDP), 'Segnalazione sulla disciplina della conservazione, a fini di giustizia, dei dati di traffico telefonico e telematico' (2 August 2021), https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9685978.
9. Giulia Formici, '"The Three Ghosts of Data Retention": passato, presente e futuro della disciplina italiana in materia di conservazione e acquisizione dei metadati per scopi investigativi. Commento a margine del d.l. 30 settembre 2021, n. 132 e relativa legge di conversione' (2022) 1 *Osservatorio AIC*.
10. Gazzetta Ufficiale della Repubblica Italiana, 'Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea - Legge europea 2017' (17G00180), 12 December 2017.
11. Arianna Vedaschi, '"Customizing" *La Quadrature du Net*: The French Council of State, National Security and Data Retention' (2021) *Brexit Institute Blog*.
12. European Union, 'Procedure 2017/0003/COD: Proposal for a Regulation Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' (2025) https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52017PC0010.
13. European Data Protection Board, 'Statement 03/2021 on the ePrivacy Regulation' (9 March 2021), https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-032021-eprivacy-regulation_en.

14. European Commission, DG for Migration and Home Affairs, 'High-Level Group (HLG) on Access to Data for Effective Law Enforcement' (22 November 2024), https://home-affairs.ec.europa.eu/networks/high-level-group-hlg-access-data-effective-law-enforcement_en.
15. Stefano Rodotà, 'Privacy, Freedom, and Dignity Conclusive Remarks at the 26th International Conference on Privacy and Personal Data Protection' *Garante per la protezione dei dati personali (GPDP)* (13 September 2004), https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1049293.

Chiara Graziani

Data Retention in a Cross-Border Perspective

Latest Insights from the European Union and the United States

As widely known, the retention of metadata constitutes an essential tool in the context of the fight against terrorism and, more broadly, serious crime. This analysis focuses on a comparison between two "giants" under the perspective of metadata retention for security purposes, i.e. Europe and the United States, and highlights some challenges that arise therefrom.

To look at recent developments, on 30 April 2024, the European Court of Justice (ECJ) has ruled again on metadata retention in *La Quadrature Du Net II* (C-470/21). The Court determined that, although metadata retention cannot be set aside as it is pivotal to ensure well-working preventative strategies against transnational crime, further guarantees need to be ensured, e.g. keeping IP addresses separated from civil identity data. Hence, it appears that the European Union (EU) is increasingly affirming itself as the main actor in the tricky balance between security, on the one hand, and human rights – such as privacy and data protection – on the other.

However, metadata retention is useful and effective only insofar as similar measures and standards are adopted throughout as many countries as possible. Specifically, it is essential that at least the "two sides" of the Western world, namely Europe and the United States, ensure well-working cooperation and similar levels of protection in this concern. Hence, a comparison between the two is very useful in order to make some considerations on this point.

The European scenario: An endless fight between the ECJ and national lawmakers

In the EU context, the ECJ has repeatedly ruled on metadata retention, not only with the landmark decision *Digital Rights Ireland*

(C-293/12 and C-594/12) in 2014 and subsequent judgments, such as *Tele2 Sverige* (C-203/15) in 2016, but also with the more recent *La Quadrature Du Net II* judgment (2024), mentioned above. In these rulings, like in other ones addressing other aspects of the balance between security and privacy rights (e.g., Opinion A-1/15, issued in 2017 and concerning the collection and retention of Passenger Name Record data), the Luxembourg Court has taken a progressively more realistic and pragmatic stance, as remarked by scholars.[1] As a matter of fact, through the time the Court has validated mass surveillance and accepted it as a *conditio sine qua non* to be introduced in any public security strategy. Yet, the judges have not renounced to reaffirm safeguards that, particularly if one looks at the recent decision, are framed in a more and more technical and precise way, taking into account even refined technicalities, as remarked by Formici's analysis in this book.

Against this background, domestic lawmakers seem not to be convinced that a balanced attitude in the security vs. privacy conundrum is the way to go: Many of them – Italy, with its 72 months retention period, is a patent example – rely on metadata retention regimes that are at least dubious – to use an euphemism – from the perspective of the principles enshrined in the ECJ's case law concerning surveillance.

This holds true not only for EU Member States. In fact, even if one looks at countries that are formally outside the EU, but play a relevant role in the European scenario, the situation is worrying. Let us just consider the United Kingdom (UK) – no longer an EU Member State, after Brexit, but surely an essential actor in the keeping of security. The UK, in spite of several supranational decisions sanctioning or condemning some aspects of its surveillance schemes (see, e.g., the *Big Brother Watch and Others v. the United Kingdom* judgment (Appl. nos. 58170/13, 62322/14 and 24960/15)

by the European Court of Human Rights and the *Privacy International* judgment (C-623/17) by the ECJ), keeps quite worrisome bulk of interception provisions under the Investigatory Powers Act 2016 c. 25.[2] For instance, rules on court authorizations are poor and the provisions on foreign surveillance are drafted very widely, so as to leave discretion to governmental authorities as to their scope.[3]

In sum, a quite divisive situation exists in Europe. Courts, especially the supranational ones, try to guarantee a well-thought-out attitude. Lawmakers, instead, give crucial importance to the security side of the binomial, and consequently they do not renounce to bulk and indiscriminate surveillance, including but not only through the use of communication metadata. Nevertheless, the very existence of such a dialogue (or maybe it would better be defined as a tug-of-war) between courts and lawmakers is a sign of sound "counter-limits" to the action of political bodies that, by their very nature, tend to be inclined towards security when it comes to the protection of their citizens and institutions.

The US scenario: A driver for the lowering of standards?

In the United States, the starting point in the field of the relationship between security and rights as privacy and data protection is very different from the European one. This is due to several factors that are inherent in the US legal system, the pertinent legal framework, as well as legal culture.

First, the Fourth Amendment – from which privacy rights are inferred – is deemed to be recessive when other needs are at stake, among them is security. If one considers the interpretation given by courts, the circumstances where warrants can be excluded or re-

duced are almost more than the ones where they are considered essential.[4]

Second, and related to the above-mentioned aspect, the well-known third-party doctrine, according to which a person has no reasonable expectation of privacy when he/she voluntarily shares information with others. This doctrine allows an almost full "liberalization" of data that individuals give to a variety of entities, and the jurisprudential stance on this doctrine is still quite consolidated, with few to no exceptions.

Third, when the tech industry is involved – like in the case of metadata surveillance, since cooperation of communication service providers with public authorities is central – the United States tend to embrace a very "libertarian" stance, more oriented towards the market than towards the protection of users' rights. This is manifest, among others, in the scarce regulation of the technology market in general, which then results in self-regulation by the industry.

All these features are clearly visible in the context of metadata retention. Not only were the United States among the pioneers of this practice, with the controversial Section 215 of the 2001 USA Patriot Act, extended several times and then incorporated into the USA Freedom Act in 2015; they also passed the Cloud Act in 2018, according to which US federal authorities can access the data stored by any US company, among others for the purpose of crime prevention. In effect, the Cloud Act applies extra-territorially, since there is no need that the company's servers are based in the United States.

