



ARTICLE

Constitutionalizing Mass Surveillance in the EU: Civil Society Demands, Judicial Activism, and Legislative Inertia

Edoardo Celeste¹  and Giulia Formici² 

¹School of Law and Government, Dublin City University, Ireland and ²Department of Law, Politics and International Studies, University of Parma, Italy

Corresponding author: Giulia Formici; Email: giulia.formici@unipr.it

(Received 20 October 2022; accepted 22 June 2023)

Abstract

Despite the shock provoked by the Snowden revelations, mass surveillance is still a reality in the EU. However, over the past few years, it has been possible to observe a gradual constitutionalization of these practices. This Article maps the ongoing process of progressively defining the constitutional limits and societal affordances of mass surveillance in the EU by focusing on the three main actors who contribute to it. First, this Article presents civil society as the propeller of this trend. Civil society not only advocated for a ban on general surveillance systems in the aftermath of the Snowden revelations, but also promoted a series of strategic litigations to challenge state surveillance practices at national and EU levels. Second, it analyses CJEU case law as the main constitutionalizing engine of this process. The Court pragmatically ascertained that an absolute prohibition of mass surveillance did not appear to be a realistic solution and put significant effort into actively defining the legal boundaries of these practices by striving to find an equilibrium between Member State interests and citizens' fundamental rights. Third, it considers the approaches taken by national legislators to be a slowing factor. States are still reluctant to incorporate the constitutional standards progressively developed by courts despite the now significant body of judicially created parameters in the field.

Keywords: Mass surveillance; constitutionalization; civil society; CJEU; legislators

A. Introduction

In 1984, European Court of Human Rights Justice Pettiti, in his concurring opinion in the decision of *Malone v The United Kingdom*, affirmed: “The danger threatening democratic societies in the years 1980-1990 stems from the temptation facing public authorities to see into the life of the citizens.”¹ This feared prophecy, unfortunately, was revealed to be accurate, and the 2013 Snowden revelations made it crystal clear: in “times of stress,”² characterized by terrorist attacks and transnational crimes, public authorities have increasingly resorted to surveillance systems as important tools to guarantee national and public security. Despite their potential to fight against terrorism and global crime, these instruments create serious intrusions into the private lives of

¹Malone v. United Kingdom, Concurring Opinion of Judge Pettiti, App. No. 8691/79 (Aug. 2, 1984), <http://hudoc.echr.coe.int/>, last accessed 20 October 2022.

²Michel Rosenfeld, *Judicial Balancing in Times of Stress: Comparing Diverse Approaches to the War of Terror*, 27 BENJAMIN N. CARDOZO SCHOOL OF LAW WORKING PAPER 2079 (2005).

millions of individuals; in particular, they endanger the right to data protection together with other rights and principles fundamental to the core of our democratic societies, such as freedom of expression and the principle of presumption of innocence. Unlike “targeted” surveillance, mass surveillance allows for the generalized and indiscriminate monitoring of every person with no need for a specific or reasonable suspicion and without an objective link connecting those subjected to control or a particular risk or crime. In recent years, the extensive employment of new technologies and big data enabling forms of mass surveillance for the sake of security has expanded already existent criticalities and added new issues related to both the increased ability to capture a vast amount of data and the capacity to automatically analyze them in an aggregated way, finding connections, determining social relations, habits, preferences, and movements;³ in other words, the profiling of users. These sophisticated techniques add further complexities that make it even more urgent to determine a clear balance between general interests, such as national security, and safeguarding fundamental rights.

In the EU, this complex challenge is central to a heated debate involving civil society, courts, legislators, and law enforcement authorities, at national and supranational levels. The quest for a ban, or at least a more stringent set of rules governing the use of highly invasive surveillance measures has characterized the reactions of citizens and NGOs who are worried about the possible detrimental impact on fundamental rights and freedoms of preventive data and metadata control by public authorities – in particular, law enforcement and intelligence agencies.⁴ In this context, civil society has played a decisive role. On the one hand, civil society groups triggered a vast judicial discussion on the necessity to determine proper and precise safeguards for mass surveillance techniques. Most of the landmark decisions of the Court of Justice of the European Union (CJEU), as well as national courts, were initiated by NGOs. They instigated a far-reaching momentum into this serious debate by pushing policymakers to (re-)think about the possibility of massively collecting, retaining, accessing, and processing private information and data for security purposes. On the other hand, civil society groups are nourishing a debate outside national and supranational courtrooms and parliaments on how to articulate the core principles of contemporary constitutionalism in the fight against global crime. Mass surveillance was merely a theoretical possibility when most constitutional charters were adopted. As this Article explains, it is rare for constitutional charters to directly limit mass surveillance. Civil society groups, through the adoption of non-legally binding declarations of digital rights, are fostering a conversation on how to ensure that traditional constitutional rights – such as the rule of law, due process, the right to privacy, and freedom of expression – are also guaranteed while deploying digital technology surveillance mechanisms for national or public security purposes.

The core argument of this Article is that these recent developments, comprehensively analyzed, denote a move towards a gradual, multilevel constitutionalization of mass surveillance. In this Article, we use this term to describe the translation and incorporation of already affirmed core constitutional values, particularly the principles of proportionality, legality, and the necessity of judicial oversight, in the specific context of state surveillance. Constitutionalization is used here as a lens to map the ongoing multilevel process of progressively defining constitutional limits and societal affordances of mass surveillance practices in the EU. Our Article is structured in three parts, focusing on the three main actors that so far triggered and shaped the constitutionalization of mass surveillance in the EU: civil society, the CJEU, and national legislators.

Section B reconstructs the role of civil society actors. We explain that surveillance practices have emerged thanks to a constitutional vacuum. Existing constitutional texts rarely address surveillance practices explicitly. This has allowed state authorities to potentiate and keep

³See Dennis Broeders, *Quis Custodiet Ipsos Custodes? Security, Big Data and Secrecy*, 3 EUR. DATA PROT. LAW REV. 306 (2017).

⁴See, e.g., Paul De Hert and Georgios Bouchagiar, *Visual and Biometric Surveillance in the EU. Saying “No” to Mass Surveillance Practices?*, 27 INFORMATION POLITY 193 (2022).

surveillance systems in place even in the aftermath of global scandals that made apparent the level to which these practices seriously violate core fundamental rights. Through an analysis of the initiatives and demands of civil society in the field of state surveillance, we show how this constitutional vacuum is no longer justified as it reflects the social reality of a time when mass surveillance was considered an unrealizable dystopia. Civil society organizations have played a crucial role in prompting a reaction to this normative void – not only by promoting strategic litigation contesting mass surveillance practices but also by explicitly advocating for a ban on mass surveillance through the adoption of non-legally binding declarations of digital rights.

Section C focuses on the constitutional input provided by the CJEU. Notwithstanding the specific demands from civil society actors, an analysis of the complex case law of the CJEU affecting state surveillance practices reveals that an absolute prohibition of mass surveillance practices does not appear to be a feasible and realistic solution. Conversely, the CJEU has put significant effort into actively defining the legal boundaries of mass surveillance practices in the EU. The constitutionalizing role played by the Court has thus consisted of constantly striving to find an equilibrium between Member State interests and fundamental rights, becoming both a defender of civil society demands and a pragmatic interpreter of the exigencies of public and national security authorities.

Section D examines the reticent – if not to say, at times ostensibly deaf – posture (still) adopted by national legislators in the field of surveillance practices, which is inexorably slowing down their process of constitutionalization. Civil society and judicial impulses have progressively impacted the normative choices available to national legislators. The *carte blanche* on surveillance powers accorded to national legislators in the aftermath of various terroristic attacks in Europe in the early 2000s is no longer available. In light of a growing body of delimitations developed by the CJEU, national legislators are now called on to pay more attention to finding pragmatic ways of striking a balance between national and public security and guaranteeing the fundamental rights at stake. Yet we conclude by denouncing how national legislators remain reluctant to incorporate the constitutional standards progressively developed by courts, thus observing the persisting ongoing nature of the multilevel process of constitutionalization of state mass surveillance practices.

B. Civil Society Demands: Invoking a Constitutional Ban on Mass Surveillance

I. In the Silence of Constitutions: The Normative Vacuum about Surveillance

Despite the “historical pedigree”⁵ of the rights to data protection and privacy in Europe, which emerged as a counteraction to the atrocities committed by the authoritarian regimes of Western and Eastern European countries before and after WWII, an absolute prohibition of mass surveillance is not explicitly enshrined in any national constitution. This can be mentioned as one factor that has allowed mass surveillance practices to survive recent scandals and court cases. Data protection legislation and the constitutional right to data protection emerged in the EU as a normative response to the risks associated with increased automation, collection, and exchange of personal data in the public and private sectors.⁶ Yet, despite the daunting potential of these technologies in the 1960s and the multiple contemporary lessons learned from authoritarian regimes in European history, surveillance is not explicitly addressed at the constitutional level.

The term “surveillance” is explicitly included in only two European national constitutions: the Swedish Constitution and the German Basic Law. The Instrument of Government, one of the four fundamental laws composing the Swedish Constitution, in Chapter 2, Article 6 reads:

⁵See Bilyana Petkova, *Privacy as Europe’s First Amendment*, 25 EUR. L. J. 140 (2019); Annabelle Lever, *Democracy, Privacy and Security* in Adam Moore, ed., *Privacy, Security, and Accountability: Ethics, Law and Policy* (2016).

⁶See GLORIA GONZÁLEZ FUSTER, *THE EMERGENCE OF PERSONAL DATA PROTECTION AS A FUNDAMENTAL RIGHT OF THE EU* (2014). Specifically on France and its ‘Safari’ scandal see Félix Tréguer, *Intelligence Reform and the Snowden Paradox: The Case of France*, 5 *Media & Communication* 17 (2017).

