Hard Cases

Digital Surveillance Under European Scrutiny
A Dangerous Alliance Unveiled

Luca Ettore Perriello*

Nothing was your own
except the few cubic centimeters in your skull
George Orwell, 1984

Abstract

Digital surveillance, whether targeted or mass, has drawn scrutiny from European courts for potentially violating human rights. The balance between security and privacy is challenging, with states often implementing invasive measures in response to threats like terrorism. The European Court of Human Rights and the Court of Justice of the European Union have been striving to balance state security needs with individual rights, reflecting growing public concern over surveillance. Their responses tend to accommodate national security demands while progressively legitimizing digital surveillance. The courts are converging towards a nuanced approach, emphasizing procedural safeguards rather than drawing red lines.

I. Digital Surveillance and Human Rights

In an increasingly digital world, human rights are vulnerable to being infringed by the illegal or improper use of new technologies. Digital surveillance, which states use to neutralize threats from individuals or groups (targeted surveillance) or to implement broad defense strategies (mass surveillance), has been brought to the attention of supranational courts due to potential violations of fundamental rights and freedoms, particularly the right to privacy and freedom of opinion and expression.[1]

The right to privacy, an aspect of the broader right to respect for private and family life, receives multilevel protection as it is provided for in many international and European charters, such as Art 12 of the Universal Declaration of Human Rights, Art 8 of the European Convention on Human Rights (ECHR), and Art 7 of the Charter of Fundamental Rights of the European Union (which today has

*Associate Professor of Private Law, Marche Polytechnic University. This work was supported by the Italian Ministry of University and Research under the project 'Digital Vulnerability in European Private Law' (DiVE) 2022-2025.

[1] A. Lubin, 'The Rights to Privacy and Data Protection Under International Humanitarian Law and Human Rights Law', in R. Kolb et al eds, *Research Handbook on Human Rights and Humanitarian Law* (Cheltenham, UK – Northampton, MA: Edward Elgar Publishing, 2013), 462.

the same legal value as the Treaties under Art 6 of the Treaty on European Union). Art 8 of the Charter lays down a specific right to the protection of personal data, which must be processed for specific purposes and based on the consent of the individual or another legitimate basis provided for by the law. Every individual has the right to access data collected about them and to obtain rectification of any errors, with these rights being overseen by an independent authority.

Freedom of opinion and expression (Art 19 of the Universal Declaration, Art 10 of the ECHR, Art 10 of the Charter) enjoys privileged protection, as any limitations are allowed only for the expression, not the opinion behind it. The negative aspect of this right includes the right not to be identified for holding a particular opinion, that is, the right to digital anonymity and to freely access encryption techniques. Interpretation of the right to freedom of opinion and expression constantly evolves due to the hermeneutic activities of supranational courts and quasi-judicial bodies operating in the international context.

Privacy and the freedom to form and express opinions have evolved from being mere individual aspirations to constitutional and collective values,[2] aimed not only at preserving personal freedom but also at strengthening the liberal democratic model[3] where anyone can freely participate and communicate without interference. In the European Union (EU), the constitutionalization of these rights has meant that the regulation of personal data processing is no longer addressed solely from a market perspective, as if the goal were only to prevent member states from restricting the free movement of data with undeniable economic value. The Treaty of Lisbon, establishing an autonomous basis for the adoption of secondary legislation on data protection (Art 16(2) of the Treaty on the Functioning of the European Union), has imposed an obligation on EU institutions to pass legislation implementing the right to data protection,[4] which was done with Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, concerning the protection of natural persons regarding the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, or GDPR).

However, human rights can clash with other collective interests represented by states intending to implement digital surveillance measures to counter serious threats to their security, which have become increasingly tangible in light of terrorist attacks, international illegal trafficking, and state conflicts. Balancing these interests

[2] H. Kranenborg, 'Article 8 – Protection of Personal Data', in S. Peers, T. Hervey, J. Kenner and A. Ward eds, *The EU Charter of Fundamental Rights – A Commentary* (Oxford: Oxford University Press, 2021), 223; S. Seubert and C. Becker, 'The Democratic Impact of Strengthening European Fundamental Rights in the Digital Age: The Example of Privacy Protection' *German Law Journal*, 21 (2021).

[3] E. Dubout, 'La Charte et le territoire. A propos du champ d'application territorial de la Charte des droits fondamentaux de l'Union européenne', in Id et al eds, *L'extraterritorialité du droit de l'Union européenne* (Bruxelles: Bruylant, 2021), 225.

[4] H. Hijmans, *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU* (New York City: Springer, 2016), 263.

is not always easy.[5] For years, non-governmental organizations dedicated to human rights protection have reported increasingly invasive surveillance measures adopted by authoritarian regimes, which have even threatened to block telecommunications services unless unconditional access to data was granted, or have required the installation of specific software in all computers sold nationally to intercept sensitive information.

Some countries, lacking national legislation on digital surveillance, have purchased sophisticated surveillance systems from private industries to monitor opposition politicians, journalists, and activists. An example is the Pegasus program sold by an Israeli company to Mexico for targeted surveillance of dissidents. States may also transfer their expertise to the private sector through specific partnerships based on the 'revolving door' system. For instance, in the Raven project, United States National Security Agency (NSA) officials with intelligence expertise were seconded to private surveillance entities, which were then engaged by the United Arab Emirates to spy on human rights activists and political dissidents.

Western democracies are not exempt from criticism either.[6] Several political campaigns have been facilitated by systematically acquiring data from social media platforms to profile users and provide tailored information that could influence voting behavior. In 2013, American whistleblower Edward Snowden revealed the NSA's use of a mass digital surveillance program to collect extensive information about foreign states and their citizens' personal data. It was later discovered that allied intelligence services, particularly British intelligence, had acquired substantial personal data from transatlantic submarine cables used for electronic communications. Following the international Datagate scandal,[7] the NSA's powers were curtailed, particularly in terms of the ability to store telephone records, which are now held directly by telephone companies.