At the same time, US courts have not taken firm stances against indiscriminate metadata retention carried out without strong guarantees. Indeed, the federal Supreme Court, when called to rule on access to communication metadata, remanded the case back to the lower court to be dismissed (see the 2018 *Microsoft Corp. v. United*

States[5] judgment, referred to a case originated before the enactment of the Cloud Act but settled shortly after the Act had been published).

Thus, in contrast to the European scenario, the US context does not see a strong role of courts trying to contain the drifts of the lawmakers, which, as a consequence, become significantly more worrying than on the European side. Additionally, recent electoral results in the United States might bring to an even more concerning situation.

Moreover, given the extra-territorial effects of metadata retention, but also of the fight against terrorism, which is a transnational crime, the implications of the US legal regime on cross-border standards of privacy protection are noteworthy. While the European system is more protective, there is indeed little to do when US law enforcement authorities request access to metadata on European servers based on the more intrusive US laws. It is true that also EU standards apply extra-territorially and the Brussels effect has its own weight. The Brussels effect can be defined as the influence of EU law even outside of the EU borders, implying that also non-EU countries may end up having to comply with EU norms due to the necessity to keep relationships with EU countries.[6] Nevertheless, given the significance of the United States on the technology market, the prevalence of its (legal) standards based on its market position is not to be excluded and would need to be opposed, e.g. through strong courts' stances in favor of privacy, in order to restore a well-balanced global context.

Some concluding considerations

The presented background is not intended to give a totally pessimistic vision, arguing that human rights standards will neces-

sarily be reduced due to the economic predominance of the United States. Rather, the analysis warns against the risk of a sort of "reverse Brussels effect", and claims that efforts should be made to avoid that the economic power of the United States brings to a lowering of privacy standards when it comes to metadata surveillance. In order to do so, European authorities should engage in careful and in-depth review of the standards adopted in the United States – and in any other third country with which the EU exchanges data. The recent review by the EU Commission on the implementation of the US Data Privacy Framework (DPB) seems to go in this direction.[7]

On a more institutional note, this comment shed light on how essential the role of courts is in the striking and keeping of a balance between security, undeniable to ensure the survival of our societies, and human rights, essential if such societies are willing to be considered as "democratic".

References

1. Arianna Vedaschi, 'Privacy and Data Protection Versus National Security in Transnational Flights: The EU-Canada PNR Agreement' (2018) 8:2 *International Data Privacy Law*.
2. Ian Leigh, 'National Security Surveillance in the United Kingdom' *Safe and Free* (14 November 2023), https://safeandfree.io/wp-content/uploads/2023/11/UK_Surveillance_FINAL.pdf.
3. For the potential effects of the recent ECJ jurisprudence on data transfers to the UK, see the contribution by Elif Mendos Kuşkonmaz in this book.
4. Justitia: US Law, 'Warrantless "National Security" Electronic Surveillance' https://law.justia.com/constitution/us/amendment-04/30-warrantless-national-security-electronic-surveillance.html.
5. Supreme Court of the United States, *United States v. Microsoft Corporation* (584 U.S. __, 138 S.Ct. 1186), Judgment of 17 April 2018.
6. Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press, 2020).
7. Data Privacy Framework Program, 'Data Privacy Framework (DPF) Overview' https://www.dataprivacyframework.gov/Program-Overview#:~:text=The%20Data%20Privacy%20Framework%20(DPF,%2DU.S.%20DPF%2C%20and%2For.

André Bartsch, Johanna Fink, Jakob Mutter, Marc André Bovermann, Isabelle Weiss

Testing the Waters of Private Data Pools

How a General Surveillance Account Could Cover Privately Collected Data

Nowadays, data is mostly collected not by state actors but by businesses. To make use of the data amassed by these companies, law enforcement authorities often oblige them to hand over their records. To ensure that the companies actually collect (and do not delete) the most useful data for these authorities, legislators have put retention obligations into place. However, only very specific data is subject to such retention, while most data is stored by companies due to their own economic interest. For the purposes of a general surveillance account, this begs the question if data collected by state actors (such as airline passenger name records [PNR][1]) should be treated differently. While many are concerned with the latter, the potential threats these private data pools pose for the exercise of fundamental rights are often overlooked. In any case, a general surveillance account requires more empirical data on the exercise of surveillance powers in order to provide a complete picture of the level of surveillance in a society.

Preventing total surveillance

The recent CJEU decision *La Quadrature Du Net II* (C-470/21) on data retention has brought back some peoples' dream of data retention obligations for telecommunications traffic data.[2] The German history of data retention goes back more than 14 years: In its 2010 data retention judgment, the German Federal Constitutional Court held traffic data retention to be generally permissible[3] – the caveat being very strict thresholds for the laws governing the retention. One of the requirements that follows from the judgment is what is dubbed an "Überwachungsgesamtrechnung" (hereafter "general surveillance account"). According to the judgment, such an account entails that the German parliament needs to consider already existing data collection procedures before enacting new

mass data collection measures. The court deemed this necessary to prevent an Orwellian dystopia where the government is able to capture all the activities of citizens.[4] In the aforementioned 2010 data retention judgment, the German constitutional court considers this prohibition of total surveillance to be part of the constitutional identity which not even EU legislation can supersede.[5] Thus, the general surveillance account is necessary to ensure the persistence of Germany's constitutional identity. In a time where private actors have amassed some of the largest data pools, this begs the question what it takes for the general surveillance account to adequately consider private data pools.

Since 2010, the general surveillance account has emancipated from this specific context to be a tool to assess surveillance measures conducted by German security authorities more generally.[6] A general surveillance account should feature a normative evaluation of the relevant surveillance measures alongside an empirical survey.[7] The normative dimension allows for an assessment of the possible intensity of a measure, while the empirical evaluation aims at assessing their intensity in practice, i. e. how often the relevant measures were conducted. Both are essential to account for the general level of state surveillance in a society.

Whether the data was collected because of a retention obligation could be an important factor for determining the possible intensity of a measure, i. e. the normative evaluation. This question explicitly extends to all kinds of data pools, even though the public discussion is often focused on telecommunications traffic data retention alone.[8] Especially with the rise of social media, data collected by online platforms has grown to be more and more important to law enforcement authorities.[9]

In order to examine how a general surveillance account can account for private data pools, we will first examine the types of data

the concept of "data retention" encompasses. Next, we take a critical look at whether it is justified not to treat private data pools as data retention. Lastly, we analyse what needs to be done to enable an effective general surveillance account, accounting for private data pools.