Everyone shall be protected [...] against examination of mail or other confidential correspondence, and against eavesdropping and the recording of telephone conversations or other confidential communications. In addition to what is laid down in paragraph one, everyone shall be protected in their relations with public institutions against significant invasions of their privacy, if these occur without their consent and involve the surveillance or systematic monitoring of the individual's circumstances.⁷

Paragraph 2 of this provision was added a decade ago after a recommendation from an ad hoc Commission on the Protection of Personal Privacy. Interestingly, the Swedish legislator added a provision that is almost redundant after protecting against the examination of all types of confidential communications, but that explicitly targets surveillance systems. Indeed, the norm of paragraph 2 explicitly refers to forms of “systematic monitoring” performed by “public institutions” without the individual's consent that produce “significant invasions” of personal privacy. Yet paragraph 2 does not seem to ban mass surveillance. By reading Article 20, one understands that the explicit protection afforded by the Instrument of Government is the application of the principle of legality to potential restrictions on the rights enshrined in Article 6. In other words, the principle of secrecy of correspondence and the right to privacy are explicitly considered relative rights in Swedish constitutional law, thereby tolerating potential compressions that must be clearly defined by law, and not extemporaneously implemented by law enforcement authorities.

The German Basic Law adopts a similar approach. Surveillance is explicitly mentioned in the German constitution and is presented as a permissible practice subject to a series of guarantees. The term “surveillance” is used in Article 13, which enshrines the inviolability of the dwelling and refers to acoustic monitoring systems. Paragraphs 3 and 4 read:

(3) If particular facts justify the suspicion that any person has committed an especially serious crime specifically defined by a law, technical means of acoustical surveillance of any home in which the suspect is supposedly staying may be employed pursuant to judicial order for the purpose of prosecuting the offence, provided that alternative methods of investigating the matter would be disproportionately difficult or unproductive. The authorization shall be for a limited time. The order shall be issued by a panel composed of three judges. When time is of the essence, it may also be issued by a single judge.

(4) To avert acute dangers to public safety, especially dangers to life or to the public, technical means of surveillance of the home may be employed only pursuant to judicial order. When time is of the essence, such measures may also be ordered by other authorities designated by a law; a judicial decision shall subsequently be obtained without delay.⁸

According to the Basic Law, surveillance is justified to investigate only *serious* crimes or dangers to public safety. A legal basis and judicial authorization are necessary to carry out surveillance practices. Surveillance is presented as a last resort practice, which can be used where no less invasive methods are available. Moreover, surveillance practices shall be limited in time. In sum, the German Constitution, in relation to acoustic surveillance of a dwelling, does not seem to avail a model of mass surveillance but that of targeted monitoring limited in time.

⁷THE CONSTITUTION OF SWEDEN: THE FUNDAMENTAL LAWS AND THE RIKSDAG ACT (Magnus Isberg ed., 2016), <http://www.riksdagen.se/globalassets/07.-dokument-lagar/the-constitution-of-sweden-160628.pdf>, last accessed 20 October 2022.

⁸See Paul M. Schwartz, *German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance Symposium: Enforcing Privacy Rights*, 54 HASTINGS L.J. 751 (2002).

Interestingly, one can notice that the normative architecture of the German Basic Law follows a classical approach, dealing with the inviolability of the dwelling and the privacy of correspondence in two separate provisions. Article 10 indeed focuses on “correspondence, posts and telecommunications” and, interestingly, enshrines a different, lighter standard of protection in relation to surveillance practices affecting this portion of our private life. Paragraph 2 of this norm reads:

(2) Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a *Land*, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature⁹

The principle of legality is still the main guarantee the German Constitution introduces to protect the privacy of communications. However, in this case, the Basic Law does not refer to judicial authorization or time limits. Contrariwise, the scope of the justifications of a potential restriction is very broad: the protection of the “free democratic basic order” and the “existence or security of the Federation or of a *Land*” instead of specific serious crimes. Second, judicial oversight is expressly replaced by law enforcement or an intelligence agency review. Third, covert surveillance is explicitly authorized since the law may require that the persons affected by the ongoing monitoring are not to be notified. In sum, apart from the requirement to find a legal basis, Article 10 does not circumscribe the possibility of introducing mass surveillance practices.

This brief analysis of constitutional provisions reveals that, while protection of private life is generally enshrined in contemporary constitutions, no explicit provisions significantly limit the possibility of resorting to mass surveillance practices, even in constitutional texts that explicitly regulate surveillance. On the contrary, national constitutions generally include provisions that potentially restrict the principle of secrecy of correspondence, the right to privacy, and the right to data protection. None of these rights are presented as absolute. They all tolerate restrictions in the name of public and national security, thus de facto opening the door to the adoption of mass surveillance systems. In light of this consideration, we contend that constitutional provisions currently in force reflect the technological state of the art of a time when mass surveillance was still utopic and, therefore, do not afford adequate protection against the potential risks of these practices. However, in this Article, we posit that a progressive process of constitutionalization is currently underway in relation to state surveillance. A series of impulses are pushing towards developing constitutional principles, limiting the possibility of resorting to mass surveillance practices, and defining acceptable levels of compression of fundamental rights. In the following sections, we will analyze civil society and judicial impulses, investigating to what extent civil society groups and courts in the EU are normatively shaping constitutional guarantees against surveillance.

II. Multilevel Constitutionalization and the Driving Role of Civil Society

The constitutionalization process that is currently shaping surveillance systems is in reality a broader phenomenon. It encompasses all major changes and threats prompted by the digital revolution. It is plural, yet unitary in its ultimate objectives.¹⁰ Recent scholarship analyzed the emergence of “digital constitutionalism” as an ideology informing and leading a multistakeholder

⁹See Jutta Stender-Vorwachs, *The Decision of the Bundesverfassungsgericht of March 3, 2004 Concerning Acoustic Surveillance of Housing Space*, 5 GERMAN L. J. 1337 (2004).

¹⁰See Edoardo Celeste, *The Constitutionalisation of the Digital Ecosystem: Lessons from International Law* in Angelo Jr Golia, Matthias C Kettemann & Raffaella Kunz (eds), *DIGITAL TRANSFORMATIONS IN PUBLIC INTERNATIONAL LAW* (2022).

movement.¹¹ One cannot identify a single constitutional framer, but several actors contributed at multiple levels to the debate on how to articulate constitutional norms that should preserve our fundamental rights in the digital ecosystem. Not only traditional, institutional actors, such as courts and legislators, but also new voices, often neglected from a legal point of view, such as civil society.¹² It is not a chaotic conversation but a process where each party stimulates and complements each other as the tesserae of a single mosaic. It is a multilevel process of constitutionalization that finds its unity in its aim to instill the core principles of contemporary constitutionalism in the context of the digital society.

Absent explicit, detailed regulation of surveillance at the level of national and supranational constitutions, civil society actors have played a driving role in the constitutionalization of mass surveillance. First, it is worth highlighting the important function that civil society played as a trigger of judicial cases. Indeed, the major decisions from national and European courts related to state mass surveillance practices, which we will analyze in more detail in the next section, were initiated by privacy activists, associations, and NGOs. Austrian privacy activist Max Schrems, Irish-based association Digital Rights Ireland, the NGOs Privacy International, la Quadrature du Net, and Big Brother Watch, who started these cases, acted not only as public watchdogs denouncing situations that conflicted with respect for the right to privacy and data protection, they also initiated strategic litigations that prompted major reforms at both EU and national levels. From a constitutional point of view, one can argue that civil society actors contribute to balancing powers, triggering a judicial reaction to legislators and governmental agencies' abuses or inaction.

Second, academics, activists, and NGOs have been among the most active actors in developing and advocating new constitutional principles that specifically target surveillance practices. Empirical studies have counted more than 200 declarations issued by civil society actors that aim to articulate and define principles and values for the digital society.¹³ These texts are generally known as Internet bills of rights and represent an interesting source to provide an analysis from a legal and, more specifically, a constitutional point of view. Indeed, Internet bills of rights are non-legally binding declarations made by a plurality of actors outside the institutionalized constitutional processes. If such an informal character makes them less interesting for black-letter law scholars, this feature undocks them from the limitations of political agenda and institutional restraints, giving them an unprecedented possibility to propose innovative normative solutions to the challenges posed by mass surveillance practices.¹⁴ From a sociolegal perspective, these non-legally binding declarations represent an invaluable source for understanding civil society's claims in the context of digital society and the extent to which these demands are accepted and integrated into the legal order.

III. Internet Bills of Rights: From the Right to Privacy to the Prohibition of Mass Surveillance

Internet bills of rights' task of articulating and defining principles and values for the digital society are not confined to a superficial conceptual make-up. These declarations do not merely specify the applicability of existing constitutional guarantees in the digital society. If one talks of a right to

¹¹Dennis Redeker, Lex Gill & Urs Gasser, *Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights*, 80 INT'L COMM. GAZETTE 302 (2018); Claudia Padovani & Mauro Santaniello, *Digital Constitutionalism: Fundamental Rights and Power Limitation in the Internet Eco-System*, 80 INT'L COMM. GAZETTE 295 (2018); Edoardo Celeste, *Digital Constitutionalism: A New Systematic Theorisation*, 33 INT'L REV. OF LAW, COMPUTERS & TECH. 76 (2019); ORESTE POLLICINO, JUDICIAL PROTECTION OF FUNDAMENTAL RIGHTS ON THE INTERNET: A ROAD TOWARDS DIGITAL CONSTITUTIONALISM? (2021); GIOVANNI DE GREGORIO, DIGITAL CONSTITUTIONALISM IN EUROPE: REFRAMING RIGHTS AND POWERS IN THE ALGORITHMIC SOCIETY (2022); Edoardo Celeste, DIGITAL CONSTITUTIONALISM: THE ROLE OF INTERNET BILLS OF RIGHTS (2022).