More recently, concerns have been raised about COVID-19 tracking apps, which, however, have seemed justified under Art 23 of the GDPR, which allows data protection restrictions to pursue public health and social security goals. Additionally, these apps are usually installed voluntarily by users.[8]

Governmental electronic surveillance programs often strain the system of rights and guarantees recognized by international charters. Distinctions between suspicious individuals and ordinary citizens are not always made. Surveillance can occur without the individual's knowledge or the opportunity to challenge it,

[5] J-P. Jacqué, 'Protection des données personnelles, Internet et conflits entre droits fondamentaux devant la Cour de Justice' *RTD Eur*, 283, 285 (2014).

[6] M. Mastracci, 'Evoluzione del diritto alla "*privacy*" tra Europa e Stati Uniti: dal "*Safe harbor*" al "*Privacy shield*" ' *La comunità internazionale*, 555, 556 (2016).

[7] For a commentary, see M. Nino, 'Il caso "*Datagate*": i problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della *privacy*' *Diritti umani e diritto internazionale*, 727 (2013).

[8] G. Della Morte, 'La tempesta perfetta Covid-19. Deroghe alla protezione dei dati personali ed esigenze di sorveglianza di massa' *sidiblog.org*, 30 March 2020.

as procedures are often classified for national security reasons.

Equally concerning is the acquisition of metadata, which, although not directly revealing communication content, are treated as data,[9] on the grounds that they can be aggregated to expose individual habits, preferences, social interactions, thereby providing a detailed profile of the target.[10] It is no coincidence that the European Court of Human Rights (ECtHR), in *Big Brother Watch and Others* v *The United Kingdom*, made it clear that the same safeguards applicable to the collection and processing of communication contents must extend to metadata.[11]

Privacy and freedom of opinion have fully entered the political agenda of supranational lawmakers and the case-law of European courts, driven by growing public concern about constant surveillance.[12] The ECtHR and the Court of Justice of the European Union (CJEU) have responded similarly to this concern, attempting to accommodate state needs for crime prevention and repression.[13]

II. The Procedural Obsession of the European Court of Human Rights

Big Brother Watch and Others v *The United Kingdom*[14] originated from an application to the ECtHR by a group of non-governmental organizations and journalists against the United Kingdom for the use of a digital mass surveillance program by British intelligence services in collaboration with their American counterparts. Much of the evidence was based on information leaked by Edward

[9] Eur. Court J., Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd* v *Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, Judgment of 8 April 2014, ECLI:EU:C:2014:238, §27; Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB* v *Post- och telestyrelsen* and *Secretary of State for the Home Department* v *Tom Watson and Others*, Judgment of 21 December 2016, ECLI:EU:C:2016:970, §99; Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others* v *Premier Ministre and Others*, Judgment of 6 October 2020, ECLI:EU:C:2020:791, §117.

[10] Highlighting the artificiality of the distinction in the acquisition of data and metadata, as the latter are likely to reveal sensitive information to the same extent, if not to a greater extent, see A. Iliopoulou-Penot, 'The Construction of a European Digital Citizenship in the Case Law of the Court of Justice of the EU' *Common Market Law Review*, 969, 989 (2022).

[11] Eur. Court H.R., Grand Chamber, *Big Brother Watch and Others* v *the United Kingdom*, Judgment of 25 May 2021, ECLI:CE:ECHR:2021:0525JUD005817013, §§342, 363-364. For a commentary, see A. Lubin, 'Introductory Note to Big Brother Watch v. UK (Eur. Ct. H.R. Grand Chamber)' *International Legal Materials*, 605 (2022).

[12] Eur. Court J., Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd* n 9 above, §37. On this point cf L. Benedizione and E. Paris, 'Preliminary Reference and Dialogue Between Courts as Tools for Reflection on the EU System of Multilevel Protection of Rights: The Case of the Data Retention Directive' *German Law Journal*, 1727 (2019).

[13] Stressing that the Court of Justice has had the merit of strengthening the protection of individual rights through the recognition of European sovereignty over personal data, see V. Benadou, 'La Cour de justice, gardienne d'une "souveraineté européenne" sur les données personnelles' *Revue des affaires europeennes*, 19 (2018).

[14] Eur. Court H.R., *Big Brother Watch and Others* v *the United Kingdom*, Judgment of 13 September 2018, ECLI:CE:ECHR:2018:0913JUD005817013, noted by M. Milanovic, 'ECtHR Judgment in Big Brother Watch v. UK' *ejiltalk.org*, 17 September 2017.

Snowden. The applicants submitted that the United Kingdom had violated the rights to respect for private life and freedom of expression, protected by Arts 8 and 10 of the ECHR.

The Court had already addressed the compatibility of mass surveillance with the Convention in previous decisions. In *Weber and Saravia* v *Germany*,[15] the Court upheld the surveillance measures adopted by the Federal Republic of Germany to prevent armed attacks or acts of international terrorism, outlining the minimum safeguards that the legislation must include to prevent abuse of power.[16] Specifically, legislation must specify: i) the nature of the offenses that may justify interception of communications; ii) the categories of individuals subject to interception; iii) the limits on the duration; iv) the procedures for examining, using, and storing the obtained data; v) the precautions to be taken when data is communicated to third parties; and vi) the circumstances in which recordings can or must be destroyed (§95). These criteria are very lenient, giving states a wide margin of appreciation.[17]

A few years later, in *Roman Zakharov* v *Russia*,[18] concerning the Russian government's power to intercept all lines using a national telephone operator, the ECtHR emphasized that surveillance must not be indiscriminate but rather must be based on reasonable suspicion that the person concerned is planning or has committed offenses or acts undermining national security. The Court also criticized the interception of all telephone communications in the area where the crime was committed, without limiting it to a specific target (§§260 and 265). These conclusions were confirmed in *Szabó and Vissy* v *Hungary*,[19] where it was held that only individual suspicion concerning a specific person conforms to the strict necessity required by Art 8 of the ECHR for any measure restricting the right to respect for private and family life (§§67 and 71). Consequently, the Court found the Hungarian anti-terrorism law – based on which two members of an opposition political organization had been subjected to digital surveillance measures – to be incompatible with the Convention.