It's not just telecommunications data

In the German context, the term "data retention" or "Vorratsdatenspeicherung" refers to the precautionary storage of personal data concerning telecommunications traffic without a specific indication. If necessary, the stored data might be used at a later date for purposes not yet foreseen. This is due to the fact that the German constitutional court developed its jurisprudence on the matter in its 2010 judgment mainly against the backdrop of telecommunications traffic data retained by service providers as required by the law transposing the Data Retention Directive 2006/24/EC.[10] However, even in this judgment, the court held that telecommunications traffic data retention could pave the way for further pre-emptive data collection,[11] thus recognising that data retention in other fields is conceivable. Bearing this in mind, it is not surprising that also the CJEU often refers to its own decisions on PNR data in its rulings on data retention (see e.g. *La Quadrature Du Net I* (C-511/18) paras. 115 seq., 130 seq.).

Indeed, in practice, data is also retained in other fields and by other means. Examples include customer and usage data stored by digital and postal services providers for operational purposes, which can be requested by law enforcement authorities under certain circumstances (e.g. Sec. 40 para. 2 and Sec. 50 para. 2 of the German Federal Criminal Office Act), as well as PNR data and financial data, which are collected by airlines or banks respectively

and transmitted to the designated national data processing authority (e.g. Sec. 2 of the German Passenger Data Act and Sec. 24c of the Banking Act). Therefore, a general surveillance account must also consider those other kinds of privately gathered data.

Public and private data retention

The pivotal point of the debate around data retention is the obligation of private actors to store certain data. The mere storage already constitutes an interference with fundamental rights, such as Articles 7 and 8 CFR, Article 8 ECHR as well as Article 2 sec. 1 and Article 1 sec. 1 German Basic Law. Additionally, the fundamental rights of a person are also affected when data is retrieved by law enforcement authorities.

Data retention obligations could therefore indeed increase the intensity of surveillance on an individual. As a result, the laws governing the retrieval of data from data pools for which data retention obligations exist (e.g. telecommunication service providers, cf. Sec. 172 (1), 176 German Telecommunications Act) could be considered more intense than those governing the retrieval of data from services where there are no retention obligations, e.g. digital services providers. The latter ones only store data for their own purposes.

When data retention obligations exist, the state can assume that the relevant data is stored, and it can reliably access the data at any time. This differs from an – from the state's point of view – "arbitrary" retention of data by digital services providers for commercial purposes.

However, taking big social media platforms and search engines into account draws a different picture. Most of these services store customer data in their own economic interest.[12] In some cases, the

data might be necessary to operate the company. For example, Netflix stores user data for billing purposes[13] and Facebook stores it to display it to other users and run advertisements.[14] In others, the data has an economic value, as it can be sold and data dominance also means market power.[15]

In these cases, the state authorities can rely on the fact that the providers store data on a large scale. Digital services providers are also likely to store more data than telecommunications providers and instead of a few months, as provided for in the time limits of Sec. 172 of the German Telecommunications Act, the data is often stored for several years.[16]

This means that even when digital services store data only for their own interest, law enforcement authorities can still access this data at virtually any time. In the end, the retention of data by digital services is just as intense for the individual as the retention of data by telecommunications providers.

However, other digital services have made privacy their business model (like Signal) and only store data which is absolutely necessary for the service. In these cases, law enforcement authorities can only access little to no data without retention obligations. Consequently, only when data retention obligations are in place can law enforcement authorities expect a minimum amount of data.

Assessing surveillance requires empirical data

Common to the different kinds of data retention is that access to stored data by law enforcement authorities touches upon the fundamental rights of the data subjects. Be it as a retrieval of privately stored data or as a change of purpose when accessing data stored by state authorities, the access to data constitutes a new interfer-

ence. Data retention in itself does not create additional knowledge for law enforcement authorities, but data access does. It is therefore essential that a general surveillance account focuses on data access. However, the (generally) increased quantity and quality of data can be accounted for with a higher intensity scoring of the relevant measures when performing the legal analysis of surveillance powers.

Next to the normative analysis, the general surveillance account still requires – as explained above – empirical data on the frequency of data access in order to provide a full understanding of the total amount of surveillance in society.[17] Quantitative data on surveillance powers is quite scarce, however. While there are reporting obligations for certain forms of surveillance – e.g. Section 101b of the German Code of Criminal Procedure requires reporting on telecommunication monitoring – there are significant gaps in the reporting requirements for many other measures. Constitutional jurisprudence by the German Federal Constitutional Court explicitly requires reporting obligations only for specific measures that interfere with fundamental rights in a particularly intense manner.[18]

A call for more empirical data about surveillance measures

This line of jurisprudence requires some revision in light of the general surveillance account. Without sufficient empirical data it is impossible to create a meaningful image of the total amount of surveillance within a society. The concept of measuring the extent of surveillance is derived from the constitutional imperative of preventing the total monitoring of society.[19] In a series of rulings, the Federal Constitutional Court has held that surveillance powers must be coordinated in a way that prevents one person from be-

coming the subject of complete surveillance through the exercise of powers by different law enforcement and intelligence authorities.[20] This concept can be extended to the broader context of the general surveillance account, which is also based on the idea of preventing total surveillance. It is the responsibility of the state to coordinate all surveillance powers in order not to exceed the permittable level of surveillance in a society.[21] As previously stated, this requires not only a normative analysis but also a quantitative analysis of the exercise of surveillance powers. Currently, this coordinative duty cannot be fulfilled with the available empirical data.

It is the shared responsibility of the legislator and law enforcement authorities to ensure compliance with constitutional requirements.[22] Consequently, the legislator should introduce more reporting obligations for the exercise of surveillance powers and security authorities should – proactively – improve their internal monitoring of the exercise of competencies. Based on such a solid empirical foundation, a complete general surveillance account becomes possible.

References

1. See Directive (EU) 2016/681. On the Use of Passenger Name Record (PNR) Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime, 27 April 2016.
2. See the contribution by Joachim Herrmann in this book.
3. German Federal Constitutional Court, (1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08), Judgment of 2 March 2010.
4. German Federal Constitutional Court, (1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08), Judgment of 2 March 2010, para. 211 et seq.
5. German Federal Constitutional Court, (1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08), Judgment of 2 March 2010, para. 218.
6. Bundesministerium der Justiz, 'Startschuss für die unabhängige wissenschaftliche Untersuchung der Sicherheitsgesetze (Pressemitteilung Nr. 2/2024)' (10 January 2024), https://www.bmj.de/SharedDocs/Pressemitteilungen/DE/2024/0110_Ueberwachungsgesamtrechnung.html.
7. Ralf Poscher and Lukas Landerer, 'Überwachungsbarometer für Deutschland – Ein Modellkonzept' *Friedrich-Naumann-Stiftung für die Freiheit* (26 January 2022), https://shop.freiheit.org/#!/Publikation/1168.
8. As already observed by Ralf Poscher and Michael Kilchling, 'Zwei Jahrzehnte nach 9/11 – Höchste Zeit für ein empirisch basiertes Monitoring staatlicher Überwachungsmaßnahmen' (2022) *Verfassungsblog*.
9. Matthias Becker, 'Fundgrube für Fahndungsdaten: Wie die Polizei soziale Netzwerke nutzt' *Deutschlandfunk* (26 May 2018), https://www.deutschlandfunk.de/fundgrube-fuer-fahndungsdaten-wie-die-polizei-soziale-100.html.
10. Bundesgesetzblatt (Nr 70/2007), 'Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG' (21 December 2007).
11. German Federal Constitutional Court, (1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08), Judgment of 2 March 2010, para. 218.
12. Meta, 'Privacy Policy' (14 November 2024), https://www.facebook.com/privacy/policy/.
13. Netflix Services Germany GmbH, 'Privacy Statement' (17 April 2024), https://help.netflix.com/en/legal/privacy.
14. Meta, 'Privacy Policy' (14 November 2024), https://www.facebook.com/privacy/policy/.

