Received: 21 June 2021 | Accepted: 3 March 2022

DOI: 10.1111/eulj.12417

KALEIDOSCOPE: ORIGINAL ARTICLE

WILEY

Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks

Valsamis Mitsilegas | Elspeth Guild | Elif Kuskonmaz | Niovi Vavoula*

Abstract

Recent and upcoming judgments of the Court of Justice of the European Union (CJEU) have resurfaced a much-debated topic on the legal limitations of law enforcement authorities and intelligence services under EU law in implementing surveillance operations. In its decisions, the CJEU has reinstated and at times remoulded its case-law on data retention, unearthing a variety of legal issues. This article aims to critically analyse the legal limitations of (indiscriminate) surveillance measures, the role of the private sector in the scheme, and the line between the competence of the Member States and that of the EU on national security matters. It also aims to remark on the latest developments on the reception of the decisions by the Member States and the EU legislator, as well as on the ongoing dialogue between the CJEU and the European Court of Human Rights (ECHR).

1 | INTRODUCTION

The collection and analysis of telecommunications data by law enforcement authorities has been considered an important security tool, with the interest of state authorities not being limited to data related to the content of communications but extended also to the use of various types of telecommunications data—the so-called metadata. As Schneier notes:

> Telephone metadata alone reveals a lot about us. The timing, length and frequency of our conversations reveal our relationships with others: our intimate friends, business associates and

* Valsamis Mitsilegas, Elspeth Guild and Niovi Vavoula are in the Department of Law, Queen Mary University of London. Elif Kuskonmaz is at the School of Law, University of Portsmouth.

> everyone in between. Phone metadata reveals what and who we are interested in and what is important to us, no matter how private. It provides a window into our personalities. It yields a detailed summary of what's happening to us at any point in time.[1]

At the EU level, data retention obligations imposed on private providers were introduced in EU law via Directive 2006/24/EU (Data Retention Directive).[2] In the landmark judgment in *Digital Rights Ireland*,[3] the Court of Justice of the European Union (CJEU) boldly annulled the Directive and rejected a model of mass surveillance based on general and indiscriminate retention of telecommunications metadata. In the absence of EU legislation, several Member States continued to apply national legislation on data retention. However, in *Tele2 and Watson*,[4] the Court examined those national retention regimes within the remit of EU law, in particular its Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (the e-Privacy Directive), only to reiterate its findings and provide guidance to EU and national legislatures on permissible surveillance.[5]

However, the conflict between the CJEU's approach to mass surveillance of telecommunication metadata and Member States' desire to maintain national retention schemes is far from resolved. More cases have reached the Court on the compatibility of United Kingdom (UK), French and Belgian data retention laws with EU law, and on 6 October 2020 two judgments were delivered. *Privacy International* concerned a preliminary reference from the UK non-governmental organisation "Privacy International" that brought an action against the British security and intelligence agencies, questioning the legality of the acquisition and use of bulk communication data by agencies such as the GCHQ, MI5 or MI6.[6] The referring court was unsure about the applicability of EU law, given that, in accordance with Article 4 of the Treaty on European Union (TEU), national security falls outside of the scope of EU law. As for *La Quadrature du Net and Others*,[7] the decision stemmed from preliminary references from the French Council of State and Belgian Constitutional Court in disputes brought against the French and Belgian governments, respectively, by numerous organisations that questioned the legality of the respective national data retention regimes based on the EU Charter of Fundamental Rights, namely the protections enshrined in its Article 7 on the right to privacy and its Article 8 on the right to protection of personal data.[8]

The two judgments must be read together. *Privacy International* sets the stage by bringing retention of telecommunications metadata for national security purposes within the scope of EU law, thus settling an issue that was highly disputed, both politically and academically. *La Quadrature du Net and Others* sets out the limits which apply to state use of the national security exception to the protection of fundamental rights set out in the EU Charter. Read together, and in line with the existing case-law, they constitute a revised EU legal framework within which security services of all Member States must operate and which must be fully respected by both the

[1]B. Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (W.W. Norton and Co., 2015) 24, cited in V. Mitsilegas, 'The Privatisation of Surveillance in the Digital Age', in V. Mitsilegas and N. Vavoula (eds.), *Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives* (Hart, 2021), 101.

[2]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 of public communications networks and amending Directive 2002/58/EC, OJ L105/54, 13.4.2006 (Data Retention Directive).

[3]Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* (C-293/12) and *Kärntner Landesregierung and Others* (C-594/12) [2014] ECLI:EU:C:2014:238.

[4]Joined Cases C-203/15 and C-689/15, *Tele2 Sverige AB v. Post- och telestyrelsen* (C-203/15) and *Secretary of State for the Home Department v. Tom Watson and Others* (C-689/15) [2016] ECLI:EU:C:2016:970.