In the *Big Brother Watch* v *The United Kingdom* decision of 2018,[20] the Court, only partially confirming its previous positions, ruled that mass surveillance programs do not inherently violate human rights and may fall within the states'

[15] Eur. Court H.R., *Gabriele Weber and Cesar Richard Saravia* v *Germany*, Judgment of 29 June 2006, ECLI:CE:ECHR:2006:0629DEC005493400. For an analysis of the ECtHR's decisions on mass surveillance and Art 8, see A. Stiano, 'Il diritto alla *privacy* alla prova della sorveglianza di massa e dell'*intelligence sharing*: la prospettiva della Corte europea dei diritti dell'uomo' *Rivista di diritto internazionale*, 511, 522 (2020).

[16] A. Lubin, ' "We Only Spy on Foreigners": The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance' *Chicago Journal of International Law*, 502, 543 (2018).

[17] V. Rusinova, 'A European Perspective on Privacy and Mass Surveillance at the Crossroads' *Higher School of Economics Research Paper No. WP BRP 87/LAW/2019*, 5 (2019).

[18] Eur. Court H.R., Grand Chamber, *Roman Zakharov* v *Russia*, Judgment of 4 December 2015, ECLI:CE:ECHR:2015:1204JUD004714306.

[19] Eur. Court. H.R., *Szabó and Vissy* v *Hungary*, Judgment of 12 January 2016, ECLI:CE:ECHR:2016:0112JUD003713814.

[20] Eur. Court H.R., *Big Brother Watch and Others* v *the United Kingdom* n 14 above.

margin of appreciation (§§314-319). It concluded that the United Kingdom's program violated Arts 8 and 10 of the ECHR only in certain aspects.

Surprisingly, the Court diluted the safeguards cautiously outlined in its previous decisions, particularly claiming that the reasonable suspicion criterion, supported by objective evidence, was in conflict with the states' margin of appreciation in adopting mass surveillance measures. In the Court's opinion, mass surveillance is inherently untargeted, and requiring reasonable suspicion would make it impractical. Even ex-post notification to the affected target would be impractical, since it presupposes surveillance directed at specific individuals, which is not evident in mass surveillance (§317).[21] Furthermore, among the criteria outlined in *Weber*, the Court rejected that national legislation must define the offenses justifying interception and the categories of individuals concerned.

Dissatisfied with the decision, the applicants appealed to the Grand Chamber, which, in a decision delivered on May 25, 2021,[22] confirmed that mass interception regimes do not *ipso facto* violate the Convention, as they can be justified by the need to investigate serious crimes and threats to national security, such as global terrorism, drug or human trafficking, and child pornography. Many of these offenses are committed within an international network of hostile actors with access to sophisticated technology allowing them to operate anonymously and compromise digital infrastructures and the functioning of democratic processes through cyberattacks (§§323, 345). Untargeted surveillance is of vital importance for countering national security threats, and no alternative appears feasible that would obtain the same results (§424).

However, to minimize the risk of abuse of power, the Court emphasized that every stage of the surveillance process must be subject to safeguards to ensure its necessity and proportionality. Mass interception should be subject to independent ex ante authorization and independent ex post review (§350).[23] For domestic legislation to pass the Court's scrutiny, it must meet eight criteria (replacing the six outlined in *Weber*), that is, it must clearly define: i) the grounds for authorizing mass surveillance; ii) the circumstances under which individual communications may be intercepted; iii) the procedure for granting authorization; iv) the procedures for selecting, examining, and using intercepted material; v) the precautions to be taken when the material is communicated to third parties; vi) the limits on the duration of interception, the storage of intercepted material, and the circumstances in which it must be deleted and destroyed; vii) the procedures and modalities for

[21] Considering the notification of digital surveillance measures an essential element to allow the individual to defend against potential abuses by government authorities, see C. Cinelli, 'Sorveglianza digitale, sicurezza nazionale e tutela dei diritti umani' *Ordine internazionale e diritti umani*, 588, 604 (2020).

[22] Eur. Court H.R., Grand Chamber, *Big Brother Watch and Others* v *the United Kingdom* n 11 above.

[23] Applauding the commitment of Italian law to impose judicial authorization to avoid abuses by the judicial police, see C. Cinelli, 'Sorveglianza digitale' n 21 above, 595.

supervision by an independent authority and its powers to sanction non-compliance; and viii) the procedures for independent ex-post compliance review and the powers of the competent authority to handle non-compliance situations (§361).

Based on these eight criteria, the Grand Chamber identified several issues in British legislation, finding a violation of the right to respect for private and family life. In making this finding, the Grand Chamber noted the lack of independent authorization (which was issued by the executive), the vagueness of search terms (also known as selectors) used to request an interception order, and the absence of further internal scrutiny when specific selectors target an individual (§425). Similar issues were found regarding the acquisition of metadata from service providers, which was deemed illegal as it was not limited to the purpose of preventing serious crimes and lacked ex-ante control by an independent judicial or administrative authority (§§518-519). Besides the violation of Art 8 ECHR, the Chamber also found that the United Kingdom's actions had infringed on the freedom of expression, as the surveillance programs did not adequately protect journalistic sources and their confidential communications (§§456-458, 524-525).