¹²See Edoardo Celeste and others, *Digital Constitutionalism: In Search of a Content Governance Standard* in Edoardo Celeste, Amélie Heldt and Clara Iglesias Keller (eds), CONSTITUTIONALISING SOCIAL MEDIA (2022).

¹³EDOARDO CELESTE, DIGITAL CONSTITUTIONALISM: THE ROLE OF INTERNET BILLS OF RIGHTS (2022).

¹⁴*Id.*, in particular Chapter 8.

freedom of expression online, one instinctively grasps that communication through digital technology should be guaranteed. The same can be said for freedom and secrecy of correspondence, freedom of association, and peaceful assembly. The development of digital technologies provides new instruments to exercise these rights. The communicative power of these constitutional provisions is generally preserved because one instinctively considers new technologies as the heir to an old means of communication. In these cases, Internet bills of rights tend to simply restate the applicability of analog constitutional provisions in contemporary society by referring to digital communication tools.

However, a similar intervention of superficial stuccoing does not always suffice. A series of fundamental rights designed for an analog world struggles to permeate and inform virtual reality. Their current formulation does not immediately speak to the actors of the digital society. Individuals and public and private institutions do not instinctively grasp the implications of these fundamental values. In these cases, Internet bills of rights intervene to extract their meaning and significance for a contemporary digital society. These declarations distill the quintessence of these constitutional values. They unfasten the pure essence of these rights from the accidentals of the society in which they emerged. At this point, the ultimate telos of the constitutional norm is plunged into the context of the digital society, from which it resurfaces with a more specifically tailored layout. Teubner, dealing with the emergence of constitutional patterns beyond the state, similarly discusses a double process of “generalization” and “re-specification.”¹⁵ The constitutional norm cannot be merely transplanted in a different societal context. One needs to understand its ultimate aim, generalize its principles, purify it from its original contextual contaminants, and then re-specify it in light of the characteristics of the new social reality.

The respect for individual privacy is an example of a fundamental value that Internet bills of rights do not merely restate with reference to digital technology but is generalized and further re-specified in light of the challenges of the digital society.¹⁶ Most of these declarations of rights generally affirm that any form of surveillance affects the individual’s privacy.¹⁷ However, some of them introduce new principles limiting mass surveillance practices. For example, in the words of the African Declaration on Internet Rights and Freedoms:

Mass or indiscriminate surveillance of individuals or the monitoring of their communications constitutes a disproportionate interference, and thus a violation, of the right to privacy, freedom of expression, and other human rights. Mass surveillance shall be

¹⁵Gunther Teubner, *Societal Constitutionalism; Alternatives to State-Centred Constitutional Theory?*, in Christian Joerges, Inger-Johanne Sand and Gunther Teubner (eds), *TRANSNATIONAL GOVERNANCE AND CONSTITUTIONALISM. INTERNATIONAL STUDIES IN THE THEORY OF PRIVATE LAW* (2004).

¹⁶Some declarations conversely limit themselves to restate the right to privacy in the online context. See *Marco Civil Da Internet, Lei No. 12.965, de 23 de Abril de 2014*, http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm (last accessed 20 October 2022), Article 7; UNESCO, *Code of Ethics for the Information Society Proposed by the Intergovernmental Council of the Information for All Programme (IFAP)* (2011), paragraphs 12 and 13, <https://unesdoc.unesco.org/ark:/48223/pf0000212696>, last accessed 20 October 2022; Praxis, *Guiding Principles of Internet Freedom*, http://www.praxis.ee/fileadmin/tarmo/Projektid/Valitsemine_ja_kodanikeuhiskond/Praxis_Theses_Internet.pdf (last accessed 20 October 2022), Principle no. 9; Social Innovation Society, *Carta Internazionale dei Diritti Digitali*, <http://www.soinsociety.org/carta-internazionale-dei-diritti-digitali/> (last accessed 20 October 2022), Article 8.

¹⁷See *Charter of Human Rights and Principles for the Internet*, http://internetrightsandprinciples.org/site/wp-content/uploads/2018/10/IRPC_english_5thedition.pdf (last accessed 20 October 2022), Article 8; Mike Godwin, *The Great Charter for Cambodian Internet Freedom*, <https://www.linkedin.com/pulse/great-charter-cambodian-internet-freedom-mike-godwin> (last accessed 20 October 2022), Article 2.5; NETmundial, *Internet Governance Principles - NETmundial Multistakeholder Statement*, <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf>, last accessed 20 October 2022; Open Society Institute - Regional Internet Program and Parliamentary Human Rights Foundation, *Open Internet Policy Principles*, <http://mailman.anu.edu.au/pipermail/link/1997-March/026302.html> (last accessed 20 October 2022), paragraph B1; *Charta der Digitalen Grundrechte der Europäischen Union*, <https://digitalcharta.eu/> (last accessed 20 October 2022), Article 7; Andrew Murray, *A Bill of Rights for the Internet*, <http://theitlawyer.blogspot.com/2010/10/bill-of-rights-for-internet.html> (last accessed 20 October 2022), Article 7.

prohibited by law. [...] In order to meet the requirements of international human rights law, targeted surveillance of online communications must be governed by clear and transparent laws which, at a minimum, comply with the following basic principles: first, communications surveillance must be both targeted and based on reasonable suspicion of commission or involvement in the commission of a serious crime; second, communications surveillance must be judicially authorized, and individuals placed under surveillance must be notified that their communications have been monitored as soon as practicable after the conclusion of the surveillance operation; third, the application of surveillance laws must be subject to strong parliamentary oversight to prevent abuse and ensure the accountability of intelligence services and law enforcement agencies.¹⁸

The constitutional message advocated by these civil society groups is clear. Internet bills of rights affirm that mass and indiscriminate surveillance represents an inadmissible limitation on the right to privacy, which cannot be considered proportionate as a matter of principle.¹⁹ Only targeted forms of surveillance, subject to specific guarantees, can be tolerated as reasonable restrictions of that right.²⁰ Interestingly, guarantees such as the requirement of serious crimes, judicial authorization, and notification to individuals align with those progressively established by the CJUE case law, as we will see in the following section.

C. Judicial Activism: A Gradual Process of Constitutionalization

I. Indiscriminate Data Retention in the EU: Legislative Genesis and First Judicial Ban

As anticipated, the “great temptation” to exploit the vast potential of technological tools and sophisticated surveillance instruments significantly expanded in the EU in the aftermath of 9/11. Considering the importance of effectively facing terroristic threats, the generalized retention of communications data by telecommunication operators immediately appeared an invaluable measure, allowing intelligence agencies and law enforcement authorities to “go back in time”²¹ and find useful investigative leads about people previously unknown to public authorities.²² For these reasons, the so-called e-Privacy Directive 2002/58²³ was adopted just a few months after the attack on the Twin Towers, followed by the Data Retention Directive (DRD),²⁴ which was rapidly implemented after the 2005 terrorist attacks in the EU. The case law, developed at the national and supranational level in the EU, concerning the implementation of data retention instruments and disciplines, represents a relevant, complex, and clear exemplification of the judicial inputs to the vast debate on surveillance tools and their constitutional limits. Analyzing the main arguments employed and the guarantees and safeguards affirmed by national and EU judges helps us better

¹⁸African Declaration Group, *African Declaration on Internet Rights and Freedoms*, <https://africaninternetrights.org/sites/default/files/African-Declaration-English-FINAL.pdf>, last accessed 20 October 2022.

¹⁹*Id.* See also Just Net Coalition, *The Delhi Declaration for a Just and Equitable Internet*, <https://justnetcoalition.org/delhi-declaration> (last accessed 20 October 2022), paragraph 16; Ujam Chukwuemeka, *Digital Rights and Freedom Bill 2016*, Section 10(3).

²⁰See African Declaration Group, *African Declaration on Internet Rights and Freedoms*, <https://africaninternetrights.org/sites/default/files/African-Declaration-English-FINAL.pdf>. (last accessed 20 October 2022) and Open Society Institute - Regional Internet Program and Parliamentary Human Rights Foundation, *Open Internet Policy Principles* (1997), in particular paragraph B.1.

²¹Iain Cameron, *Balancing Data Protection and Law Enforcement Needs: Tele2 Sverige and Watson*, 54 COMM. MARK. L. REV. 1467 (2017); Daragh Murray & Pete Fussey, *Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data*, 52 ISRAEL L. REV. 31 (2019).

²²Cameron, *supra* note 21; Arianna Vedeschi & Valerio Lubello, *Data Retention and its Implications for the Fundamental Right to Privacy. A European Perspective*, 20 TILBURG L. REV. 14 (2015).

²³EC Directive 2002/58 of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, O.J. 2002 L 201/37.

²⁴EC Directive 2006/24 of 15 March, O.J. 2006 L 105/54.

understand the consequent reactions and the normative solutions developed or still being discussed today by legislators.

Starting from the first adopted provision concerning data retention, Article 15 of the e-Privacy Directive establishes a broad derogation to the general obligation to erase or anonymize metadata. In particular, Member States can implement legislative measures allowing communications data to be exceptionally retained for a specific and limited time period when it is considered a “necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defense, public security and the prevention, investigation, detection, and prosecution of criminal offenses or unauthorized use of the electronic communications system.”