[5]Directive 2009/136/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L337/11, 18.12.2009 (e-Privacy Directive).

[6]Case C-623/17, *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others* ECLI:EU:C:2020:790.

[7]Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others v. Premier Ministre and Others*, ECLI:EU:C:2020:791.

[8]European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02 (Charter).

national and EU legislatures. This guidance is of key importance in view of the ongoing revision of the e-Privacy Directive,[9] with a number of Member States resisting obedience to the Court's findings.[10] *Privacy International* and *La Quadrature du Net and Others* form the latest episode of the evolution of the Court's case-law on (indiscriminate) data retention, and the resistance from Member States to the Court's rulings highlights the political struggle between EU institutions and Member States on the future of mass surveillance. Amidst these issues, the next question is how the CJEU (potentially in dialogue with the ECtHR) will succeed in facing the complex institutional conflicts.

The CJEU, in a way, has initiated a perilous *pas de deux*, trying to ensure fundamental rights protection through the applicability of EU law while opening the back door to mass surveillance through 'fifty shades' of public interests. The evolution of the Court's case-law highlights the intricate institutional architecture at play when it comes to defining the future of mass surveillance and democracy in the digital era, with a complex part played by the judiciary, the legislative and the executive in a multi-level polity such as the EU. It remains to be seen whether the European formal system of checks and balances will be met substantially through the conciliation of the highest level of fundamental rights protection with the imperatives of national security safeguards.

Against this background, this contribution aims to critically draw four lessons for the EU and national legislatures with regard to (i) the public–private partnership for surveillance activities (Section 2); (ii) the codification of lawful data retention (Section 3); (iii) the permissibility of and applicable criteria for automated analysis of traffic and location data (Section 4); and (iv) the oversight of decisions on data retention (Section 5). Whereas these four themes by no means provide an exhaustive analysis of the judgments, they pick out and attempt to elucidate particularly contentious issues. Taking stock of the multilevel political and legal framework in which EU law inscribes itself, this article further links the CJEU's findings with the latest developments on national courts' reactions to Member States' resistance (Section 6) and the legislative reform of the Directive 2002/58/EC (e-Privacy Directive) (Section 7). It also aims to consider the recent decisions of the European Court of Human Rights (ECtHR) on the bulk interception regime and the question of case-law alignment between the ECtHR and the CJEU on restraining public authorities' power to collect and use personal data (Section 8). A conclusion summarises the main findings of the research and the key legal questions that remain open (Section 9).

2 | SURVEILLANCE AS A PUBLIC–PRIVATE PARTNERSHIP: THE QUESTION OF THE APPLICABLE LAW

The adoption of EU legislation on data retention of telecommunication metadata has brought to the fore the role of the private sector in being co-opted by the state into assuming tasks of generalised and indiscriminate surveillance.[11] As mentioned above, despite the annulment of the Data Retention Directive, EU Member States either continued to apply domestic legislation on retention of telecommunications data or introduced new legislation, much of which enabled the very forms of generalised surveillance found unlawful in *Digital Rights Ireland*. In this context, a key and primary question for safeguarding fundamental rights is whether EU law applies in those cases where there is no specific EU secondary legislation on data retention but retention is mandated by national law. In approaching this question in a series of judgments, the CJEU has centred its analysis on the nature of this public–private partnership in the field of surveillance and extended the reach of EU law by focusing on the key role of the private sector in enabling a system of generalised surveillance under data retention duties.

[9] See Section 7 in this regard.
[10] See Section 6 in this regard.
[11] Mitsilegas, above, n. 1.

2.1 | Developing a holistic approach to mass surveillance: From *Tele2 and Watson* to *Ministerio Fiscal*

In *Tele2 and Watson*, the questions for a preliminary ruling involved national data retention legislation operating in an area where secondary EU law on data retention no longer existed. In that respect, Member States put forward two main arguments to evade the scrutiny of domestic data retention systems in light of EU law. First, following the annulment of the Data Retention Directive, there was no longer a link between domestic schemes and EU law. The latter was thus not applicable. However, the CJEU did establish the applicability of EU law by placing its assessment of national law within the framework of compliance with the e-Privacy Directive. Second, Member States argued that even if EU law was in principle applicable in this context, national laws ultimately were exempt from scrutiny. They fell outside the scope of the e-Privacy Directive on the grounds that the case concerned criminal law and public and national security. In particular, it was submitted that Article 1(3) of the e-Privacy Directive excluded from its scope 'activities of the State' in specified fields, including criminal law and public security, defence and State security,[12] and that Article 15 of the e-Privacy Directive allowed States to restrict its provisions (including via the adoption of data retention measures) to achieve crime control and security objectives which substantially overlapped with those stated in Article 1(3).[13] However, these arguments were not accepted by the CJEU. The Court employed the *effet utile* argument, noting that the measures referred to in Article 15 did fall within the scope of the e-Privacy Directive. Otherwise, Article 15 would be deprived of any purpose.[14]