15. Bennett Cyphers, 'Google Says It Doesn't "Sell" Your Data. Here's How the Company Shares, Monetizes, and Exploits It.' *Electronic Frontier Foundation* (19 March 2020), https://www.eff.org/de/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and.
16. Meta, 'Privacy Policy' (14 November 2024), https://www.facebook.com/privacy/policy/.
17. Ralf Poscher and Michael Kilchling, 'Zwei Jahrzehnte nach 9/11 – Höchste Zeit für ein empirisch basiertes Monitoring staatlicher Überwachungsmaßnahmen' (2022) *Verfassungsblog*.
18. German Federal Constitutional Court, *Bestandsdatenauskunft II* (1 BvR 1873/13, 1 BvR 2618/13), Order of 27 May 2020.
19. German Federal Constitutional Court, (1 BvR 966/09, 1 BvR 1140/09), Judgment of 20 April 2016.
20. German Federal Constitutional Court, (2 BvR 581/01), Judgment of 12 April 2005; German Federal Constitutional Court, (2 BvR 543/06), Judgment of 11 May 2007; German Federal Constitutional Court, (1 BvR 966/09, 1 BvR 1140/09), Judgment of 20 April 2016; German Federal Constitutional Court, (2 BvR 916/11, 2 BvR 636/12), Judgment of 1 December 2020.
21. German Federal Constitutional Court, (1 BvR 966/09, 1 BvR 1140/09), Judgment of 20 April 2016.
22. German Federal Constitutional Court, (1 BvR 966/09, 1 BvR 1140/09), Judgment of 20 April 2016.

Thomas Christian Bächle

New Media, New Data and a Dark Foreboding

Surveillance as Observation, Simulation, and Weapon

The last two decades have seen major changes in surveillance practices; there has been a shift in focus from state power and control to big tech corporations and monetisation. What we are currently witnessing is yet another shift, which is establishing surveillance practices as a means of hybrid warfare. Surveillance can be used as a weapon, and not just in military contexts. The AI-driven vision of accessing what people think and feel might seem harmless in comparison, but it may turn out to be a much more powerful sword.

Surveillance practices old and new

From the 18th century, surveillance was a mainly a state-run endeavour, utilised for administrative purposes, to exercise control and power. Previous surveillance technologies were limited by today's standards, as not every action was photographed or filmed, not every conversation recorded. Part of its efficiency was derived from a nimbus of perceived pervasiveness, a variation of the panopticon effect that today is framed as a "chilling effect" in legal discussions: you did not know if there was someone listening in on your phone call, but the possibility that someone *could potentially* be listening made you already change your behaviour.

With the astonishing rise of digital platforms, there has been a considerable shift in surveillance practices: who does it, how do they do it, and why?[1] Large corporations offer services that produce data sets that are in turn used for monetisation. The power dynamics heavily favor a form of surveillance-based capitalism. Search engines, content-providing platforms and social media – each step that is taken on there is constituted in data and leaves data behind. As more and more parts of our lives are constituted by and lived within data, this type of surveillance is almost all-encompassing.

Its main objective is not, in essence, political; the power exercised over users lies in the extraction of data and the manipulation of behaviours with the ultimate goal of making money.[2] Despite being aware that all communications are recorded and analysed, the majority of people accept it, ignore it or see a greater benefit in the free services they consume.

Of course, states are keen on obtaining this data, as it is information that is so available and tempting. Proposals by EU policy-makers to make providers automatically analyse messenger data in order to scan for illegal content is one recent example of this desire.[3] In light of more general drift towards democratic backsliding that can be observed in the US and EU member states, the combination of universal datafication, the targeting of individuals and the dissolution of the state/corporate boundary in times of autocratic tendencies seems like quite the dark triad of surveillance practices.

Weaponising surveillance

This dark triad points to yet another shift, the weaponisation of surveillance. Pegasus, a spyware tool offer by the Israel-based NSO Group, describes itself as offering cyberintelligence to help governments fight terrorism and crime. In practice, it works by infiltrating an individual phone – for example, via messenger services – enabling the spyware to harvest any data that is produced (contacts, communications, contents). Even though it is marketed as a tool to prevent or investigate terrorism and crime, this type of intelligence gathering can be used for targeted attacks against individuals for political gain. Using knowledge about individuals – such as journalists or political opponents – to threaten or blackmail them is an effective and low-effort strategy for weaponising

surveillance. Rather than running their own intelligence efforts, state actors and agencies have found themselves in the role of customers of private companies that offer their exclusive spying services to them. Given that, in democratic systems, this is being conducted under the label of fighting crime and countering terrorism, these highly invasive measures can happen largely outside of legal oversight.

This is even more so the case when digital surveillance is used in open conflicts for automated information gathering and target selection, as it is reportedly being done in Russia's aggression against Ukraine as well as in the Israeli strikes against Gaza following the Hamas attacks on October 7, 2023. According to journalistic accounts, Israel's Lavender system reportedly used surveillance data to identify terrorists and Hamas operatives.[4] To take another example, the Palantir system – as envisioned and promoted by the company – promises a natural language interface that aggregates all available data to boost situational awareness in conflicts, to analyse the possible and most effective courses of action, and to make corresponding recommendations. Some of this functionality is being used and applied in Ukrainian efforts against the Russian invaders.

In more abstract terms, these practices of weaponised surveillance are also rooted in the platform-derived techniques of datafication, profiling, targeting and recommending. The core difference, however, is that the probabilistic score does not denote potential customers or users who are susceptible to ads, but enemy combatants or terrorists. The data-rich networked and platform-based type of warfare is reflective of what goes under the label of hybrid warfare. What often gets overlooked is that this hybridity also entails a dissolution of established conceptual boundaries: Are the actors state, private or corporate ones? Are they mil-

itary or civilian? What about the use of technologies? And, above all: At what point are nations at war with each other? How can we still discern this most blurry line?

Expanding the purposes and objects of surveillance

These blurring boundaries also change the foundation of what surveillance practices are or entail. Take, for example, the idea of "autonomous weapons", often simply envisioned as killer robots or, in more nuanced approaches, as unmanned vehicles, equipped to select and engage targets without human intervention. When the conceptual basis for surveillance is conceived of as a combination of data collection, automated data analysis, pattern recognition and recommended actions as described above, yet another boundary becomes blurry: Are we dealing with a relatively innocent practice of information gathering or intelligence, or should these types of surveillance rather be understood as an "autonomous weapon" in their own right, as the step from recommendation to actual decision can be quite a small one?