When the exacerbated terrorist threat pushed the EU legislators to increase and intensify harmonized answers in the context of a war on terror, the DRD, complementing the vague discipline provided by Article 15 of the e-Privacy Directive,²⁵ obliged Member States to implement national legislation requiring all service providers to retain a vast list of communications data for a period between six months and two years, attributing to the discretionary evaluation of each national legislator the adoption of specific access conditions and procedures as well as the definition of which “serious crimes” would legitimize the processing of metadata by law enforcement authorities.²⁶

Setting aside the challenges concerning the DRD’s legal basis (decided by the CJEU in Ireland v Parliament and Council),²⁷ the mass surveillance measures and obligations established by the Directive have been controversial from the outset. The complex legislative debate at the EU level and the doubts expressed by the Article 29 Working Party²⁸ and numerous NGOs²⁹ had a significant impact. In several Member States, the domestic laws implementing the DRD were challenged before the national courts, which were asked to assess the compatibility of a bulk retention regime with national fundamental rights and principles.³⁰ In most cases, the relevant

²⁵See European Commission, *Extended Impact Assessment – Annex to the Proposal for a Directive of the EU 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*, COM(2005)438 final – SEC/2005/1131, Sept. 21, 2014.

²⁶Mark Taylor, *The EU Data Retention Directive*, 22 *COMPUTER L. & SEC. REPORT* 309 (2006); Eleni Kosta & Peggy Valcke, *Retaining the Data Retention Directive*, 22 *COMPUTER L. & SEC. REPORT* 371 (2006); Francesca Bignami, *Privacy and Law Enforcement in the European Union: The Data Retention Directive*, *CHICAGO JOURNAL OF INTERNATIONAL LAW, DUKE SCIENCE, TECHNOLOGY & INNOVATION PAPER* No. 13 (2007); Theodore Konstadinides, *Destroying Democracy on the Ground of Defending it? The Data Retention Directive, the Surveillance State and our Constitutional Ecosystem*, 1 *EUR. CURRENT L. ISSUE* XI (2012).

²⁷Case C-301/06, *Ireland v. European Parliament and Council of the European Union*, 2009 E.C.R. I-00593. See Ester Herlin-Karnell, *Annotation of Ireland v. Parliament and Council*, 46 *Comm. Mark. L. Rev.* 1667 (2009); Theodore Konstadinides, *Wavering between Centres of Gravity: Comment on Ireland v. Parliament and Council*, 35 *Eur. L. Rev.* 88 (2010); Sara Poli, *The Legal Basis of Internal Market Measures with a Security Dimension: Comment on Case C-301/06*, 6 *EUR. CONST. L. REV.* 153 (2010).

²⁸Article 29 Data Protection Working Party, *Opinion 4/2005 on the 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 (COM(2005)438 final of 21.09.2005, 1868/05, WP 113, Oct. 21, 2005; see also EDPS, Opinion of the European Data Protection Supervisor on the 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 (COM(2005) 438 final), 2005/C 298/01, Sept. 26, 2005. See also Lukas Feiler, *The legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection*, 1 *EUR. J. OF L. & TECH.* 1 (2010).*

²⁹See on this point Chris Jones & Ben Hayes, *The EU Data Retention Directive: A Case Study on the Legitimacy and Effectiveness of EU Counter-Terrorism Policy*, *SECURING EUROPE THROUGH COUNTER-TERRORISM – IMPACT, LEGITIMACY & EFFECTIVENESS PAPER* (2013).

³⁰Eleni Kosta, *The Way to Luxembourg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection*, 3 *SCRIPTed* 339 (2013); Ludovica Benedizione & Eleonora Paris, *Preliminary Reference and Dialogue between Courts as Tools of Reflection on the EU System of Multilevel Protection of Rights: The Case of the Data Retention Directive*, 16 *GERMAN L.J.* 1727 (2015).

judicial decisions on mass surveillance and blanket data retention measures were declared to be a disproportionate intrusion into the private sphere. Notwithstanding the different approaches,³¹ this case law revealed an important opportunity for national judges to deal with the profound issues of a generalized surveillance system, particularly the need for precise guarantees and limits to restrict intrusive measures.

Even though none of these national decisions considered the validity of the Directive itself, this piece of EU legislation was challenged before the CJEU soon after. What is now defined as the “data retention saga,” which is continuing nowadays, represents, together with the important judicial impulses coming from national courts, the most significant stimulus to the constitutional debate over data retention systems in the EU, promoting a complex process of constitutionalization of mass surveillance regimes in general. In fact, in the landmark *Digital Rights Ireland* decision,³² the CJEU affirmed some crucial and unprecedented principles on mass surveillance systems. First, generalized and indiscriminate metadata retention, independently from potential subsequent access to the retained data by state authorities, was considered an invasion of users’ private life *per se*. The Court recognized that communications data, regardless of the content of the communication itself, may allow precise conclusions on users’ habits, everyday life, place of residence, daily movements, activities, relationships, and social environments, which can generate “in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance” (paragraph 37). By demonstrating a profound awareness of the possible risks and consequences related to the existence of massive retention systems, even if motivated by security purposes, the Court noted that mandatory *bulk* and generalized retention, covering *all* electronic communications services as well as the *entirety* of users and communications data produced, could not represent a measure limited to what is strictly necessary. The Court underlined that a form of legitimate and proportionate retention could only be identified in a *targeted* regime, which means a retention limitedly affecting people for whom there is evidence capable of “suggesting that their conduct might have a link, even an indirect or remote one, with serious crime” (paragraph 58), or specifically limited to a geographic area and/or a time period and at the unique purpose of preventing or fighting against *serious* crimes. The lack of these limitations, regarded as essential to ensure a legitimate and proportionate compression of individuals’ fundamental rights, determined the invalidation of the DRD.

By defining a clearer standard for the future development of mass surveillance techniques in the EU, the CJEU determined that security purposes, even when motivated by terrorist threats, cannot be placed outside the constitutional human rights guarantee framework established by national constitutional charters and supranational fundamental rights declarations.³³ In their decision, the EU judges affirmed some limits and conditions on surveillance mechanisms by prompting the adoption of targeted measures in clear contrast with the generalized dimension of massive surveillance systems.

With the invalidation of the DRD, Article 15 of the e-Privacy Directive once again became the only piece of EU law that regulated the possibility of retaining communications data for security

³¹Eleni Kosta, *The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection*, 3 SCRIPTed 339 (2013); Ludovica Benedizione & Eleonora Paris, *Preliminary Reference and Dialogue between Courts as Tools of Reflection on the EU System of Multilevel Protection of Rights: The Case of the Data Retention Directive*, 16 GERMAN L.J. 1727 (2015).

³²Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources et al.*, (Apr. 8, 2014), <http://curia.europa.eu/>.

³³Marie-Pierre Granger & Kristina Irion, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection*, 16 *European Law Review* 849 (2014); Orla Lynskey, *The DRD Is Incompatible With the Rights to Privacy and Data Protection and Is Invalid in its Entirety: Digital Rights Ireland*, COMM. MARK. L. REV. 1789 (2014); Federico Fabbrini, *Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the United States*, 28 HARV. HUM. RTS. J. 65 (2015).

purposes, with Member States soon adopting different approaches to data retention discipline. National courts were once again asked to evaluate the compliance of internal data retention regimes with national and EU fundamental rights, as interpreted by the CJEU.³⁴ Doubts and criticalities emerged again concerning competence matters and the proportionality of national bulk data retention systems. The attention and activism on this topic reflected the difficulty, also for national judges, in determining a correct balance between security needs, supposedly better guaranteed by bulk surveillance instruments, and protecting rights and freedoms.

In light of the different and fragmented reactions of national courts and legislators, several preliminary rulings were promoted by Swedish, British, and Spanish courts, all asking for clarifications as to the interpretation of Article 15 of the e-Privacy Directive. In the important *Tele2*³⁵ and *Ministerio Fiscal*³⁶ cases, the CJEU reaffirmed the principles already established in *Digital Rights Ireland*, stressing that national provisions on data retention and access to retained communications data for security purposes fall entirely within the scope of application of EU law. In all these cases, in which the EU Court was first confronted with surveillance tools, the judges acted as constitutional “lawmakers,” giving very precise indications to national legislators,³⁷ prompting the incorporation of core constitutional values such as the rule of law, due process guarantees, and the presumption of innocence into the discipline regulating data retention. By explicitly declaring that Article 15 of the e-Privacy Directive, read in light of the CFREU, must be interpreted as precluding national legislation from providing general and indiscriminate retention of all traffic and location data of all users, including all means of electronic communication, the Court reiterated the importance of clear and precise rules for establishing a form of *targeted* data retention regime, together with strict rules and prior control regulating access to data by law enforcement or intelligence authorities.³⁸

II. Constitutional Fine-Tuning: Security and the Ban of ‘Systematic’ Mass Surveillance

Notwithstanding the important constitutionalization path of the data retention surveillance instrument promoted by the abovementioned CJEU case law, Member States demonstrated a reticent approach; they were reluctant to abandon bulk regimes perceived as invaluable and irreplaceable tools in the fight against national and transnational security threats.³⁹ The solution of targeted data retention, highly criticized for its limited efficacy and potential discriminatory

³⁴Franziska Boehm & Mark D. Cole, *Data Retention after the Judgement of the Court of Justice of the European Union*, THE GREENS IN THE EP WORKING PAPER (2014), https://www.zar.kit.edu/DATA/veroeffentlichungen/237_237_Boehm_Cole-Data_Retention_Study-June_2014_1a1c2f6_9906a8c.pdf, last accessed 20 October 2022; Xavier Tracol, *Legislative Genesis and Judicial Death of a Directive: the European Court of Justice Invalidated the Data Retention Directive (2006/24/EC) Thereby Creating a Sustained Period of Legal Uncertainty about the Validity of National Laws which Enacted it*, 30 COMPUTER L. & SEC. REV. 736 (2014); Jürgen Kuhling & Sonja Heitzer, *Returning Through the National Back Door? The Future of Data Retention After the ECJ Judgement on Directive 2006/24 in the UK and Elsewhere*, 40 EUR. L. REV. 263 (2015); Niklas Vainio & Samuli Miettinen, *Telecommunications Data Retention After DR: Legislative and Judicial Reactions in the Member States*, 23 INT’L J. OF L. & INFO. TECH. 290 (2015); Lucia Zedner, *Why Blanket Surveillance Is No Security Blanket. Data Retention in the UK After the European Data Retention*, in RUSSELL A. MILLER, ed., PRIVACY AND POWER. A TRANSATLANTIC DIALOGUE IN THE SHADOW OF THE NSA AFFAIR 564-85 (2017); Privacy International, *2017 National Data Retention Laws Since the CJEU’s Tele2/Watson Judgement. A Concerning State of Play for the Right to Privacy in Europe*, Sep. 2017, https://privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf, last accessed 20 October 2022.