In establishing the applicability of that Directive in the cases before it, the Court focused on the *activities* of private providers, governed by Article 15 of the e-Privacy Directive,[15] and on the fact that *processing* of personal data is involved in this context. The Court noted that the scope of the e-Privacy Directive extended, in particular, to a legislative measure, such as that at issue in the main proceedings, that required such providers to *retain* traffic and location data, since *to do so necessarily involves the processing, by those providers, of personal data*.[16] Importantly, in establishing the applicability of EU law, the Court linked expressly retention of data by the private sector with *access* to this data by state authorities, by treating retention and access as a continuum of activity. According to the Court, the scope of the e-Privacy Directive extended to a legislative measure relating to the *access* of the national authorities to the data retained by the providers of electronic communications services.[17] Access to the data retained by those providers amounts to processing of personal data which falls within the scope of the e-Privacy Directive.[18] Since data is retained only for the purpose of becoming accessible to competent national authorities, if necessary, national legislation that imposes the retention of that data necessarily entails, in principle, the existence of provisions relating to access by the competent national authorities to the data retained by the providers of electronic communications services.[19] By adopting a holistic approach to the establishment of data retention schemes, and by highlighting the link between retention and access with focus on *national* measures on mass, pre-emptive surveillance, the CJEU sent another clear signal that EU law is applicable in these circumstances and that national legislation is subject to the scrutiny of the Court and to the fundamental rights benchmarks of EU law. Subsequently, the Court found the national schemes in question in breach of EU law. The Court confirmed this approach in favour of the applicability of EU law in *Ministerio Fiscal*, which involved data retention mandated by the state in the context of criminal proceedings.[20]

[12] *Tele2 and Watson*, para. 69.
[13] Ibid., paras. 71–72.
[14] Ibid., para. 73.
[15] Ibid., para. 74. Emphasis added.
[16] Ibid., para. 75. Emphasis added.
[17] Ibid., para. 76. Emphasis added.
[18] Ibid., para. 78.
[19] Ibid., para. 79. See also para. 80: That interpretation is confirmed by Article 15(1b) of Directive 2002/58, which provides that providers are to establish internal procedures for responding to requests for access to users' personal data, based on provisions of national law adopted pursuant to Article 15(1) of that directive.
[20] Case C-207/16, *Ministerio Fiscal* [2018] ECLI:EU:C:2018:788.

In this decision, the CJEU was confronted with questions relating to access by the public authorities, such as the police, to subscriber data for the objective of preventing, investigating, detecting and prosecuting *criminal offences* more generally. The Court opined that access to determine the owners of the SIM cards used for activation of a mobile device entails a (non-serious) interference with the rights to privacy and data protection. Therefore, if the purpose for accessing the retained data is solely to obtain the subscriber identity, Article 15(1) of the e-Privacy Directive allows restrictions of these rights for the prevention, investigation, detection and prosecution of criminal offences. *Ministerio Fiscal* clarified that there may be different levels of interference that require additional or fewer justifications. The Court thus arguably cracked a door open to surveillance activities in cases related to less serious crimes, although access would involve fewer and less sensitive data and only for a restricted period of time.[21] The findings of *Digital Rights Ireland* and *Tele2 and Watson* remained applicable to location and traffic data but not to subscriber data.[22] Furthermore, the scope of the judgment was limited to conditions governing access to personal data. The Court did not discuss their retention.

2.2 | (Over)playing the national security exception card: *Privacy International* and *La Quadrature du Net and Others*

Despite the Court's rulings in *Tele2 and Watson* and *Ministerio Fiscal*, a number of Member States continued with the adoption of domestic data retention legislation, generating another wave of Luxembourg litigation. Having lost the arguments on the non-applicability of EU law based on the crime/security exception, states decided to play in *Privacy International* and *La Quadrature du Net* the national security card. EU law was not applicable in the first place because the domestic measures in question were essentially national security measures and, thus, exempt from the scope of EU law under Article 4(2) of the TEU.