The changing purposes of surveillance have been accompanied by an increasing expansion of the objects of surveillance.

The first expansion is rooted in the belief that the future can be observed in the present. Observation practices such as intercepting phone conversations or video surveillance are based on the pretty straightforward notion of seeing what people actually do. Techniques such as profiling and probability-based extrapolations of likely future behaviours create the idea of observing what has not happened yet. In other words, *surveillance becomes simulation*. It no longer just looks at simply the things that people do – their actual movements, search queries, contacts and communications. It is concerned with what people will, it is assumed, likely do in the

future based on the statistical proximity to particular groups conveyed by certain markers, such as affiliation with the purely mathematical-fictional unit of "persons who behaved similarly in the past". As a side effect, the individual is no longer the undividable object of surveillance. What is under surveillance is an individual's complex entanglements with a profile: the in-dividual is split into identity markers such as gender, race or age, group affiliations of behavioural patterns.

The second expansion is based on developments in media and interface technologies that sell the idea of accessing what people think and how they feel. When using and navigating our smart phones, smart speakers, smart homes or smart watches, we are no longer limited to purely text-based interactions. We use our voices, gestures and facial expressions – and in doing so we inadvertently help produce unprecedented amounts and types of data. In allowing more direct interactions, the new interfaces access knowledge on social dynamics or emotional states by tracking natural language, non-verbal interactions with the machine and with each other while the device conveniently keeps on recording couple or family dynamics. Applications such as avatar friends or bots specifically target our social and emotional needs – and in doing so elicit more and more data in these areas.

Besides the idea of observing future behaviours, the aggregation and analysis of data that seemingly captures the social and emotional realities of those surveilled, promotes a fairly recent technological imagination: observing the inside of people's minds – emotions, attitudes, beliefs – accurately (a recurring imagination if you look at the historical example of the polygraph[5]). The consequences of this development are becoming particularly noteworthy and consequential in the field that brands itself as emotion analytics.

A dire premonition: The surveillance of what people think and feel

The premise of so-called affective computing and emotion analytics is to make human affect and emotion machine-readable in an effort to improve human-machine interactions by paying particular attention to those elements that also play a huge role in communication and interactions between humans. Gestures and movements of the body, facial expressions or speech patterns in natural language use are converted into computable data sets. The use of anthropomorphic design elements, interactive bots or human-like social robots offer interfaces that cue humans to make more use of non- and paraverbal modes of communication. While these goals underline particular functional benefits in human-machine interactions, emotion analytics and affective computing – when combined with the shifting of the surveillance practices discussed above – also induce a sense of foreboding.

As we have seen, surveillance as simulation does no longer limit itself to what people actually do but what they are virtually about to do in a probabilistic future. Computing affect and emotion creates a surveillance practice that expands to human thoughts and feelings. At least, this is the promise of emotion analytics. In reality, it further dissociates the object of surveillance, its referent, from the surveillance technique that claims to make it visible. The reason for this is that the epistemological foundations for the analysis of emotions are highly questionable. In many cases, they rely on a particular dictionary of emotions that is able to translate what can actually be observed into the corresponding mental states behind this symbolic code. The notorious FACS model – facial action coding systems – converts visible muscle movements in a human's

face into corresponding emotions. It still offers one of the most popular taxonomies for the analysis of emotions based on visually traceable data, not least because of its almost simplistic implementation of machine-readability. The foundations of this conversion of facial expression into knowledge about a human's emotions are highly questionable: it neglects social and cultural contexts, assumes the universality of emotional expression and is partly based on a hyperbolic and almost comical system of representation.[6]

Despite the likelihood of creating a fair amount of empirical artefacts, the analysis of emotions or affects within the power dynamics of current surveillance practices might develop a mighty knowledge of its own: Surveillance as simulation and imputation. If programmers of surveillance techniques define situations as real, they become real in their consequences (here, I am corrupting the Thomas theorem a little for the sake of argument). The emotion-surveillance technique creates an affect-laden subject with attendant simulation knowledge on thoughts and feelings. This is a real risk, as the models even claim to detect emotions that the subject is trying to hide.

A look ahead

If the current developments promoted by private companies are any indicator of what state actors will soon be eager to trace, track and potentially utilise for political reasons or policing in authoritarian systems, the mere idea of affective computing and emotion analytics is a dire premonition of what is to come. This outlook is further substantiated by the mass implementation of AI-based emotion recognition tools, which is already happening in China.

This type of surveillance produces knowledge that not only claims to reveal what people are likely to do in the future but also what they feel and think, paired with the promise of reading the actual truth behind the fake emotion – as one surely can always feign the right attitude or required ethos. The consequences of this epistemological bending are potentially grave. The AI-powered machine reading tool can quite easily be framed as generating impartial and objective knowledge about disloyal mindsets and attitudes that are in need of sanctioning or prosecution. This might even mark the return to a form of criminal law that is attitude-based rather than act-based. The mere thought of committing an illegal act might after all be something that violates the law.

References

1. David Lyon, 'Surveillance' (2022) 11:4 *Internet Policy Review*.
2. Ulises A. Mejias and Nick Couldry, 'Datafication' (2019) 8:4 *Internet Policy Review*.
3. Erik Tuchtfeld, '"Thank You Very Much, Your Mail Is Perfectly Fine": How the European Commission Wants to Abolish the Secrecy of Correspondence in the Digital Sphere' (2022) *Verfassungsblog*.
4. Yuval Abraham, '"Lavender": The AI Machine Directing Israel's Bombing Spree in Gaza' *+972 Magazine* (3 April 2024), https://www.972mag.com/lavender-ai-israeli-army-gaza/.
5. Warren L. Swanson and Roger Elchmeier, 'Lie-Detector Tests and Freedom of the Will in Germany' (1957) 47:5 *Journal of Criminal Law and Criminology*.
6. Thomas Christian Bächle, 'Faking It Deeply and Universally? Media Forms and Epistemologies of Artificial Faces and Emotions in Japanese and Euro-American Contexts' (2022) 29:2 *Convergence: The International Journal of Research into New Media Technologies*.

Sarah Stummer

A Right to Anonymity in the Digital Age

A Discussion of the Opportunities, Risks and Limitations

Although digital anonymity is associated with a wide range of opportunities and is important for natural persons, it also harbors risks and can stand in the way of successful criminal prosecution – digital anonymity should therefore be granted within limits.

The right to respect of private and family life (Article 7 of the Charter of Fundamental Rights of the European Union (CFR)), as well as the right to protection of personal data (Article 8 CFR) are of fundamental importance for natural persons. This is not only a subjective perception but is also reflected in an empirical study the Fraunhofer Institute for Secure Information Technology conducted.[1] This empirical study shows not only the importance for the participants to decide for themselves (to the greatest possible extent) which pieces of personal information they disclose to whom, but also the importance of anonymity to natural persons. However, since life is increasingly taking place online, (supposed) anonymity can also be exploited to spread hate, discriminatory content, and fake news. Thus, in the digital age, anonymity also harbors risks. Considering these risks, the European Court of Justice (ECJ), has (contrary to its previous case law[2]) opened the door to data retention in Europe and thereby restricted digital anonymity with the decision *La Quadrature Du Net II* (C-470/21) in focus here. This contribution therefore discusses whether and to what extent individuals should be granted a right to anonymity in the digital age.