³⁵See Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post-och telestyrelsen PTS et al.*, (Dec. 21, 2016), <http://curia.europa.eu/>.

³⁶Case C-207/16, *Ministerio Fiscal*, (Oct. 2, 2018), <http://curia.europa.eu/>.

³⁷David Fennelly, *Data Retention: the Life, Death and Afterlife of a Directive*, 19 ERA PAPER 1 (2018).

³⁸Xavier Tracol, *The Judgement of the Grand Chamber Dated 21 December 2016 in the Two Joint Tele2 Sverige and Watson Cases: The need for a harmonised legal framework on the retention of data at EU level*, 33 COMPUTER L. & SEC. REV. 541 (2017).

³⁹See section B. II.

impact,⁴⁰ was not implemented at the national level.⁴¹ The vast majority of governments, legislators, and, in some cases, courts⁴² adopted a “defensive” approach, trying to promote an interpretation of the CJEU case law that would not definitively ban generalized and indiscriminate retention systems but provide these regimes with stronger and more precise rules governing the access phase by state authorities. This erosion of the stringent principles declared in the data retention saga raised strong criticisms in civil society and NGOs. They considered national legislation that allowed mass surveillance instruments to be *per se* incompatible with the fundamental rights guaranteed by the CFREU as interpreted by the CJEU judgments on the topic.

In an impressive number of cases,⁴³ the divergent views expressed in front of national courts led to a request for the intervention of the CJEU, underlining how the limits and safeguards described in the previous case law produced controversial effects and required clearer explanations. In particular, governments, law enforcement authorities, and, in some cases, national courts asked the CJEU to “clarify, refine or even reconsider various aspects of its case law,”⁴⁴ arguing that strict safeguards and limits on access to data would be sufficient to balance the interference produced by generalized and indiscriminate retention. In all these decisions, EU judges pronounced unprecedented and crucial principles destined to influence the employment of mass surveillance techniques.

Having reiterated that mass surveillance techniques cannot be exempted from the control of EU law and the CJEU,⁴⁵ the judges strongly reaffirmed that *bulk* data retention for public security purposes – namely, the fight against serious crimes – cannot be considered proportionate and legitimate. By identifying targeted data retention as the only form of surveillance allowed, the Court refused to accept alternative retention regimes such as the *restricted* one⁴⁶ and decided not to succumb to the strong and profound criticism governments and law enforcement authorities expressed on the effectiveness and non-discriminatory nature of the targeted solution. If these positions represented a clear reaffirmation of the principles established in the previous case law, the most innovative part of these recent decisions – in particular those of October 2020 – was the one recognizing a sort of mitigation of the previous approach, highlighting the ongoing and still evolving nature of the process of constitutionalization performed by the Court. Protecting national security from serious threats such as terrorism or other activities capable of destabilizing a country’s fundamental constitutional, political, economic, or social structures provides Member States with wider maneuvering room. The seriousness of this objective may justify even more severe interferences with fundamental rights, including bulk data retention techniques.⁴⁷

⁴⁰See Cameron, *supra* note 21; see also Consultative Forum of Prosecutors General and Directors of Public Prosecutors of the Member States, REPORT ON DATA RETENTION IN THE FIGHT AGAINST SERIOUS CRIME: THE WAY FORWARD, Dec. 11, 2015.

⁴¹Eurojust, *Data Retention Regimes in Europe in Light of the CJEU Ruling of 21 December in Joined Cases C-203/15 and C-698/15*, Nov. 6, 2017.

⁴²MAREK ZUBIK, JAN PODKOWIK & ROBERT RYBSKI, eds., EUROPEAN CONSTITUTIONAL COURTS TOWARDS DATA RETENTION LAWS (2020).

⁴³Case C-623/17, *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs et al.*, (Oct. 6, 2020), <http://curia.europa.eu/>; Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net et al. v. Premier Ministre et al.*, (Oct. 6, 2020), <http://curia.europa.eu/>; Case C-746/18, *H.K. v Prokuratuur*, (Mar. 2, 2021), <http://curia.europa.eu/>; Case C-140/20, *G.D. v. The Commissioner of the Garda Síochána et al.*, (Apr. 5, 2022), <http://curia.europa.eu/>; Joined Cases C-793/19, *SpezNet AG et al. v. Federal Republic of Germany et al.*, (Sept. 20, 2022), <http://curia.europa.eu/>; C-350/21 *Spetsializiran nakazatelen sad (Bulgaria)*, (Nov. 17, 2022), <http://curia.europa.eu/>.

⁴⁴Opinion of the Advocate General Campos Sanchez-Bordona at para. 69,70, Case C-520/18, *La Quadrature du Net et al. v. Premier Ministre et al.* (Jan. 15, 2020), <http://curia.europa.eu/>. Europol also proposed the alternative option of the “restricted data retention regime”, which represent a more intrusive and a more effective solution if compared to the “targeted data retention,” but which also results as less generalized relative to “bulk data retention” (on this point see Europol, *Proportionate Data Retention for Law Enforcement Purposes*, WK 9957/2017, Sept. 21, 2017).

⁴⁵*La Quadrature du Net*, Joined Cases C-511/18, C-512/18, and C-520/18 at para. 99.

⁴⁶As proposed by Europol, *supra* note 44.

⁴⁷*La Quadrature du Net*, Joined Cases C-511/18, C-512/18 and C-520/18 at paras 134 and 139. Consider the approach taken by the European Court of Human Rights in surveillance-related cases, which seems to be partly similar and partly divergent:

Although this affirmation can appear as a major victory for governments and public authorities vocally invoking the possibility of adopting forms of massive surveillance and retention, the Court carefully and precisely specified all the limits and conditions to harness the use of such a highly invasive instrument. We can identify a further constitutionalizing effort by the CJEU, which introduced constitutional safeguards and boundaries by requiring national legislators to determine: (i) a precise legislative framework disciplining the possibility of adopting bulk data retention regimes; (ii) a specific time limit to the use of this instrument; (iii) rigorous data security safeguards able to protect from the risks of abuses; and (iv) control by courts or independent administrative bodies. Moreover, the Court specified that a bulk data retention regime could never be admitted in the context of the fight against serious crime, while it can be justified to face national security threats; However, even in this case, it cannot be systematic in nature, and its adoption has to be subordinate to the existence of serious, real, present, or at least foreseeable, threats to national security.⁴⁸ Although the guarantee of national security is considered vital, reaching this critical objective cannot be untied from respect for the rule of law, which notably is

characterized first and foremost by the requirement that power and strength are subject to the limits of the law and, in particular, to a legal order that finds in the defense of fundamental rights the reason and purpose of its existence. (. . .) If it simply gave primacy to mere effectiveness, a State based on the rule of law would lose that distinguishing quality and might, in extreme cases, itself become a threat to the citizen. If the public authorities were armed with a panoply of instruments of criminal prosecution such as to enable them to disregard or violate fundamental rights, there would be no way of ensuring that their uncontrolled and entirely unfettered actions would not operate ultimately to the detriment of everyone's freedom.⁴⁹

The Court tried to establish a correct balance between the need to safeguard national and public security effectively and to ensure the respect of the democratic bases of our societies. This balancing exercise passed through a progressive constitutionalization of data retention regimes, through which the Court pushed national legislators and EU institutions towards adopting constitutional principles able to determine the limits of acceptability and the justifiability of fundamental rights' compression for both public and national security purposes.⁵⁰

Centrum For Rattvisa v. Sweden, App. No. 35252/08 and *Big Brother Watch et al. v. UK*, App. No. 58170/13, 62322/14 and 24960/15, both decided by the Grand Chamber on May 25, 2021; Vera Rusinova, *A European Perspective on Privacy and Mass Surveillance at the Crossroads*, WORKING PAPERS HSE (2019); Plixavra Vogiatzoglou, *Centrum For Rattvisa v. Sweden: Bulk Interception Communications by Intelligence Services in Sweden Does Not Violate the Right to Privacy*, 4 EUR. DATA PROT. L. REV. 1 (2019); Bart Van der Sloot & Eleni Kosta, *Big Brother Watch and others v. UK: Lessons From the Latest Strasbourg Ruling on Bulk Surveillance*, 2 EUR. DATA PROT. L. REV. 1 (2019); Asaf Lubin, *Big Brother Watch v UK*, INTERNATIONAL LEGAL MATERIALS 1 (2019).

⁴⁸*La Quadrature du Net*, Joined Cases C-511/18, C-512/18 and C-520/18 at para. 138.

⁴⁹Opinion of the Advocate General Campos Sanchez-Bordona, at para. 130, Case C-520/18, *La Quadrature du Net et al. v. Premier Ministre et al.* (Jan. 15, 2020).