The Court refuted this claim. In particular, in *La Quadrature du Net and Others*, the Court reiterated that Article 15(1) of the e-Privacy Directive covers national measures which regulate the activity of providers of electronic communications services.[23] Thus, the scope of that Directive extends not only to a legislative measure that requires providers of electronic communications services to retain traffic and location data, but *also to a legislative measure requiring them to grant the competent national authorities access to that data*.[24] Such legislative measures necessarily involve *the processing* of the data by those providers and *cannot*, to the extent that they regulate the activities of those providers, *be regarded as activities characteristic of states*, as referred to in Article 1(3) of that Directive.[25] Hence, the Court focused on the centrality of the activities of the private sector to trigger the applicability of EU law and extended the scope of the concept not only to retention but also to enabling access to data by state authorities. The Court found that national security arguments based on Article 4(2) of the TEU cannot invalidate that conclusion. The mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law.[26] The Court declined to apply here its case-law on the PNR legal basis litigation[27] and noted that all operations processing personal data carried out by providers of electronic communications services fall within the scope of the e-Privacy Directive, including processing operations resulting from obligations imposed on those providers by the public authorities.[28] The *source* of the obligation

[21]H. Hijmans, 'Data Protection and Surveillance: The Perspective of EU Law', in V. Mitsilegas and N. Vavoula (eds.), *Privacy and Surveillance in the Digital Era: European, Transatlantic and Global Perspectives* (Hart, 2021), 235.
[22]Council, Document 14,319/18 (23 November 2018).
[23]*La Quadrature du Net and Others*, para. 95, by reference to *Ministerio Fiscal*, para. 34.
[24]Ibid., para. 96, by reference to *Ministerio Fiscal*, paras. 35 and 37. Emphasis added.
[25]Ibid. Emphasis added. Finding otherwise would undermine the effectiveness of EU law. See para. 97.
[26]Ibid., para. 99.
[27]Joined Cases C-317/04 and C-318/04, *European Parliament v. Council of the European Union* (C-317/04) and *Commission of the European Communities* (C-318/04) [2006] EU:C:2006:346, paras. 56–59. This judgment was published in the era of the EU three-pillar structure. The ECJ found that the Agreement between the EU and the US on the transfer of PNR data should have been adopted under the third pillar, as a security measure, and not under the first pillar as originally adopted.
[28]*La Quadrature du Net and Others*, para. 101.

imposed on the private sector is thus immaterial. What matters in order for EU law to apply is the actual activity performed by the private sector. The Court attempted to distinguish private sector activity, in which EU law is applicable, from cases where Member States *directly* implement measures *without imposing processing obligations* on providers of electronic communications services.[29] In these cases, national law applies, which must comply with national constitutional law and the European Convention on Human Rights (ECHR).[30] The Court thus opined that national legislation which requires providers of electronic communications services to retain traffic and location data for the purposes of protecting national security and combating crime, such as the legislation at issue in the main proceedings, falls within the scope of the e-Privacy Directive.[31] By focusing on the central role of the private sector in domestic data retention schemes and defining such role substantively to include both retention and access by the state in its scope, the Court recognised the privatisation of surveillance as a key factor to ensure the applicability of EU law. In this manner, the Court sent a strong signal against Member States' insistence in enacting large-scale data retention measures in domestic law and in thus breaching their fundamental rights obligations under EU law.

3 | OPENING THE BACK DOOR TO MASS SURVEILLANCE? A HIERARCHY OF SECURITY OBJECTIVES

By rejecting the national security exception card and asserting the applicability of EU law, the CJEU was able to assess the compatibility of the legislation in question with the Charter rights. It did so through laying out different clusters of public interest objectives and pairing them with different data retention measures based on its reading of different threat levels and seriousness that denote each objective. The following section traces these rather complex clusters in the CJEU's findings to illustrate the impact of the CJEU's approach in potentially expanding the limitations to mass surveillance.

3.1 | The changing landscape of data retention: A compass for the EU and national legislatures

In *Privacy International*, the Court largely followed the same approach as in *Tele2 and Watson* in finding that the transmission of data to security and intelligence services constitutes a particularly serious interference with the rights to respect for private life and to protection of personal data as well as freedom of expression.[32] Importantly, it constitutes a breach of confidentiality in a general and indiscriminate way, having the effect of transforming the exception to the obligation to ensure the confidentiality of data into the rule, whereas the e-Privacy Directive requires that that exception remain an exception.[33] The Court further stressed that given the quantity of data at issue, their mere retention entails a risk of abuse and unlawful access.[34] The Court distinguished between safeguarding national security and public security as purposes for data retention, with the former viewed as capable of justifying more intrusive measures than those that may be justified by other objectives.[35] However, the Court unequivocally confirmed that commercial operators are not allowed to disclose traffic data and location data to the security and intelligence agencies by means of general and indiscriminate transmission.