Anonymity in the digital age

Recital 26 of the General Data Protection Regulation (GDPR, Regulation (EU) 2016/679) states that anonymous data is "information which does not [or no longer] relate to an identified or identifiable

natural person". Hence, according to the GDPR anonymous data is the opposite of personal data and anonymity is given if no natural person can be identified based on the processed information.[3] Taking into account the wording of recital 26 GDPR as well as the case law of the ECJ in *Mircom International v. Telenet BVBA* (C-597/19) a factual and (mostly) relative understanding of the term anonymity must be assumed.[4] Whether data is anonymous or not thus depends on whether the identification of natural persons is *de facto* impossible, in particular due to excessive effort required for identification. Since only the knowledge of those parties who have lawful access to the (supposedly anonymous) data is likely to be used in the sense of recital 26 GDPR – provided an unlawful access to the data is made sufficiently unlikely by technical and organizational protective measures – their knowledge is the decisive factor for whether the data can be considered anonymous from a data protection point of view.

However, even if data are not considered generally anonymous from a data protection point of view, they can still be anonymous relatively to certain persons. On the internet, for instance, natural persons can usually be identified by their IP address (even if they do not actively disclose any personal information). Therefore, on the internet, general anonymity does not exist from the perspective of data protection law. However, identification by an IP address is subject to certain legal requirements (e.g. suspicion of a criminal offense committed in or with help of the internet), so that identification by an IP address is neither always possible nor possible for everyone. Hence, anonymity on the internet still exists relatively to certain persons. For example, a social media user who only uses a pseudonym as well as non-identifying images and information may be anonymous in relation to other internet users, while simultaneously, in the event of a criminal offense, can be

identified by law enforcement authorities. In Germany, for example, in the event of a criminal offense, law enforcement authorities can use the IP address (including time stamp) to request information from the telecommunications provider as to whom the relevant IP address was assigned to at the time in question (§ 100j (2) of the German Code of Criminal Procedure).

Opportunities of anonymity in the digital age

Even though anonymity on the internet usually only exists relatively to certain persons, such relative (and subjectively perceived) anonymity is important to natural persons. This is shown by an empirical study the Fraunhofer Institute for Secure Information Technology conducted with 100 individuals from Germany.[5] In this study, 83% of the participants stated that they would (whenever possible) prefer the use of anonymized data originally concerning them to the use of their personal data. Reasons for this include, among others, the fact that anonymity makes some of the participants feel less observed (stated by 77% of the participants with at least "tend to agree") and safer (stated by 71% of participants with at least "tend to agree").

On the internet, anonymity enables the construction and exploration of (online-)identities[6] and creates a space for expression and (self-)representation.[7] Therefore, it bears the potential for internet users to exercise their rights and freedoms without restrictions. This is particularly important for vulnerable groups, such as children or minorities, who are particularly affected by hate speech, discrimination, and other offenses. Because of the anonymity they enjoy online, they are less likely to experience hate, discrimination or other abuse when expressing (political) opinions and views.[8] Furthermore, anonymity can create an added value for society

since it enables the discussion of social taboo topics (e.g. sexuality, violence and abuse as well as issues of minorities), which can lead to better education and interpersonal understanding.[9]

Risks of anonymity in the digital age - the other side of the coin

On the other hand, due to the online disinhibition effect,[10] anonymity on the internet can lead to persons losing accountability for their own actions[11] and adhering less to social norms and rules or even to laws.[12] In consequence, this can result in persons using their (supposed) digital anonymity to say or do things they would not say or do in the analogous world, in view of (features of) their civil identity. These things can possibly include a wide range of offenses, from hate speech to the dissemination of discriminatory content and false information to stalking.[13] Furthermore, it can lead to serious crimes such as drug-, human- or arms-trafficking.[14] Thus, (supposed) anonymity can, on the negative side, affect other persons and their rights and freedoms.

The right to digital anonymity: A right within limits

In view of the aforementioned opportunities and risks of digital anonymity – the opportunity to protect rights and freedoms on the one hand, and the risk of affecting rights and freedoms of others, on the other – a right to digital anonymity should (as every right) be granted within limits.

Nevertheless, it is questionable whether a right to digital anonymity exists at all in the current legal situation and, if so, to what extent there are limits to this. A right to anonymity is not

directly provided for – neither in German law nor in European or international law. However, it can be derived from other (fundamental) rights and freedoms.[15] In German law, for example, a right to anonymity can be derived from the right to informational self-determination in terms of Article 2 (1) in conjunction with Article 1 (1) of the German Constitution.[16] Also, it is related to other fundamental rights, in particular the fundamental right to freedom of expression, arts and sciences (Article 5 German Constitution) as well as the right to privacy of correspondence, posts and telecommunications (Article 10 German Constitution). Similarly, at European level, a right to anonymity can be derived from the Charter of Fundamental Rights of the European Union, in particular from the rights to respect for private and family life (Article 7 CFR), the right to protection of personal data (Article 8 CFR) as well as the right to freedom of expression and information (Article 11 CFR). At the global level, a right to anonymity can be derived from international conventions on human rights, among others, from the European Convention on Human Rights (ECHR) and the International Covenant on Civil and Political Rights (ICCPR).[17] These conventions include a right to respect for private and family life (see Article 8 ECHR, Article 17 ICCPR) as well as a right to freedom of opinion and expression (see Article 10 ECHR, Article 19 ICCPR), both of which – like the aforementioned German and European fundamental rights and freedoms – are closely linked to (digital) anonymity and thus constitute the basis for a (derived) right to anonymity.

However, none of the aforementioned rights and freedoms are absolute. Rather, they can be restricted at the national, European and global level respectively, especially when this is necessary to protect the rights of others (see e.g. Article 5 (2) German Constitution, Article 10 (2) German Constitution, Article 52 (1) CFR, Article

8 (2) ECHR, Article 10 (2) ECHR, Article 19 (2) ICCPR). Consequently, like other fundamental rights and freedoms, the right to anonymity is not an absolute right but a right within limits.[18] This is, as the presentation of the opportunities and risks of anonymity in the digital age has shown, necessary to make use of the opportunities offered by the right to (digital) anonymity while at the same time countering the risks that arise from anonymity in the digital age.