⁵⁰For an in-depth analysis of these decisions, see Iain Cameron, *Metadata Retention and National Security: Privacy International and La Quadrature du Net*, 58 COMM. MARK. L. REV. 1433 (2021); Antonio Caiola, *Transmission and Retention of Data in Relation to National Security: Clarifications and Nuances Emerging in Case Law*, 4 REVUE DES AFFAIRES EUROPÉENNES 923 (2020); Monika Zalnieriute, *A Struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of the EU*, 85 MODERN L. REV. 1 (2021). All the indicated principles established by the 2021 CJEU decisions have been vastly confirmed in *H.K., C-746/18, G.D. v. The Commissioner of the Garda Síochána et al.*, C-140/20 as well as, more recently, in Joined Cases C-793/19, *SpeceNet AG et al. v. Federal Republic of Germany et al.*, (Sept. 20, 2022), <http://curia.europa.eu/>. On these decisions, which added some interesting evaluations on the access to retained data phase, see Sophia Rovelli, *Case Prokuratuur: Proportionality and the Independence of Authorities in Data Retention*, 6 EUROPEAN PAPERS 199 (2021); Maximilian Gerhold, *Rote Ampel für Geisterfahrer*, VERFASSUNGSBLOG, Sept. 21, 2022, <https://verfassungsblog.de/rote-ampel-fur-geisterfahrer/>, last accessed 20 October 2022.

To conclude this overview of the CJEU's contribution to the constitutionalization of mass surveillance practices in the EU, it is worth mentioning that the data retention saga did not represent the only case in which the CJEU was asked to deal with mass surveillance. The CJEU jurisprudence concerning the transfer of personal data collected in European territory and directed outside EU borders confirmed the profound impact on fundamental rights produced by massive collection, retention, and access to personal data operated by public authorities, even when motivated by security purposes concerning third countries.⁵¹ In the Schrems I and Schrems II cases, the CJEU indirectly analyzed the intrusiveness of American mass surveillance systems such as Prism and Upstream by twice invalidating the adequacy decisions regarding data transfers to the US. Considering these provisions, the Court stated that "legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter,"⁵² while a law not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection (Article 47 CFREU).

In the *Schrems* saga, the Court tried to transpose the constitutional principles and guarantees already affirmed inside EU territory in cases wherein the surveillance is perpetrated by foreign authorities, with a complex and – from some aspects – questionable approach.⁵³ Similarly, in its Opinion 1/15, the CJEU invalidated the draft PNR agreement with Canada concerning transferring and processing EU passengers' PNR data to Canadian law enforcement and security authorities. Here, the Court clearly reaffirmed the necessity of a connection or at least an indirect link between a possible threat and the retention, accessing, and processing of personal data, as well as the need for specific and precise safeguards guaranteeing the adequate protection of data

⁵¹As affirmed in C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, (Oct. 6, 2015) and in C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, (July 16, 2020), <http://curia.europa.eu/>, the so-called "Schrems saga". On data transfer decisions, see Maria Tzanou, *EU Regulation of Transatlantic Data Transfers and Online Surveillance*, 17 HUM. RTS L. REV. 545 (2015); DAVID COLE, FEDERICO FABBRINI & STEPHEN SCHULHOFER, eds., *SURVEILLANCE, PRIVACY AND TRANS-ATLANTIC RELATIONS* (2015); Sergio Carrera & Elspeth Guild, *The End of Safe Harbour: What Future for EU-US Data Transfer?*, 3 MAASTRICHT J. OF EUR. & COMPARATIVE L. 651 (2015); Gert Vermeulen, *The Privacy Shield's Blunt Denial of Continued Bulk, Mass or Indiscriminate Collection or Processing and Unnecessary or Disproportionate Access and Use by US Intelligence and Law Enforcement Authorities* in GERT VERMEULEN & EVA LIEVENS, eds., *DATA PROTECTION AND PRIVACY UNDER PRESSURE. TRANSATLANTIC TENSIONS, EU SURVEILLANCE AND BIG DATA*, 49 (2017); Fabien Terpan, *EU-US Data Transfer from Safe Harbour to Privacy Shield: Back to Square One?*, 3 EUROPEAN PAPERS 1058 (2018); Francesca Bignami, *Schrems II: the Right to Privacy and the New Illiberism*, 3 MEDIA LAWS 308 (2020); Oreste Pollicino, *Diabolical Persistence. Thoughts on the Schrems II Decision*, 3 MEDIA LAWS 315 (2020); FEDERICO FABBRINI, EDOARDO CELESTE & JOHN QUINN, eds., *DATA PROTECTION BEYOND BORDERS: TRANSATLANTIC PERSPECTIVES ON EXTRATERRITORIALITY AND SOVEREIGNTY* (2021).

⁵²*Maximillian Schrems*, C-362/14 at para. 94.

⁵³See Richard A. Epstein, *The ECJ's Fata Imbalance: Its Cavalier Treatment of National Security Issues Poses Serious Risk to Public Safety and Sound Commercial Practices*, 12 EUR. CONST. L. REV. 339 (2016); Christopher Kuner, *Reality and Illusion in the EU Data Transfer Regulation Post Schrems*, 4 GERMAN L.J. 898 (2017); Serena Crespi, *The Applicability of Schrems Principles to the Member States: National Security and Data Protection Within the EU Context*, 43 EUR. L. REV. 669 (2018); Luca Pietro Vanoni, *Balancing Privacy and National Security in the Global Digital Era: A Comparative Perspective of the EU and US Constitutional Systems*, in LORENZA VIOLINI & ANTONIA BARAGGIA, eds., *THE FRAGMENTED LANDSCAPE OF FUNDAMENTAL RIGHTS PROTECTION IN EUROPE*, 114 (2018); Jan X. Dhont, *Schrems II. The EU Adequacy Regime in Existential Crisis?*, 5 MAASTRICHT J. OF EUR. & COMPARATIVE L. 601 (2019); Edoardo Celeste, *The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios*, 1 EUR. CONST. L. REV. 134 (2019); Giulia Formici, *The External Dimension of the European Rule of Law in the Digital Age: An Analysis Through the Lens of the ECJ Case-Law on Data Transfer*, 6 CAHIERS JEAN MONNET, 215 (2020); Ira Rubinstein & Peter Margulies, *Risk and Rights in Transatlantic Data Transfers: EU Privacy Law, US Surveillance and the Search for Common Ground*, ROGER WILLIAMS UNIVERSITY LEGAL STUDIES PAPER, Feb. 18 (2021).

outside EU borders.⁵⁴ The attention and relevance attributed to retention, concerning not only communications data but also other information such as PNR, clearly emerged from the numerous proposed preliminary rulings regarding the validity of the PNR Directive,⁵⁵ challenging its legitimacy based on the “constitutional” principles emerging from the data retention and *Schrems* saga.⁵⁶

D. Advancing in the Path of Constitutionalization? Legislative Inertia and Future Scenarios

The reiterated intervention of the CJEU in the field of data retention and data transfers demonstrates the profound questions and the complex debate caused by the use of mass surveillance techniques. Member States have reacted in very different ways to the ongoing path of constitutionalization launched by the EU judges, creating a fragmented landscape of solutions and approaches. For example, following the October 2020 decisions, the Belgian Constitutional Court⁵⁷ annulled national legislation regulating data retention, considering the bulk nature of that regime as fundamentally incompatible with the principles affirmed by the CJEU. The Belgian Government then proposed a reform to create a targeted data retention system based on geographical criteria, differentiated according to the threat authorities are asked to face; that is, different levels of danger associated with varying degrees of legitimate intrusion into the private sphere.⁵⁸ With this attempt, the Belgian

⁵⁴Opinion 1/15 (Grand Chamber), July 26, 2017, <http://curia.europa.eu/>. See Christopher Docksey, *Opinion 1/15 Privacy and Security, Finding the Balance*, 6 MAASTRICHT J. OF EUR. & COMPARATIVE L. 768 (2017); Arianna Vedaschi, *Privacy and Data Protection Versus National Security in Transnational Flights: The EU-Canada PNR Agreement*, 2 INT'L DATA PRIVACY L. 124 (2018); Xavier Tracol, *Opinion 1/15 of the Grand Chamber Date 26 July 2017*, 34 COMPUTER L. & SECURITY REV. 830 (2018); Valentin M. Pfisterer, *The Right to Privacy. A Fundamental Right in Search of Its Identity: Uncovering the CJEU's Flawed Concept of the Right to Privacy*, 20 GERMAN L.J. 722 (2019).

⁵⁵EU Directive 2016/681 of April 27, 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, O.J. 2016 L 119/132.

⁵⁶Even if the recent decision C-817/19, *Ligue des Droits Humains v. Conseil des Ministres*, (June 1, 2022), <http://curia.europa.eu/>, has not declared the retention of PNR data concerning all passengers of extra-EU flights *per se* incompatible with EU law and in particular with Articles 7 and 8 CFREU, the judges have nonetheless provided a “restrictive” interpretation of some specific provisions of Directive 2016/681 – and consequently of the national legislations implementing it. A general retention of PNR data for a period of five years, “applicable indiscriminately to all air passengers, including those for whom neither the advance assessment under Article 6(2)(a) of that directive nor any verification carried out during the period of six months referred to in Article 12(2) of the said directive nor any other circumstance have revealed the existence of objective evidence capable of establishing a risk that relates to terrorist offences or serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air” cannot be considered as compliant with EU law. Furthermore, national legislation is precluded from imposing “in the absence of a genuine and present or foreseeable terrorist threat with which the Member State concerned is confronted (. . .) a system for the transfer, by air carriers and tour operators, as well as for the processing, by the competent authorities, of the PNR data of all intra-EU flights and transport operations carried out by other means within the European Union, departing from, going to or transiting through that Member State, for the purposes of combating terrorist offences and serious crime”. The necessity to justify the intrusive data retention and processing, applied to the PNR data transfer discipline, seems to confirm the ongoing constitutionalisation of surveillance instruments provided by the CJEU. Also, in this case, by evaluating the different interests at stake – in particular the fight against terrorism – the Court does not deny the PNR data transfer *tout court* but promotes a balance to consider the need to limit unjustifiable and excessive interferences into passengers’ private lives. Subsequently to the *Ligue des Droits Humains* decision, the proposed and – at that time – pending preliminary rulings (C-148/20, *AC v. Deutsche Lufthansa AG* lodged on Jan. 20, 2020; C-150/20, *BD v. Deutsche Lufthansa AG*, lodged on Mar. 17, 2020; C-215/20 *JV v. Federal Republic of Germany*, lodged on May 19, 2020; C-222/20, *OC v. Federal Republic of Germany*, lodged on May 27, 2020) were removed from the register, after the *Verwaltungsgericht Wiesbaden* decided not to confirm the preliminary ruling request.