Whereas *Privacy International* does not add too much to the data *retention* powers of Member States, it does hint towards a more nuanced approach to this matter. *La Quadrature du Net and Others* is much clearer in that respect. Looking into the various objectives for which telecommunications traffic and location data are retained, one may discern three clusters of public interest objectives. Each of them corresponds to a different degree of threats in

[29]Ibid., para. 103. Emphasis added.
[30]Ibid.
[31]Ibid., para. 104. See, also, for a similar reasoning, *Privacy International*, paras. 30–49.
[32]*Privacy International*, paras. 70–72.
[33]Ibid., para. 69.
[34]Ibid., para. 73.
[35]Ibid., para. 75.

TABLE 1 Data retention after *La Quadrature du Net and Others*

Public interest objectives	Permissible data processing activities	Judgment(s)
Safeguarding national security when there is a 'serious threat', which is 'genuine and present or foreseeable'	Preventive mass retention of traffic and location data of all types	*La Quadrature du Net and Others*, paras. 137–139
	Automated analysis of traffic and location data[a]	*La Quadrature du Net and Others*, paras. 172–182
	Preventive targeted retention of traffic and location data	*La Quadrature du Net and Others*, paras. 146–151
	Real-time collection of traffic and location data	*La Quadrature du Net and Others*, paras. 183–189
	Expedited retention	*La Quadrature du Net and Others*, paras. 160–167 (particularly para. 166)
	Preventive mass retention of civil identity data	*La Quadrature du Net and Others*, paras. 157–159
Combating serious crime, preventing 'serious threats' or 'serious attacks' on public security (and a fortiori national security)	Preventive targeted retention of traffic and location data limited by: (a) persons must be pre-identified on the basis of objective evidence; (b) geographical criterion	*La Quadrature du Net and Others*, paras. 146–151
	Preventive mass retention of traffic and location data without differentiation/exception/limitation is prohibited Except preventive mass retention of IP addresses	*Digital Rights Ireland/Tele2 and Watson/La Quadrature du Net and Others*, paras. 140–145 and 152–159
	Real-time collection of traffic and location data (in particular situations: terrorism only?)	*La Quadrature du Net and Others*, paras. 183–189
	Expedited retention	*La Quadrature du Net and Others*, paras. 160–167
	Preventive mass retention of data on civil identities	*La Quadrature du Net and Others*, paras. 157–159
Combating crime and safeguarding public security	Preventive mass retention of data on civil identities	*Ministerio Fiscal*, para. 62/*La Quadrature du Net and Others*, paras. 157–159

[a]Notably, the CJEU found the automated analysis of personal data in and of itself an interference with fundamental rights irrespective of their subsequent collection.

terms of their nature and seriousness, which may thus justify different sets of retention activities. Table 1, while taking stock of previous case-law, illustrates how *La Quadrature du Net and Others* has provided different thresholds of protection depending on the public interest at stake—national security, including the prevention of terrorism, the fight against serious crime or the prosecution and punishment of less serious offences[36]—enabling a gradation of legislative measures on data retention, with the first level of objective being safeguarding national security when there is a 'serious threat', which is 'genuine and present or foreseeable', followed by the second level of objective of combating serious crime, preventing 'serious threats' or 'serious attacks' on public security, and the final level of objective of combating crime and safeguarding public security.

[36]L. Woods, 'When Is Mass Surveillance Justified? The CJEU Clarifies the Law in Privacy International and Other Cases' (*EU Law Analysis*, 7 October 2020), http://eulawanalysis.blogspot.com/2020/10/when-is-mass-surveillance-justified.html.

In particular, the Court looked at the objective of national security, which in its view:

> corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic and social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities.[37]

This objective is different from the objectives of combating crime in general, even serious crime, and of safeguarding public security. Threats to national security are distinguished, in terms of their nature and particular seriousness, from the general risk of tensions or disturbances, even of a serious nature, affecting public security.[38] Therefore, whereas the objectives of public security and fighting serious crime cannot justify mass data retention, as per the Court's pronouncements in *Digital Rights Ireland* and *Tele2 and Watson*, safeguarding national security may justify more serious interferences, such as the general and indiscriminate preventive retention of traffic and location metadata.[39]

However, such preventive retention on all users of electronic communications systems is permitted *only if* certain conditions are fulfilled. Mass retention must be for a limited period and only as long as there are sufficiently solid grounds for considering that the Member State is confronted with a serious threat to national security, which is shown to be genuine and present or foreseeable.[40] The time-limited character of retention is crucial. The Court contends that, due to the ongoing nature of a threat to national security, renewing the instructions to telecommunications providers to retain data is possible for a 'foreseeable period of time'.[41] Furthermore, data retention cannot be systematic in nature and must be subject to limitations and strict safeguards against the risk of abuse.[42] In addition, the instruction to communications providers to retain data must be subject to effective review, either by a court or by an independent administrative body whose decision is binding, so as to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed.[43] Another novelty of the judgment is that the objective of safeguarding national security, 'particularly to prevent terrorism'—thus not excluding other instances—justifies automated analysis of traffic and location data, which involves general and indiscriminate processing of that data by public authorities, subject to specific safeguards, as analysed in the next section.[44]