The Court's judgment is not a victory for privacy rights and freedom of opinion but reflects a cautious and procedural attitude, which is disappointing in terms of protecting human rights. The principles of necessity and proportionality of surveillance measures translate into mere declarations, with their compliance taken for granted. The Court did not engage in balancing, did not question whether the benefits of surveillance programs outweigh the intrusion into the individual's most intimate relationships, assuming this assessment had already been made by national authorities.

Moreover, prior authorization is not deemed a requirement (instead, it is only recommended), nor is it necessary for authorization to be issued by a judicial authority, as long as it is issued by a body independent of the executive (§351). The procedural framework substantiating the principles of necessity and proportionality is very weak, as national legislation is subject to a global evaluation (§360). Consequently, if one of the eight criteria is lacking, the state can compensate by scrupulously observing another criterion. To this end, the opinion, partially concurring and partially dissenting, of Judge Pinto de Albuquerque appears persuasive, to the extent that it criticizes the unbearable vagueness of the Grand Chamber's language, revealing the concealed intent to expand states' discretion and hesitation in exercising judicial functions, ultimately weakening the ECHR's authority and diminishing the decision's substantive impact.

Following the ruling in *Big Brother Watch*, governments may continue using mass digital surveillance programs with little hindrance and may even share the information obtained with third countries or allow these countries direct access to their archives. The Court subjected intelligence-sharing[24] to some additional

[24] See M. Milanovic, 'Intelligence Sharing in Multinational Military Operations and Complicity under International Law' *International Law Studies*, 1269 (2021).

procedural safeguards: i) domestic legislation must clearly indicate the circumstances under which transmission of information can occur; ii) the transferring state must ensure that the receiving state has adequate protections, particularly regarding safe data storage and restrictions on their disclosure, without necessarily requiring the same level of protection as the transferring state, nor requiring the receiving state to provide assurances before each data transfer; iii) enhanced safeguards are necessary when the transferred material is particularly sensitive; and iv) the transfer *should* be subject to independent oversight (§362).

In this case, the British legislation was found compliant with these standards, which is not surprising given the vague and not entirely adequate criteria that barely touch on the merits of the surveillance measures under scrutiny and the related risks. These risks are particularly high when information is shared with states that do not respect human rights. The Court, without any appreciable reason, overlooked the lack of authorization from an independent body in British legislation. It is unclear why, in this respect, intelligence-sharing should receive different treatment from mass surveillance for internal state purposes.

III. The Demise of Judicial Safeguards by the European Court of Justice

Recent decisions of the European Court of Justice (CJEU) have aligned with similar positions. Indeed, there has been a noticeable shift away from the protective stance seen in the Court's early rulings on digital surveillance, which emerged during the Snowden revelations era.

In *Digital Rights Ireland*,[25] the Court invalidated Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks. This directive, which had been adopted in response to the terror attacks in Madrid and London, mandated telecommunications service providers to retain metadata for up to two years and make it available to public authorities for security purposes. The challenge was brought by an Irish non-governmental organization, Digital Rights Ireland, following significant civil society mobilization. They leveraged the principle, which had been recently established by the Court,[26] that the GDPR does not preclude a national law allowing a consumer protection association to bring legal action, without a specific mandate and regardless of the infringement of specific rights of data subjects, against the alleged violator of data protection laws, claiming breaches of the prohibition of unfair commercial practices, violations of consumer protection laws, or nullity of unfair contract terms, provided the

[25] Eur. Court J., Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd* n 9 above.

[26] Eur. Court J., C-319/20, *Meta Platforms Ireland Limited* v *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, Judgment of 28 April 2022, ECLI:EU:C:2022:322.

data processing in question could harm the rights recognized by this regulation to identified or identifiable individuals.

Digital Rights Ireland was the first decision declaring the invalidity of a secondary European legislative source for violating the Charter of Fundamental Rights of the European Union,[27] particularly Arts 7 and 8, which, according to the Court, prohibit the mass and indiscriminate retention of data. The Court warned member states that only targeted data processing with robust safeguards is permissible. This ruling reflects a strategic defense by e-privacy organizations seeking to have the Court annul a legislative act or ensure its interpretation aligns with individual rights in data protection.

In the subsequent *Tele2* case,[28] the Court clarified that the prohibition on mass surveillance also applies to the laws of individual member states, emphasizing that only targeted retention of metadata, coupled with a stringent system of safeguards, is compatible with Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, read in light of the Charter of Fundamental Rights.[29] Following this ruling, some commentators argued that it would hinder public security by preventing law enforcement from accessing historical communication data, thereby depriving states of an effective tool to combat serious crime.[30] Some criticized the Court for unjustified interference in the sovereign prerogatives of states, particularly their fundamental function of ensuring security within their territories, as explicitly recognized by Art 4(2) of the Treaty on European Union (TEU).[31] Many national governments called for a reassessment of the balance between individual freedoms and national security in data processing matters.

Despite the outcry over the *Tele2* decision, the prohibition on general data retention was reaffirmed in *Privacy International*,[32] which concerned the bulk transmission of metadata by British intelligence services for national security

[27] M.P. Granger and K. 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' 4 *European Law Review*, 835 (2014).

[28] Eur. Court J., Joined Cases C-203/15 and C-698/15, *Tele2 Sverige* n 9 above.

[29] Highlighting that the European system for the protection of fundamental rights does not offer double standards in data protection; both the EU and member states are subject to the same duties of protection, see K. Lenaerts, 'The European Union as a Union of Democracies, Justice and Rights' 2 *International Comparative Jurisprudence*, 132 (2017).