The future of the right to digital anonymity

On April 30, 2024 the ECJ ruled (*La Quadrature Du Net II* (C-470/21)) that the general and indiscriminate retention of data does not necessarily constitute a serious interference with guaranteed rights (para. 79) but can be justified by the objective of combating criminal offenses. However, this is only the case if it is genuinely ruled out that the retention could give rise to serious interferences with the private life of the person concerned (para. 82). To rule out such a serious interference, several conditions must be met. Amongst them, it must be ensured that each category of data, including data relating to civil identities and IP addresses, is stored under technical modalities in such a way that no precise conclusion about the persons private life can be drawn. In particular, each category of data must be completely separate from the other categories of data retained (paras. 86-87). As a result of the ruling, the ECJ partially lowers the requirements for linking IP addresses to identities, thereby shifting the limits of the right to digital anonymity. This, however, does not undermine the rights of those who merely take advantage of the opportunities of the right to digital anonymity. Rather, it protects the victims of those who exploit digital anonymity for offenses and serious crimes, thus affecting

the rights of others. Since criminal offenses are increasingly shifting to the digital space and,[19] in consequence, the threat situation is evolving, appropriate countermeasures are needed to enable criminal prosecution and protect victims. This – and not the general restriction of the right to digital anonymity – is what the recent decision of the ECJ is about.[20] Hence, the right to digital anonymity remains untouched for those who act lawful. Those who exploit anonymity for unlawful activities, on the other hand, can be prosecuted more easily based on the ECJ's decision.

Conclusion

Digital anonymity is associated with a wide range of opportunities for individuals and society, but it also harbors risks for other persons. Like any (fundamental) right, the right to digital anonymity must therefore always be balanced against the rights and freedoms of others. As criminal offenses are increasingly shifting to the digital space, the threat situation is changing and countermeasures to enable successful prosecution in the digital age are required. This is made possible by the ECJ decision of April 30, 2024. However, it remains to be seen whether and to what extent the ruling of the ECJ will affect the legal developments in Germany and other EU member states.

This research work has been funded by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE. This article reflects the personal opinion of the author.

References

1. Sarah Stummer and Phillip Hähle, 'Anonymität und deren Verifikation' (2024) 48 *Datenschutz und Datensicherheit – DuD*.
2. See CJEU, *La Quadrature du Net I*, Joined Cases C-511/18, C-512/18 and C-520/18, Judgment of 6 October 2020.
3. Sarah Stummer, 'Personenbezogenheit vs. Anonymität: Ein Mapping des rechtlichen und technischen Begriffsverständnisses von "Personenbezogenheit", "Pseudonymität" und "Anonymität"' (2023) 47 *Datenschutz und Datensicherheit*.
4. Sarah Stummer, 'Identifizierbarkeit und Anonymität im Internet: Metriken zur Verifikation des Anonymitätsgrads im Rahmen der Internetnutzung' (2023) 3 *Zeitschrift für Digitalisierung und Recht*.
5. Sarah Stummer and Phillip Hähle, 'Anonymität und deren Verifikation' (2024) 48 *Datenschutz und Datensicherheit – DuD*.
6. Rishab Bailey, Vrinda Bhandari, and Faiza Rahman, 'Examining the Online Anonymity Debate: How Far Should the Law Go in Mandating User Identification?' (2021) *Data Governance Network, Working Paper 18*.
7. Michael Friedewald, Michael Kreutzer, and Marit Hansen, *Selbstbestimmung, Privatheit und Datenschutz: Gestaltungsoptionen für einen europäischen Weg* (Springer Vieweg Wiesbaden, 2022).
8. Eric Jardine, 'The Dark Web Dilemma: Tor, Anonymity and Online Policing ' (2015) *Global Commission on Internet Governance, Paper Series: No. 21*.
9. Rishab Bailey, Vrinda Bhandari, and Faiza Rahman, 'Examining the Online Anonymity Debate: How Far Should the Law Go in Mandating User Identification?' (2021) *Data Governance Network, Working Paper 18*.
10. John Suler, 'The Online Disinhibition Effect' (2004) 7:3 *CyberPsychology & Behavior*.
11. Ciarán Burke and Alexandra Molitorisova, 'What Does It Matter Who is Browsing? ISP Liability and the Right to Anonymity' (2017) 8:3 *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law*.
12. Rishab Bailey, Vrinda Bhandari, and Faiza Rahman, 'Examining the Online Anonymity Debate: How Far Should the Law Go in Mandating User Identification?' (2021) *Data Governance Network, Working Paper 18*.
13. Ciarán Burke and Alexandra Molitorisova, 'What Does It Matter Who is Browsing? ISP Liability and the Right to Anonymity' (2017) 8:3 *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law*.
14. David Kaye, *Report of the Special Rapporteur on the Promotion And Protection of the Right to Freedom of Opinion And Expression* (UN Human Rights Council, 2017).
15. Bayerisches Wissensnetzwerk Digitale Infrastrukturen, IT-Sicherheit und Recht für Unternehmen, 'Grundrecht auf Anonymität' https://www.baywidi.de/enzyklopaedie/grundrecht-auf-anonymitaet/.

16. Dirk Heckmann, 'Persönlichkeitsschutz im Internet' (2012) 65:36 *Neue Juristische Wochenschrift*.

17. Evgeni Moyakine, 'Online Anonymity in the Modern Digital Age: Quest for a Legal Right' (2016) 1:1 *Journal of Information Rights, Policy and Practice*.

18. Evgeni Moyakine, 'Online Anonymity in the Modern Digital Age: Quest for a Legal Right' (2016) 1:1 *Journal of Information Rights, Policy and Practice*.

19. Bundeskriminalamt, 'Positionspapier des BKA zu erforderlichen Speicherfristen von IP-Adressen' (21 July 2023), https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/230623_Mindestspeicherfristen_IP-Adressen.html.

20. Lina Marquard, 'EuGH: Vorratsdatenspeicherung auch bei allgemeinen Straftaten zulässig' (2024) 12 *ZD-Aktuell*.

Sabine Leutheusser-Schnarrenberger, Isabella Risini, Erik Tuchtfeld

The Challenges of Nuance

Five Questions to Sabine Leutheusser-Schnarrenberger

The symposium *Eyes Everywhere*, which forms the basis of this edited volume, was concluded with an interview with former Federal Minister of Justice Sabine Leutheusser-Schnarrenberger for our weekly editorial format "Five Questions to…".

Sabine Leutheusser-Schnarrenberger is one of the most prominent voices in German data protection law; in this interview she reflects on the means and ends and how they relate to each other over time in the context of surveillance practices.

The interview was conducted by Isabella Risini and Erik Tuchtfeld.

1. In light of the ECJ case *La Quadrature du Net II* (C-470/21), Joachim Herrmann, the Bavarian Minister of the Interior, emphasizes in his contribution to this book that "the level of threat determines the proportionality of the means – both are subject to the constant change over time". Do you see such a change, the increased threat level described by Herrmann, and do you share his assessment that national security needs a "Zeitenwende"?