The second level in the hierarchy of objectives includes combating serious crime, preventing 'serious threats' or 'serious attacks' on public security, and a fortiori national security. In line with the Court's findings in *Digital Rights Ireland* and *Tele2 and Watson*, the e-Privacy Directive and the Charter do not preclude measures of *targeted* retention of traffic and location data only, which nonetheless *also* entail a 'particularly serious interference' with the rights to privacy and protection of personal data and freedom of expression.[45] Perhaps, if the Court had taken on board previous criticism that bulk retention of telecommunications metadata amounts to a violation of the essence of the right to privacy and data protection and freedom of expression, then confusion regarding which interferences are particularly serious would not have occurred.[46] The Court provided further guidelines on how to interpret the term 'targeted surveillance'. Individuals affected must be identified in advance, on the basis of objective evidence, as posing a threat to public or national security.[47] As mentioned in *Tele2 and Watson*, the instruction for targeted surveillance may also be based on a geographical criterion, and the areas may include places with a high incidence of serious crime, places that

[37] *La Quadrature du Net and Others*, para. 135.
[38] Ibid., para. 136.
[39] Ibid.
[40] Ibid., para. 137.
[41] Ibid., para. 138.
[42] Ibid.
[43] Ibid., para. 139. More on this requirement in Section 5.
[44] These safeguards mainly derive from Opinion 1/15 [2016] ECLI:EU:C:2016:656, which is discussed below in Section 4.1.
[45] *La Quadrature du Net and Others*, para. 146.
[46] For a discussion, see Mitsilegas, above, n. 1.
[47] *La Quadrature du Net and Others*, para. 149.

are particularly vulnerable to the commission of serious criminal offences, such as places or infrastructure which regularly receive a very high volume of visitors, or strategic locations, such as airports, stations or tollbooth areas.[48]

Whereas preventive general and indiscriminate retention of traffic and location data in relation to serious crime and the prevention of serious threats to public security and national security is prohibited, in a deviation from previous case-law, the Court provides an exception in relation to IP addresses, which, still according to the Court, constitute traffic data. In particular, the Court found that their retention—relating to the source of communication and not its recipient—is less sensitive than the other traffic data. They do not disclose any information about third parties who were in contact with the person who made the communications.[49] That said, IP addresses may be used for tracking an Internet user's complete clickstream. Hence, the entire online activity that facilitates the construction of a detailed profile of the user may be deduced.[50] Therefore, the retention and analysis of that type of data constitutes a serious—but not a *particularly* serious—interference with the rights to privacy and protection of personal data.[51] In balancing those rights with the needs of law enforcement, the Court considered that in cases of offences committed online, such as in cases concerning particularly serious child pornography offences,[52] the IP addresses might be the only means of investigation to identify the person to whom that address was assigned when the offence was committed.[53] As a result, a more nuanced approach was preferred to allow general and indiscriminate retention of IP addresses of all persons who own terminal equipment permitting access to the Internet without, at first sight, any connection with the objectives pursued, and without being suspected of serious crimes. Nevertheless, the retention period must not exceed what is strictly necessary in light of the objective pursued, and substantive and procedural conditions regulating the use of that data must be foreseen.[54]

The Court further affirmed that expedited retention of traffic and location data processed and stored by service providers for a specified period of time is permissible for combating serious crime and safeguarding national security.[55] Such expedited retention may take place in situations in which it becomes necessary to retain the data beyond statutory data retention periods so as to shed light on serious criminal offences or attacks on national security when the offences or attacks have already been established or if their existence may reasonably be suspected.[56] Specific safeguards must exist here as well. Expedited retention must be ordered by a decision subject to effective judicial review[57] and may not only involve the suspected perpetrators of the offence in question but also extend to the victim, their social or professional circle or even specified geographical areas, such as the place where the offence was committed or prepared.[58] In addition, access to the retained data for prosecuting and punishing an ordinary criminal offence may in no event be granted where the retention of such data has been justified by the objective of combating serious crime or safeguarding national security.[59]

As for the retention of real-time traffic and location data, this also constitutes a *particularly serious* interference with the rights to privacy, data protection and freedom of expression, 'since that data provides the competent national authorities with a means of accurately and permanently tracking the movements of users of mobile telephones'.[60] As a result, the data must be considered as 'particularly sensitive', because the monitoring is 'virtually