[30] H. Hijmans, 'Data Protection and Surveillance: The Perspective of EU Law', in V. Mitsilegas and N. Vavoula eds, *Surveillance and Privacy in the Digital Era* (London: Bloomsbury Publishing, 2021), 235.

[31] J. Sirinelli, 'La protection des données de connexion par la Cour de justice: cartographie d'une jurisprudence européenne inédite' 2 *Revue trimestrielle de droit européen*, 313 (2021).

[32] Eur. Court J., C-623/17, *Privacy International* v *Secretary of State for Foreign and Commonwealth Affairs and Others*, Judgment of 6 October 2020, ECLI:EU:C:2020:790. Defining the decision a victory for fundamental rights, see M. Tzanou, 'European Union Regulation of Transatlantic Data Transfers and Online Surveillance' *Human Rights Law Review*, 545, 546 (2017).

reasons. In the CJEU's opinion, a national law requiring electronic communications service providers to transmit metadata in a generalized and undifferentiated manner to intelligence agencies is disproportionate and unjustified in a democratic society (§81). The British legislation was problematic for several reasons: i) it applied to all users without specifying whether the data transmission should be real-time or delayed; ii) once transmitted, the data underwent automated analysis to uncover unknown threats; iii) the collected data could be cross-referenced with other databases containing different categories of personal data or disclosed outside the agencies and to third countries; and iv) there was no requirement for prior authorization from a judge or independent administrative authority, nor notification to the affected individuals (§§25 and 52).

In the *Schrems* cases,[33] the Court further clarified that European standards for online privacy guarantees must also apply to data transfers outside the Union,[34] invalidating the Commission's adequacy decision on the Safe Harbor principles and the EU-US Privacy Shield, which allowed data transfers to US providers. Given the omnipotence of the US digital surveillance regime, which does not provide adequate protection for European citizens,[35] the Commission's decisions were deemed incompatible with Directive 95/46 (*Schrems I*) and the GDPR (*Schrems II*), read in light of Arts 7 and 8 of the Charter of Fundamental Rights of the European Union. The Court ruled that the adequacy of data protection required for extra-EU transfers must be essentially equivalent to that provided by EU law,[36] ensuring that personal data of any individual within European territory can only be transferred to third countries offering equivalent protection standards. This significantly reduces the Commission's power to negotiate international

[33] Eur. Court J., C-362/14, *Maximillian Schrems* v *Data Protection Commissioner* (*Schrems* I), Judgment of 6 October 2015, ECLI:EU:C:2015:650; Eur. Court J., C-311/18, *Data Protection Commissioner* v *Facebook Ireland Ltd and Maximillian Schrems* (*Schrems* II), Judgment of 16 July 2020, ECLI:EU:C:2020:559.

[34] Highlighting that violations of individual rights perpetrated through mass surveillance techniques have a necessarily extraterritorial nature, see M. Catanzariti, 'La dimensione extraterritoriale della sorveglianza di massa' *Rassegna di diritto pubblico europeo*, 335 (2019). See also P. Cruz Villalon, 'Un principe de continuité? Sur l'effet extraterritorial de la Charte des droits fondamentaux de l'UE', in J. Wildermeersch and P. Paschalidis eds, *L'Europe au présent! Liber Amicorum Melchior Wathelet* (Bruxelles: Bruylant, 2018), 317.

[35] Highlighting the diversity of the European model compared to the American one, to the point where data protection has become the First Amendment of the European Union, see B. Petkova, 'Privacy as Europe's First Amendment' *European Law Journal*, 140 (2019).

[36] Ideally speaking of a 'territory of the Union,' understood as a legal space with a special regime having strong positive implications for the citizens of the Union, see N. Nic Shuibhne, 'The 'Territory of the Union' in EU Citizenship Law: Charting a Route from Parallel to Integrated Narratives' *Yearbook of European Law*, 267 (2019). However, concerns are raised by J. Atik and X. Groussot, 'A Weaponized Court of Justice in Schrems II' *Nordic Journal of European Law*, 18 (2021), claiming that 'constitutional values of one party are ill-suited to satisfactorily resolve a legal conflict between two parties. A constitutional court, such as the CJEU – that sees its own law and not that of the counterparty to the conflict – makes reconciliation and resolution far less likely. Europe may 'win' this contest with the United States – and the CJEU's judgment in Schrems II may contribute to its policy success. But such a 'win' reflects the exercise of power more than law'.

data management agreements. The core idea is that personal data protection within the European space cannot be circumvented through data transfer to non-EU countries without adequate protection standards. Individuals must retain control over their data even when it leaves the Union.

This case law aligns with the GDPR. While it does not contain specific provisions on data acquisition within digital surveillance proceedings conducted by member states for national security reasons, the GDPR requires a data protection impact assessment for systematic large-scale surveillance of a publicly accessible area (Art 35(3)(c)). The data controller must, before proceeding, conduct an assessment of the impact on personal data protection, considering the nature, scope, context, and purposes of the processing, and the high risk that the use of new technologies may pose to individual rights and freedoms. The entire regulation is centered on the idea that citizens control the traces they leave in the digital environment and remain sovereign over their digital identity (see particularly recitals 7, 68, 75, 85).[37] Individual control over one's data underpins many other rights, such as the right of access (Art 15), the right to rectification (Art 16), the right to be forgotten (Art 17), the right to data portability (Art 20), and the right to object (Art 21). Member states may limit these rights if necessary to safeguard, among other things, national security and defense, provided that such limitation respects the essence of the rights and freedoms and is a necessary and proportionate measure in a democratic society (Art 23). The CJEU's case law reflects the logic of individuals' control as subjects of rights, opposing their transformation into objects of generalized surveillance.