Although there are always problematic developments in national security, threat situations can also be overstated. Overall, Germany is a safe country. There is no doubt that the internet has fundamentally changed crime, which has increasingly shifted to the digital space. However, the call for new surveillance powers or even a "Zeitenwende" ignores very important aspects. Firstly, most digital threats must be addressed in a very real way – and crime solving rates are stable in the digital world. Secondly, it is questionable whether the demanded instruments actually provide more security. There is a lack of sufficient evidence here, partly because there are often no evaluation clauses. Instead of addressing these points and arguing for an evidence-based, fundamental rights-oriented reform

of the security architecture, Mr. Herrmann and others often provide simplified answers. Of course, digital surveillance measures restrict the freedoms of citizens. The fathers and mothers of our Basic Law already saw this "certainty of the past". Fundamental rights were never intended to be "fair-weather institutions". They are intended to ensure the protection of the individual, especially in times of uncertainty and threat, even if it seems appropriate for the majority or the state to restrict them.

2. In last year's summer, the Federal Government seemed to see a need for such changes and voted in favor of the possibility of AI-supported biometric analysis of the internet as part of the "security package" (parts of the package were stopped by the Bundesrat, however). Critics fear that this will only be possible via extensive databases with all image material from the internet in order to search for suspects in this stored material. What do you think of these measures?

Biometric analysis of the internet opens up new surveillance possibilities that were unimaginable just a few years ago. AI technology is developing rapidly and without a foreseeable endpoint, so the openness of the technology (to be implemented) was a central problem of the security package. Due to the wide range of implementation options, it remained unclear to what extent fundamental rights would be curtailed. However, key decisions like this should be made directly in the law, in the interests of fundamental rights. There was a lively debate on the security package, during which many problematic provisions were improved or equipped with safeguards. The debate about which AI systems we no longer consider tolerable in a democracy was conducted extensively at the European level as part of the AI Act ((EU) 2024/1689). AI systems that extract images from the internet in an untargeted manner in

order to create or expand databases for biometric facial recognition are prohibited under the AI Act. This clear line should also be defined in national laws. The fact that parts of the security package have now been stopped in the Bundesrat, because some states demanded more surveillance, suggests that some want to reopen this debate in Germany. I warn against this being done with populist slogans and within only a few weeks. This requires a broader and less agitated debate.

3. The ECJ expressed, in April 2024, the fear that without IP data retention there would be "a real risk of systemic impunity". This argument is repeatedly put forward in calls for data retention. Do you have the impression that the extensive data pools collected by private providers for commercial purposes are sufficiently taken into account? Should these be included in an "general surveillance account"?

The idea that only data retention can prevent impunity has been disproved. There has been no data retention in Germany for more than ten years and the security authorities still announce better crime solving rates every year. When the data retention laws were abolished, I commissioned a study in my role as Federal Minister of Justice to identify possible gaps in protection. The result was clear: there are no such gaps. In addition, the Quick Freeze model, an alternative to indiscriminate data retention, has been an option for years. Implementing this model and then evaluating it would be a sensible way to provide the security authorities with a new, legally secure instrument with which they can access IP address data, among other things.

The idea behind the so-called "general surveillance account" is that permanent surveillance fundamentally changes the nature of society. It is part of the constitutional identity of the Federal

Republic of Germany that the exercise of freedom may not be fully recorded or monitored. Legislators must therefore take existing surveillance powers into account when considering new instruments. If the state wants to extend its surveillance reach by accessing private data collections, these must also be included in the overall calculation, that is quite clear to me.

4. Do you think it is necessary for German or European legislators to take stronger action against such private data collection, for example by reforming the GDPR ((EU) 2016/679) or introducing the ePrivacy Regulation, which has been on hold for a long time?

Extensive data collection makes us vulnerable, both individually and as a society. One example is Meta's data collection, which almost completely records users' online activity inside and outside of Facebook, which can create a feeling of constant surveillance. The ECJ emphasized this in *Maximilian Schrems v. Meta* (C-446/21) in October and found, among other things, that Meta is not allowed to use data indefinitely for targeted advertising, but on the contrary violates the principle of data minimization. This underlines the importance of the GDPR principles; however, it also shows that they are often only enforced by data protection activists (such as Max Schrems in this case). Not only because the practices are obscured, but also because many perceive them as unavoidable or even normal. Better law enforcement is therefore needed at this point and the resumption of negotiations on the ePrivacy Regulation could also be useful.

5. Time and again, massive antisemitic insults and incitement to hatred occur on the internet. You were the Anti-Semitism Commissioner of the state of North Rhine-Westphalia until

the end of October of this year and in this role you dealt professionally with antisemitic crimes on the internet. Do you have the impression that anonymity on the internet facilitates such acts or represents a relevant obstacle to the prosecution of such acts?

Anonymity protects freedom of expression and is essential for a democracy – both offline and online. It enables people to talk about highly personal, religious and political issues without having to fear immediate ostracism and repression. The problem is not that the internet offers room for anonymity, but the growing social acceptance of antisemitic statements. It has reached a level that must wake us up. Increasingly, people are openly spreading antisemitic hate speech under their real names – in social media, comments and threat letters. But also on the street, as part of openly antisemitic demonstrations, often disguised as criticism of Israeli policy. People who want to spread hatred are clearly no longer sufficiently deterred by laws. The flip side of anonymity on the internet would be the so-called "mandatory real name verification", which has been a subject of controversy since the beginning of the internet. Even such a measure does not lead to success, as the example of South Korea shows. Malicious comments such as defamation and insults hardly decreased there – despite the fact that such defamation is also punishable under Korean criminal law.[1] A study by the University of Zurich even shows that users are often more aggressive under their real names than anonymous users.[2] We therefore need truly effective methods to structurally and consistently combat punishable forms of hate online. It is unacceptable for prosecutable crimes to go unpunished for organizational, financial or personnel reasons.

References

1. John Leitner, 'Identifying the Problem: Korea's Initial Experience with Mandatory Real Name Verification on Internet Portals' (2009) 9 *Journal of Korean Law*.
2. Katja Rost, Lea Stahel, and Bruno S. Frey, 'Digital Social Norm Enforcement: Online Firestorms in Social Media' (2016) 11:6 *PLoS ONE*.

Read More

Verfassungsblog
Verfassungsblog is a not-for-profit academic and journalistic open access forum of debate on topical events and developments in constitutional law and politics in Germany, the emerging European constitutional space and beyond. It sees itself as an interface between the academic expert discourse on the one hand and the political public sphere on the other. Check out Verfassungsblog.de to discover all our articles, debates and other resources.

Our Books
We've got more open access books on other topics available for you at Verfassungsblog.de/Books.

Our Journal
With Verfassungsblatt, we collate a month's worth of texts that have been published on the blog into one publication. This format enables our readers to better keep an eye on which topics were important in a given month and to more easily find what interests them. Take a look at Verfassungsblog.de/Blatt.

Support Us
As a not-for-profit organisation, Verfassungsblog relies on its readers' support. You can help us keep up our work by making a donation here.

In *La Quadrature Du Net II*, the CJEU significantly lowered standards for mass data retention under the EU Charter, prioritizing security over privacy. This edited volume brings together European and international scholars and practitioners to explore how this shift may affect EU citizens' protection of fundamental rights and substantially redefine the surveillance and data retention framework for public and private agents.

focus

FUNDAMENTALS OF EU CHARTER USE IN SOCIETY