[48]Ibid., para. 150.
[49]Ibid., para. 152.
[50]Ibid., para. 153.
[51]Ibid.
[52]Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ L 335/1, 17.12.2011.
[53]*La Quadrature du Net and Others*, para. 154.
[54]Ibid., para. 156.
[55]Ibid., para. 164.
[56]Ibid., para. 161.
[57]Ibid., para. 163. This is in line with the Council of Europe's Convention on Cybercrime of 23 November 2001 (European Treaty Series No. 185), art 16 of which stipulates that the parties to that convention are to adopt such legislative measures as may be necessary to enable their competent authorities to order or similarly obtain the expedited preservation of traffic data that has been stored by means of a computer system, in particular where there are grounds to believe that that data is particularly vulnerable to loss or modification.
[58]Ibid., para. 165.
[59]Ibid., para. 166.
[60]Ibid., para. 187.

total'.[61] Therefore, such retention may be justified for the purpose of the prevention of terrorism only in respect of persons for whom there is a valid reason to suspect that they are involved in terrorist activities.[62] The measure authorising real-time collection must be subject to a prior review carried out either by a court or by an independent administrative body whose decision is binding.[63] Lastly, the Court notes that, in urgent cases, the review should take place within a short time.[64]

Under the third level of public interest objectives, the objective of preventing, investigating, detecting and prosecuting criminal offences—irrespective of their seriousness—and safeguarding public security are included. In that respect, the Court reiterated its pronouncements in *Ministerio Fiscal* that general and indiscriminate retention of subscriber information—in the Court's words, data about 'civil identity'—is permitted. This is because such information does not allow ascertaining the date, time, duration, and recipients of the communications made, the locations where those communications took place or their frequency with specific people in a given period.[65] As a result, no information on the communications and consequently on the users' private lives was sent.[66] Therefore, this interference does not qualify as serious.

3.2 | A CJEU compass for fundamental rights protection or mass surveillance?

La Quadrature du Net and Others has provided a handy codification of previous case-law, as well as important clarifications *and qualifications* as regards states' powers to conduct generalised and indiscriminate or targeted surveillance of electronic communications data.[67] These judgments should be seen as a culmination of efforts on behalf of the Court to reach a compromise and re-strike the balance between fundamental rights and the (loud and clear) desire of the Member States to uphold data retention schemes in favour of the latter. In order to address criticisms against its previous approach, the Court broke open the door of mass surveillance to security and intelligence services, including in its most intrusive forms, namely automated analysis and real-time collection.[68] This flexibility is even extended to the admissibility of unlawfully collected evidence. After all, even if national data retention laws are violating EU law, national courts are given the discretion to accept such retained data as evidence in criminal proceedings, as the admissibility of evidence will largely depend on the national procedural rules.[69] As a result, the judgment may be seen as primarily a victory for the law enforcement community, the surveillance powers of which have been significantly expanded.

The isolation of IP addresses from other types of traffic data is another important expansion of surveillance powers. The finding that IP addresses are part of traffic data is interesting, as in Member States an IP address, port number for dynamic IP addresses and subscriber identification module (SIM) and device identification numbers (e.g. international mobile subscriber identity (IMSI) or international mobile equipment identity (IMEI)) are deemed either as subscriber data or traffic data.[70] Had the Court considered IP addresses as falling within the category of subscriber data, the pronouncements in *Ministerio Fiscal* would have applied and mass retention would be possible.

[61]Ibid.. See *Ben Faiza v. France* [2018] ECHR 153, para. 74.
[62]Ibid., para. 188. Otherwise, the pronouncements of *Tele2 and Watson* (para. 119) will apply, and objective evidence is required so that it can be deduced that that data might, in a specific case, make an effective contribution to combating terrorism.
[63]Ibid., para. 189.
[64]Ibid.
[65]Ibid., para. 157.
[66]Ibid.
[67]For example, a clarification was made on the meaning of national security which must be distinguished from public security and therefore covers more serious issues than the objectives listed in Article 15 of the e-Privacy Directive. Another important clarification involved the flawed reference in *Digital Rights Ireland* that Article 6 of the Charter provides a right to security. The Court held that since that provision applies to deprivations of liberty by a public authority, the Article cannot be interpreted as imposing an obligation on public authorities to take specific measures to prevent and punish certain criminal offences (paras. 123–125).
[68]J. Sajfert, 'Bulk Data Interception/Retention Judgments of the CJEU—a Victory and a Defeat for Privacy' (*EU Law Blog*, 26 October 2020), https://europeanlawblog.eu/2020/10/26/bulk-data-interception-retention-judgments-of-the-cjeu-a-victory-and-a-defeat-for-privacy/.
[69]Ibid.
[70]Commission, 'Study on the retention of electronic communications non-content data for law-enforcement purposes' (2020), https://op.europa.eu/en/publication-detail/-/publication/081c7f15-39d3-11eb-b27b-01aa75ed71al.