This protective stance remained unchanged until the CJEU's ruling in *Quadrature du Net*,[38] which also originated from a challenge by non-governmental organizations and concerned data retention mandated by French law for national security reasons. The CJEU first clarified a competence issue, addressing member states' claims that Directive 2002/58/EC does not apply to national laws safeguarding national security, as intelligence activities aimed at maintaining public order are essential state functions, falling within their exclusive competence under Art 4(2) TEU. Disputing this claim, the Court affirmed the full applicability of EU law to member state legislation requiring electronic communications service providers to retain metadata for national security and crime-fighting purposes (§104). While generally reiterating the prohibition on general and indiscriminate data retention (in this case, metadata), the Court, in response to concerns raised by national governments related to counter-terrorism, allowed for the exception of safeguarding national security against a serious, current, or foreseeable threat. However, the goals of crime-fighting and public safety protection can only justify targeted data retention measures.

[37] Already before the GDPR, see O. Lynskey, *The Foundations of EU Data Protection Law* (Oxford: Oxford University Press, 2015), 14.

[38] Eur. Court J., Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net* n 9 above.

Central to the Court's reasoning is the distinction between national security, on the one hand, and public safety and crime-fighting, on the other. Art 4(2) TEU assigns exclusive competence to each member state for national security, reflecting the primary interest in protecting the essential functions of the state and fundamental social interests, including preventing and sanctioning activities capable of destabilizing the nation's constitutional, political, economic, or social structures, particularly those directly threatening society, residents, or the state itself, such as terrorist activities (§135). Safeguarding national security, however, goes far beyond the goals of general, even serious, crime-fighting and public safety protection. National security threats cannot be confused, by nature and severity, with the risk of public safety disturbances or tensions. The goal of safeguarding national security can justify more severe intrusions into fundamental rights than measures justified by other objectives (§136).

This position was recently confirmed in *G.D.* v *Commissioner of An Garda Síochána*,[39] where the CJEU stated that crime-fighting, including serious crime, cannot be equated with a national security threat. Otherwise, an intermediate category between national security and public safety would be created in order to apply national security requirements to public safety (§63). Unlike crime, a national security threat must be real and current, or at least foreseeable, which requires specific circumstances justifying a generalized and indiscriminate metadata retention measure for a limited period. By nature and severity, such a threat differs from the risk of public safety tensions or disturbances or the commission of crimes (§62). Consistently, the Court specified that metadata cannot be subject to general and indiscriminate retention for crime-fighting purposes, and access for these purposes must be prohibited. If these data have been exceptionally retained, without distinction, to safeguard national security against a serious, current, or foreseeable threat, national criminal investigation authorities cannot access these data in criminal proceedings, lest the prohibition on data retention for crime-fighting purposes be rendered ineffective (§100).

Accordingly, the Court outlines a hierarchy of objectives that can be pursued by legislation on digital surveillance: national security is placed first, followed by combating serious crime and preventing threats to public security. The bulk retention of data is permitted in the event of a national security threat, provided certain procedural conditions are met: i) the retention must be for a limited and strictly necessary period of time. Although the retention of data may be renewed due to the persistence of the threat, the duration must not exceed a foreseeable time frame; ii) the member state must be facing a serious, actual or foreseeable national security threat; iii) strict limitations and safeguards must be in place to effectively protect the personal data of the individuals concerned against the risk of abuse; and iv) the measures requiring electronic communication service

[39] Eur. Court J., C-140/20, *G.D.* v *The Commissioner of the Garda Síochána and Others*, Judgment of 5 April 2022, ECLI:EU:C:2022:258.

providers to retain data must be subject to review by a judge or an independent authority, whose decision must be binding and aimed at verifying compliance with the prescribed conditions and safeguards.[40] These are precisely outlined criteria, based on an extensive reading of secondary rules in light of the Charter of Fundamental Rights and the principle of proportionality. The Court's activism may raise suspicions that it is overstepping its role and becoming a quasi-legislative body,[41] which, however, seems necessary given the lack of harmonization, at the European level, regarding digital surveillance.

In compliance with these safeguards, member states may continue to intercept anyone using electronic communication means, without the individuals concerned having to find themselves, even indirectly, in a situation that could lead to criminal investigations. Mass digital surveillance can also involve people for whom there is no indication that their behavior might have a connection, even indirectly or remotely, with serious crimes, and, in particular, without there being a correlation between the data to be retained and a threat to public security.[42]

While specifying that bulk data retention cannot be systematic and must meet certain conditions, the Court nevertheless leaves some questions open: what is meant by a foreseeable threat? What is the maximum duration for data retention?

Another crucial issue is whether it is possible for data acquired in a generalized and indiscriminate manner for national security purposes to be declassified and transmitted to authorities for use in other purposes, such as combating crime. In the *Quadrature* case, the Court seems to give a negative answer, holding that member states must clearly establish, in their legislation, the purpose for which data retention can occur (§164) and that access to such data can, in principle, only be justified by the general interest for which the retention was imposed on communication service providers (§166). The reasons for accessing the data must be the same as those that originally justified their retention.

In contrast, the fight against serious crime and the prevention of equally serious threats to public security are secondary objectives, which can only justify targeted digital surveillance measures. These measures must be limited to what is strictly necessary concerning the categories of data to be retained, the means of communication used, the individuals involved, and the time period (subject to possible renewal due to the ongoing necessity for such retention). Specifically, the scope of targets should be confined based on objective elements capable of revealing at least an indirect connection with acts of serious crime, contributing

[40] Eur. Court J., Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net* n 9 above, §§137-139.