⁵⁷Belgian Constitutional Court, *Arrêt* 57 of Apr. 22, 2021.

⁵⁸The *Avant-Project de Loi*, 7 May 2021 was approved by the Belgian parliament in July 2022 (*Loi 20 Juillet 2022 Loi relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités*); for an in-depth analysis of the issues still identifiable in the new legislation, mainly linked to the fear that the criteria and conditions for a targeted data retention could be too vast and vague, thus allowing a *de facto* bulk data retention : see *Ligue des Droits Humains, Avis de la Ligue des Droits Humains sur le projet de*

Government demonstrated its willingness to renounce the bulk data retention instrument for public security purposes, trying to conform its national legislation to the constitutional principles and proportionality evaluations promoted by the CJEU data retention case law as well as confirmed by national courts – the Belgian Constitutional Court had already annulled a national data retention law in the aftermath of the *Digital Rights Ireland* decision.⁵⁹

Compared with Belgium, France adopted a very different approach. On April 21, 2021,⁶⁰ the Conseil d'État considered France's national law providing a generalized data retention regime for national security purposes compliant with EU legislation and the CFREU – except for some specific provisions or omissions, such as the lack of a preliminary control by an independent authority and the lack of a periodic review aiming at verifying the persistence of serious, present, or foreseeable risks to national security. Embracing a permissive interpretation of the stringent requirements imposed by the CJEU,⁶¹ the French judges recognized the impossibility of adopting a targeted data retention regime, as suggested by the CJEU, considering it unfeasible to determine in advance the possible geographical areas, subjects, or categories of data that could be useful for preventing or investigating serious crimes. These considerations appear in clear contrast with the solutions proposed by the Belgian government and the Belgian Constitutional Court, which clearly made efforts to go in the direction of the requirements indicated by the CJEU case law.

While the abovementioned landmark decisions adopted by the CJEU caused diverse legislative and judicial reactions all over Europe, there are countries where this case law has not produced a significant impact. In Italy, for instance, the debate on the proportionality and legitimacy of data retention was not fully considered by either the Italian legislator or the national courts. Only in recent times, after the CJEU decision in *H.K. v. Prokuratuur*, the Tribunale di Rieti decided to promote the first preliminary ruling related to data retention and access regime in Italy,⁶² prompting an unprecedented but highly awaited multilevel dialogue between national and supranational courts.⁶³ This decision represents a significant novelty compared to the Italian Supreme Court approach, which had always considered the national data retention legislation perfectly compliant with the complex and highly discussed CJEU requirements.⁶⁴ Considering the

loi du 17 mars 2022 relatif à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités, May 2022, <https://www.liguedh.be/wp-content/uploads/2022/05/Avis-LDH-DATA-RETENTION-2022-final.pdf>, last accessed 20 October 2022; EDRI, *Letter addressing the draft law on the collection and retention of identification data and metadata in the electronic communications sector and the provision of such data to authorities*, June 2022, https://edri.org/wp-content/uploads/2022/06/EDRI-Liga-Letter-Draft-Law-Data-Retention-BE_EN.pdf, last accessed 20 October 2022.

⁵⁹Belgian Constitutional Court, *Arrêt* 84 of June 11, 2015; see Laurens Naudts, *Belgian Constitutional Court Nullifies Belgian Data Retention Law*, 3 EUR. DATA PROT. L. REV. 210 (2015); Fanny Coudert & Verbruggen, *Conservation des Données de Communications Électronique en Belgique: Un Juste Équilibre?*, in DANIEL FRANSSSEN & VANESSA FLORE, eds., SOCIÉTÉ NUMÉRIQUE ET DROIT PÉNAL, 248 (2019).

⁶⁰French Conseil d'État, Decision n. 393099 of Apr. 21, 2021; Loïc Azoulai & Dominique Ritzler, *L'État c'est moi. Le Conseil d'État, la sécurité et la conservation des données*, 2 REVUE TRIMESTRIELLE DE DROIT EUROPÉEN 349 (2021); Matthieu Audibert, *Conservation des données de connexion. Comment le Conseil d'État a sauvé la majorité des enquêtes judiciaires*, 96 VIEILLE JURIDIQUE 16 (2021); Araceli Turmo, *National Security as an Exception to EU Data Protection Standards: The Judgment of the Conseil d'État in French Data Network and Others*, HAL OPEN SCIENCE, Apr. 1, 2022.

⁶¹Arianna Vedaschi, "Customizing" *La Quadrature du Net: the French Council of State, National Security and Data Retention*, BRIDGE BLOG, May 5, 2021, <https://bridgenetwork.eu/2021/05/05/customizing-la-quadrature-du-net-the-french-council-of-state-national-security-and-data-retention/>, last accessed 20 October 2022.

⁶²Request for a preliminary ruling C-334/21 from the Tribunale di Rieti, lodged on May 26, 2021. The case has been closed after the withdrawal request made by the Tribunale di Rieti. As will be explained, this decision became necessary after a legislative reform modified the provision on which the preliminary ruling was based.

⁶³Luca Lupària, *Data retention e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, 4 GIURISPRUDENZA PENALE 757 (2019); GIULIA FORMICI, LA DISCIPLINA DELLA DATA RETENTION TRA ESIGENZE SECURITARIE E TUTELA DEI DIRITTI FONDAMENTALI. UN'ANALISI COMPARATA (2021); Ufficio del massimario e del ruolo, Servizio penale, Corte Suprema di Cassazione, *Relazione su novità normativa. Misure urgenti in tema di acquisizione dei dati relativi al traffico telefonico e telematico a fini di indagine penale*, Oct. 13, 2021.

⁶⁴See, among the others, Italian Corte di Cassazione, decision no. 10022 of Nov. 10, 2020.

intense debate generated by the approach promoted by the Tribunale di Rieti, the Italian legislature decided to intervene. In November 2021, a significant reform was approved by the parliament,⁶⁵ which modified the data access regime by introducing, for the first time, a prior control by a judge as well as a specific list of serious crimes legitimizing access to metadata. However, despite these changes, which promoted more stringent guarantees and ultimately greater compliance with the CJEU requirements regarding the access procedure, the Italian legislator decided not to reform the core architecture of its data retention regime. In Italy, current legislation establishes a retention period of seventy-two months without distinguishing between national security purposes or public security objectives and confirms a bulk and generalized data retention system. These provisions contrast with the specific limits established by the CJEU case law yet are still in place despite strong criticism by the Italian Data Protection Authority, academics, and experts.⁶⁶

The reactions and lively debate on the path of constitutionalization developed by the CJEU on data retention and mass surveillance, more generally, are still expanding. In April 2022, the Portuguese Constitutional Court declared many articles of the so-called metadata law,⁶⁷ adopted in accordance with the DRD provisions, unconstitutional.⁶⁸ It took several years for Portuguese constitutional judges to adopt such a decision, preceded by a lively political and judicial discussion that had brought, in the past, the same Court to express a very different position on the national data retention legislation. In Case no. 420/2017, the Portuguese judges (mainly) confirmed the legitimacy of bulk retention of basic metadata, for example, name and IP address. They relied on the Public Prosecutor's Cybercrime Office affirmations, according to which the "Digital Rights ruling should not impair the bulk retention of metadata under Law 32/2008," because "retention must be indiscriminate," and "must include all citizens."⁶⁹ Overcoming these positions, the 2022 decision opened a different and more careful approach to mass surveillance instruments in Portugal, prompting a serious debate on a renewed data retention legal framework and its proportionality. Once again, this example reveals, on the one hand, the key role played by the CJEU case law and, on the other hand, the difficulty for national legislators and Courts to promote a profound debate and normative process on how to constitutionalize surveillance tools that could incorporate fundamental rights protection and paramount constitutional principles successfully.⁷⁰

⁶⁵Law n. 178, 23 November 2021. See 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*, 1 OSSERVATORIO COSTITUZIONALE 125 (2022).

⁶⁶Garante per la Protezione dei Dati Personali, *Segnalazione sulla disciplina della conservazione, a fini di giustizia, dei dati di traffico telefonico e telematico*, Aug. 2, 2021; Federica Resta, *La nuova disciplina dell'acquisizione dei tabulati*, GIUSTIZIA INSIEME, Oct. 2, 2021.

⁶⁷Lei no. 32/2008 de 17 de Julho, *Consevacao de dados gerados ou tratados no contexto oferta de servicos de comunicacoes electronicas*.

⁶⁸Case no. 268/2022.

⁶⁹Francisco Pereira Coutinho, *Better Late than Never: Blanket Data Retention Struck Down at Last by the Portuguese Constitutional Court*, DIRITTI COMPARATI, June 21, 2022, <https://www.diritticomparati.it/better-late-than-never-blanket-data-retention-struck-down-at-last-by-the-portuguese-constitutional-court/>, last accessed 20 October 2022.