[41] See O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet. A Road Towards Digital Constitutionalism?* (London: Bloomsbury Publishing, 2021), 99, criticizing the judicial attempt to build a European fortress of personal data and to regulate in a regional manner a matter necessarily requiring a transnational dimension.

[42] Eur. Court J., Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net* n 9 above, §143.

in some way to the fight against serious crime, preventing a significant risk to public security, or a risk to national security. In *GD* v *Commissioner of the Garda*,[43] the Court emphasized the need to adopt non-discriminatory criteria for targeted surveillance, focusing, for instance, on individuals under investigation or other ongoing surveillance measures or those listed in the national criminal registry with a previous conviction for serious crimes that may pose a high risk of recidivism (§70).

There are also some concerns around targeted surveillance, related to the ambiguity of the requirement of a serious threat to public security. Although it is true that individuals subject to interception must be identified in advance based on objective criteria, the connection to serious crime can also be indirect, significantly broadening the pool of surveilled subjects.

The Court also allows for a geographic connection when national authorities consider that one or more areas are characterized by a high risk of preparing or committing acts of serious crime. Such areas can include places with a high incidence of crime or those prone to criminal acts, such as infrastructures regularly attended by large numbers of people, or strategic locations like airports, train stations, or toll areas.[44] In the subsequent case *GD* v *Commissioner of the Garda*, the Court specified that national authorities could adopt targeted retention measures based on a geographic criterion, such as the average crime rate in a geographic area, even without evidence of the preparation or commission of serious crimes in the affected areas.[45]

However, such a criterion, as the experience in the US has shown, risks being discriminatory and disproportionately directing targeted surveillance toward vulnerable groups in society, such as immigrants, ethnic minorities, and the poor, who often reside in high-crime areas.[46] The consequence could be that the most marginalized individuals in society are the ones being surveilled.

IV. Open Doors to Mass Data Retention and Automated Data Analysis

Mass and targeted data retention for national and public security purposes are not the only measures allowed to member states. In *Quadrature*, the Court of Justice also permitted, with some precautions, the indiscriminate retention of IP addresses and data related to the civil identities of users of electronic communication systems, as well as the automated analysis of metadata.

IP addresses do not reveal a specific communication but are generated to

[43] Eur. Court J., C-140/20, *G.D.* v *The Commissioner of the Garda Síochána and Others* n 39 above.

[44] Eur. Court J., Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net* n 9 above, §150.

[45] Eur. Court J., C-140/20, *G.D.* v *The Commissioner of the Garda Síochána and Others* n 39 above, §80.

[46] See C. O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (New York: Crown, 2016), passim.

identify the owner of the terminal from which internet communication is made. In the Court's opinion, IP addresses have a lower sensitivity level and can receive differentiated treatment compared to other traffic data, as long as only the IP address of the origin of the communication, and not that of the recipient, is retained. This means no information would be disclosed about third parties who were in contact with the person originating the communication (§152). At the same time, the Court acknowledged that the retention of these addresses amounts to a serious interference with the fundamental rights of the internet user, as they can be used to track the user's entire browsing history and thus their online activity, allowing for the creation of a detailed profile of the monitored person (§153).

However, measures for processing IP addresses can be justified as the only investigative tool that allows the identification of the person to whom the address was attributed at the time of committing online crimes, especially serious offenses such as child pornography, including the purchase, distribution, transmission, or making available of child pornographic material online (§154). Given the severity of the interference with the exercise of fundamental rights enshrined in Arts 7 and 8 of the Charter of Fundamental Rights, the generalized and indiscriminate retention of IP addresses is subject to some precautions: i) the retention period must not exceed what is strictly necessary in light of the pursued objective; and ii) such a measure must include strict conditions and safeguards regarding the use of such data, particularly through tracking, in relation to the communications and activities carried out online by the individuals concerned (§156).

As mentioned, alongside the retention of IP addresses, the Court also allowed the retention of data related to the civil identity of all users of electronic communication means for the purposes of preventing, investigating, detecting, and prosecuting crimes, as well as safeguarding public security, without the requirement that the crimes or threats to public security be serious. Such data, in fact, do not per se allow for knowing the date, time, duration, and recipients of the communications made, nor the locations where such communications occurred or their frequency with certain individuals over a specified period. Aside from providing contact information such as addresses, they do not offer any information on data communications and, consequently, on the users' private lives. Accordingly, the interference caused by the retention of such data cannot, in principle, be classified as serious (§157). Indiscriminate access to IP addresses and the civil identities of digital users signals that the era of online anonymity is effectively over.[47]

As far as the automated analysis of metadata is concerned, namely data related to traffic and location, in *Quadrature*, the Court of Justice acknowledged that the interference with personal rights is particularly severe, as the data subject to automated analysis can reveal the nature of the information consulted online. Furthermore, such analysis applies globally to all individuals using electronic

[47] M. Tzanou, '*Privacy International* and *Quadrature du Net*: One Step Forward Two Steps Back in the Data Retention Saga?' 28(1) *European Public Law*, 123, 141 (2022).

communication means, including those for whom there is no indication that their behavior might have even an indirect or remote connection to terrorist activities (§174).

Automated analysis can meet the requirement of proportionality only when the member state faces a serious threat to national security that is real and current or foreseeable, provided that data retention is limited to the strictly necessary period (§177). Additionally, strict conditions must be observed: i) national regulations must establish the substantive and procedural conditions for using the data automatically (§176); ii) the measure authorizing automated analysis must undergo effective oversight by a judge or an independent administrative body, whose decision is binding, to verify the existence of a situation justifying the measure and compliance with the required safeguards (§179); iii) the models and predefined criteria underlying this type of data processing must be specific and reliable, enabling results that identify individuals reasonably suspected of participating in terrorist activities, and non-discriminatory (§180); iv) since automated analysis inevitably involves a certain error rate, any positive result must undergo individual review with non-automated tools before any individual measure with adverse effects on the concerned person is taken and the reliability and updating of the predefined models and criteria as well as the databases used must be regularly reviewed (§182); and v) the national authority must publish general information related to automated analysis without individually informing the concerned persons. However, if the data meet the parameters specified in the measure authorizing automated analysis and the authority identifies the concerned person to analyze their data more thoroughly, individual notification of such a person is necessary. This notification must occur only when it does not compromise the functions of the authority (§191).

The Court acknowledged that automated analysis based on criteria such as ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health, or sexual orientation of a person could violate the rights guaranteed by Arts 7 and 8 of the Charter of Fundamental Rights, in conjunction with Art 21 of the same Charter. The predefined models and criteria for such analysis aimed at preventing terrorist activities posing a serious threat to national security cannot be based solely on such sensitive data (§181). However, the scope of the prohibition on using sensitive data in automated anti-terrorism analyses is not clear. It appears that national authorities may use databases that combine sensitive and non-sensitive data, but the Court overlooked that discriminatory effects can also arise indirectly from the intersection of multiple non-sensitive data, including proxy attributes, such as postal codes of certain geographical areas, which can sometimes reveal a person's ethnic origin. On the other hand, the complete exclusion of sensitive data from the dataset used to train the algorithm does not seem entirely advisable, as it could paradoxically negatively impact the precision and accuracy of the algorithm, and distort the reality the artificial

intelligence relies on, rather than the biases on which it bases its decisions.[48]

Further concerns arise from the right to individual review that the Court granted to every subject subjected to automated analysis and the corresponding *ex post* duty (since it is subsequent to the processing) imposed on national authorities. This protection is not entirely in line with what is provided by Art 22 GDPR, which, on one hand, stipulates that the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or significantly affects them in a similar way. On the other hand, in exceptional cases where automated decision-making is authorized by EU or member state law to which the data controller is subject, the data subject has at least the right to obtain human intervention from the controller, to express their point of view, and to challenge the decision. The GDPR generally prohibits automated decision-making, except in some cases, while the Court requires individual review in absolute terms, without exceptions, not even questioning whether, in principle, automated analysis is necessary or prohibited for anti-terrorism purposes, or if, when necessary, it is indispensable or simply useful along with other measures. Furthermore, the individual review mentioned by the Court does not include a prior control of the algorithm, which, on the contrary, the GDPR implements through the data protection impact assessment (Art 35). The Court did not seem to consider the difficulties of ex post review either, given that the algorithm is often a black box, and the justificatory reasons behind its choices are not always trackable, not even through reverse engineering techniques.[49]

V. Dangerous Arrangements and Procedural Fetishes of European Courts

A careful analysis of the decisions of the ECtHR and the CJEU reveals some differences. While the latter operates within a framework of a fundamental incompatibility of mass surveillance with fundamental rights, even when justified by security reasons, the ECtHR views indiscriminate and undifferentiated data retention as a valid technological tool for identifying and combating new threats in the digital world.[50]

The ECtHR considers mass interception as a gradual process where

[48] C. Dwork et al, 'Fairness Through Awareness' *Cornell University ArXiv*, 2012, arxiv.org/abs/1104.3913. Arguing that the use of sensitive data is essential precisely to avoid algorithmic discrimination: I. Žliobaitė and B. Custers, 'Using Sensitive Personal Data May Be Necessary for Avoiding Discrimination in Data-Driven Decision Models' 24 *Artificial Intelligence and Law*, 183 (2016).

[49] On the black box problem in algorithms, see Y. Bathaee, 'The Artificial Intelligence Black Box and the Failure of Intent and Causation' 31(2) *Harvard Journal of Law & Technology*, 889 (2018).

[50] Eur. Court H.R., Grand Chamber, *Big Brother Watch and Others* v *the United Kingdom* n 11 above, §323.

interference with the right to respect for private and family life increases with each stage: i) initial interception of communications and metadata; ii) application of specific selectors to the obtained data; iii) data analysis; and iv) retention and use of the final product, and possible sharing of data with third parties.[51] Conversely, the CJEU seems to consider each of these phases as potential autonomous interferences with fundamental rights.

In reality, beyond these minimal divergences, it appears that in balancing the relationship between new technologies and personal rights, the two courts are heading in the same direction.[52] Both courts have abandoned the strict defense of privacy to build a more nuanced approach to mass surveillance, based on what has effectively been called a procedural fetish.[53] This approach minimally affects the substantive interests of intercepted individuals but provides some procedural safeguards for data authorization, retention, access, and review of decisions made by authorities.[54] There are no more red lines, prohibitions, or limits; digital surveillance measures are now permitted based on procedures, safeguards, and criteria.

The responses given by supranational courts are undoubtedly capable of satisfying the security demands repeatedly raised by national governments, but at the same time, they alter the balance between the right to respect for private and family life, freedom of opinion and expression, and the public interest in fighting crime through the progressive legitimization of digital surveillance, even targeted surveillance. It is likely that the convergence between the two courts will influence future European reforms on personal data protection, strengthening the negotiating power of governments and national security authorities.

[51] ibid §325.

[52] M. Zalnieriute, 'A Dangerous Convergence: The Inevitability of Mass Surveillance in European Jurisprudence' *ejiltalk.org*, 4 June 2021.

[53] M. Zalnieriute, 'Procedural Fetishism and Mass Surveillance under the ECHR' *Verfassungsblog*, 2 June 2021.

[54] M. Milanovic, 'The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för rättvisa' *ejiltalk.org*, 26 May 2021.