⁷⁰Similar considerations could be made with respect to Germany. After the September 2022 decisions (the already mentioned C-793/19 and C-794/19), an intense political debate has been boosted in order to approve a new legislative framework on data retention. This was not the first time the German Parliament was called to discuss this complex discipline. After the 2010 German Federal Constitutional Court decision determining the illegitimacy of the data retention law, a long and profound political debate led to a more stringent normative solution, providing for more guarantees – especially with regard to the duration of the retention – that established, nonetheless, generalized data retention. Following the CJEU intervention, the current legislative discussion also introduced a new instrument potentially able to safeguard security needs and, at the same time, solve some of the criticalities characterizing the retention regime. The Federal Minister of Justice, in fact, proposed the adoption of a "quick freeze" procedure. Law enforcement authorities could use this tool to impose communication service providers to retain data concerning a specific geographic area or population if an initial suspicion arose. The information retained could later be "unfrozen" if the suspicion is confirmed by subsequent investigation. It will be

The varied but cautious and reluctant approaches adopted by Member States following the CJEU rulings in this field clearly emerge when analyzing the e-Privacy Regulation proposal, which aims to modify the existing and quite outdated e-Privacy Directive. The text, approved by the EU Council in February 2021 and currently subject to the legislative procedure, includes a specific provision⁷¹ aimed at excluding from the scope of the application of the e-Privacy Regulation and EU law, more generally, all data processing procedures intended to protect national security, thus bypassing the application of the CJEU's stringent requirements, and potentially representing a stop to the path of constitutionalization described above.⁷² The debate on adopting this new Regulation is still ongoing. It has encountered several difficulties and forced stops due to the lack of consensus between Member States and between different EU Institutions on some thorny issues. Data retention discipline is one of them.

The CJEU's impulses on the surveillance debate in the EU and its Member States are questioned for different and opposing reasons. Several governments and legislators, sometimes even courts, considered the EU judges proportionality test on data retention too strict and the proposed limits and solutions, such as the targeted data retention, unfeasible or useless. On the contrary, as we have seen in previous sections of this work, human rights activists and experts pushing for a total ban on mass surveillance instruments looked at the more recent CJEU case law as a form of legalizing unlimited surveillance methods for national security purposes. Consequently, problems and uncertainties still persist in this field. As Podkowik and others put it, "both the EU Commission and the national legislatures have been struggling with the proper introduction of these standards into the EU and national legislation."⁷³ Notwithstanding this relevant consideration, it cannot be denied that the efforts and inputs provided by the CJEU decisions, reinforced by the multilevel dialogue with national Courts, have determined the affirmation of a consistent and comprehensive path of constitutionalization intended to define how mass surveillance tools can be legally incorporated into a constitutional framework. Whether the more recent rulings represent a "progressive legitimization" of mass surveillance in certain cases or a "shift towards a more pragmatic approach,"⁷⁴ the CJEU intervention in many cases, even if with different degrees of efficacy, helped raising the level of fundamental rights protection by national legislators with regard to mass surveillance instruments.

Whether the current guarantees comply with the principles established by the EU judges is a question still open to discussion.⁷⁵ Nonetheless, in recent years, several national normative solutions proposed a serious attempt to constitutionalize mass surveillance through a path that Tzanou defined as "proceduralization." This ongoing process and debate do not aim to prohibit mass surveillance per se but include constitutional guarantees into its normative discipline. The constitutionalizing process boosted by the rich case law on data retention should not be seen as limited to this particular surveillance tool. On the contrary, the importance of the principles affirmed should be likewise usefully applied to other instruments of massive surveillance, such as

interesting to see if and how this particular form of retention will be disciplined and accepted by civil society, human rights activists, and law enforcement authorities.

⁷¹Proposal for a Regulation concerning respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC, Article 2, para. 2: "The Regulation does not apply to activities, which fall outside the scope of Union law, and in any event measures, processing activities, and operations concerning national security and defense, regardless who is carrying out those activities whether it is a public authority or a private operator acting at the request of a public authority."

⁷²Marcin Rojszczak, *The Uncertain Future of Data Retention Laws in EU: Is a Legislative Reset Possible?*, 41 *COMPUTER L. & SEC. REV.* 1 (2021).

⁷³Jan Podkowik, Robert Rybski & Marek Zubik, *Judicial Dialogue on Data Retention Laws: A Breakthrough for European Constitutional Courts?*, 19 *International J of Const Law* 5, 1597-1631 (2022).

⁷⁴Maria Tzanou, *Public Surveillance Before the European Courts. Progressive Legitimation or a Shift Towards a More Pragmatic Approach?*, *Verfassungsblog*, Apr 6, 2022, <https://verfassungsblog.de/os6-courts-surveillance/>, last accessed 20 October 2022.

⁷⁵Nora Ni Loideain, *EU Data Privacy Law and Serious Crime. Data Retention and Policymaking* (2022).

those based on artificial intelligence. Considering the firm push provided by this judicial intervention, legislators are now in charge of a difficult and delicate task: providing individuals with the constitutional safeguards that have progressively emerged from civil society demands and the vast case law described through clear legislative choices.

E. Conclusion

By establishing an intrusive form of control over people's communications, the data retention regime and its regulation represent a central case study for an in-depth analysis of civil society and judicial impulses characterizing the constitutionalizing efforts in the field of mass surveillance. The opposition expressed by national security and enforcement authorities reveals a strong need to correctly balance the efficacy of investigative instruments and the guarantee of high-level security on the one hand and the protection of constitutional principles on the other. This prevents intrusive measures from eroding the trust between citizens and public authorities, which characterizes democratic societies based on the rule of law.

The multiple cases decided by the CJEU and the different approaches exhibited by Member States show how the challenges and issues linked to the use of surveillance instruments remain open and at the center of a complex and delicate debate that raises serious concerns. While not determining a rigid ban on every possible form of surveillance, at least for national security purposes, EU judges have tried to set precise limits to bulk data retention mechanisms by promoting a strong proportionality test. The clear voice of the CJEU, in contrast to the stunning silence of the European legislator, is now destined to leave space for the reactions of national courts, parliaments and the EU Commission. While the former should consider the need to modify national legislation regulating bulk data retention regimes, the latter must decide whether to promote a new *ad hoc* legislative proposal on data retention that prompts a homogeneous discipline backed by Member States, able to include the results of the process of constitutionalization promoted by the CJEU. Notwithstanding the difficulty of foreseeing possible future evolutions in this articulated field, the future of mass surveillance in the EU seems to be more predictable, thanks to the constitutionalizing efforts of civil society, the CJEU, and national courts in this context.

As evidenced by the impulses analyzed in this Article, the necessity to establish limits and conditions for vast surveillance instruments represents a complex challenge that does not have a solid, conclusive answer in practical terms. On the one hand, the role played by civil society acted as a significant stimulus to the development of an articulated set of judicial decisions related to the delimitation of mass surveillance systems. This highlights a profound awareness of the intrusiveness and impact of these instruments not only on the rights to privacy and data protection but also, more broadly, on the very relationship between citizens and public powers and between freedoms and controls. On the other hand, the questions of the relevance and effectiveness of bulk interceptions, retention, and access operations for security purposes make it hard to establish restrictive limits to the use of these tools in light of the seriousness of the threats they aim to face.

Notwithstanding specific demands from civil society actors, incorporating an explicit constitutional provision affirming an absolute prohibition of mass surveillance practices does not appear to be a feasible or realistic solution. Analyzing the combination of civil society and judicial impulses shows a more complex process of gradual constitutionalization of mass surveillance. Core constitutional principles and their corollaries, such as the principle of proportionality and strict necessity, the need to guarantee prior authorization and control by independent authorities, and the presumption of innocence imposing targeted approaches and objective criteria linking the surveillance measure to a real threat, are being progressively instilled at the regulatory level regarding surveillance instruments. The constitutionalization of mass surveillance does not imply a constitutional codification of an outright prohibition: a ban would eventually fail to strike a balance between the protection of state security and the compression of fundamental rights.

Constitutionalizing mass surveillance in the EU is taking place by introducing specific limits and procedural guarantees derived from translating existing constitutional values in the context of the digital society.

This phenomenon is part of a broader multilevel and multistakeholder process of constitutionalization, progressively pushing the constitutional ecosystem to react to the challenges of the digital revolution.⁷⁶ The strengthening of this tendency and its effectiveness in relation to the constitutionalization of mass surveillance will depend on the simultaneous and interconnected work of various players, from civil society actors, who act as a watchdog and as a trigger of strategic litigation, to supranational and national courts and national legislators. This Article has shown that, after the significant efforts of these first two groups of actors, the question of the future implementation of legitimate mass surveillance systems now lies in the hands of legislators. The effective constitutionalization of mass surveillance practices implies the incorporation of the constitutional values and principles advocated by civil society and translated by case law into precise surveillance laws and regulations at both the national and EU levels.

Acknowledgements. We want to thank those who participated in the data protection and surveillance panel of the Annual BILETA Conference 2021 for their feedback on an earlier version of this Article. We want to thank Ms Cerys Lee for her research assistance. Giulia Formici would like to express her gratitude to the University of Milan, in particular to the Department of Italian and Supranational Public Law, where she held the position of Research Fellow until November 2023. While the Article has been elaborated jointly by the co-authors, Sections A and B were written by Edoardo Celeste, and Sections C and D by Giulia Formici.

Competing interests. The authors declare none.

Funding. The authors declare no specific funding.

⁷⁶See ORESTE POLLICINO, *supra* note 11; see also Celeste, *supra* note 13.