Therefore, it may be speculated that the ambiguity in categorising IP addresses at the national level led the Court to isolate that type of metadata from traffic data and permit their general and indiscriminate retention.

Further questions are raised as to whether *La Quadrature du Net and Others* has in fact given Member States a *carte blanche* to issue time-limited, but renewable general and indiscriminate data retention instructions, for the objective of safeguarding national security, under an ongoing specific threat.[71] Another related concern involves the Court's silence on the conditions of access to traffic and location data generally and indiscriminately retained for the objective of national security, with the view put forward that such access is not limited to intelligence services for the purposes of safeguarding national security. If the conditions of access are taken from *Tele2 and Watson*, then by combining the conditions for general and indiscriminate data retention from *La Quadrature du Net and Others* and the conditions for access from *Tele2 and Watson*, Member States could first demonstrate and specify a threat to national security, then order the general and indiscriminate retention of traffic and location data, and finally allow access to such retained data to law enforcement authorities for the purpose of fighting serious crime.[72] This is a particularly worrying scenario, but one must not forget that not any threat to national security reaches the threshold to justify bulk retention, and the requirement for prior review by a judicial or another independent authority, as will be discussed in Section 4, is meant to halt possible abuses in this respect. Importantly, in its analysis on the expedited retention of data, the Court is mindful to clarify that access to traffic and location data may in principle be justified only by the public interest objective for which providers were ordered to retain that data. Consequently, access to data for purposes related to an ordinary offence may in no event be granted where the retention has been justified by the objective of combating serious crime or safeguarding national security.[73] An application by analogy of this line of argumentation points to the direction that a 'mix-and-match' approach, whereby access to retained data concerns objectives of a different, less serious degree, as per the classification earlier, will be unlawful. Such expansive interpretation of the Court's approach would negate previous case-law, even though that same case-law has been relied upon and there is no indication of the Court backing down from that line of thinking. Table 1 further confirms this argument that the Court's approach has been built around and largely in line with its previous case-law—albeit with certain nuances. That said, it is acknowledged that a clear distinction between the classification of the different public interest objectives may not always be an easy task. In any case, support for such reading does not seem to be widespread, as the judgments have not been received with enthusiasm by the Member States. On the contrary, Member States continue to try to find loopholes to circumvent the Court's findings, even though on initial observation, national courts seem to have followed them.[74]

A cautious and restrictive interpretation of the findings of the Court is instead supported by a close reading of its latest judgment on the data retention saga. In *HK*, the Court was called to reply to queries regarding the access to electronic communications data by law enforcement authorities and their use in criminal proceedings. The Court found that access for the purposes of the prevention, investigation, detection and prosecution of criminal offences to a set of traffic or location data that are liable to provide information regarding the communications made by a user of a means of electronic communication, or the location of the terminal equipment and thus to allow precise conclusions to be drawn concerning their private life is only permitted in relation to serious crimes. Consequently, any attempt to disassociate retention from access are destined to fail the legality test. Contrary to the Opinion of the Advocate General on this matter,[75] further considerations and criteria such as *the length of the period* for which access to those data is sought and the *quantity or nature of the data available* in respect of such a period are irrelevant in this assessment.[76]

[71]Sajfert, above, n. 68.
[72]Ibid.
[73]*La Quadrature du Net and Others*, para. 166.
[74]Section 6. Also, see 'EU: Data Retention: Council Presidency Tells National Ministers that "a Solution is Necessary"' (*Statewatch*, 8 March 2021), https://www.statewatch.org/news/2021/march/eu-data-retention-council-presidency-tells-national-ministers-that-a-solution-is-necessary/.
[75]Case C-746/18, *HK v. Prokurauur*, Opinion of Advocate General Pitruzzella delivered on 21 January 2020.
[76]Case C-746/18, *HK v. Prokuratuur* [2021] ECLI:EU:C:2021:152, para. 35.

After all, in its latest episode on the adjudication of national data retention regimes, the CJEU seemed to have retreated from a strong condemnation of indiscriminate data retention regimes while applying EU law to the domain of national security that Member States have pleaded to escape the Court's jurisdiction. Still, it tried to contain surveillance powers in light of different clusters of public security objectives. Ultimately, the difficult equilibrium exercise performed so far by the Court between fundamental rights protection and other legitimate interests pursued by Member States seems to point to a weakening of the former to the benefit of the latter. In so doing, the Court legitimises a discourse whereby fundamental rights protection and national security considerations are pitted against each other.

With more cases on mass surveillance pending, such as *Ligue des droits humains*,[77] on which Advocate General Pitruzzella recently issued its opinion,[78] the questions that the Court will have to decide inscribe themselves in the framework of one of the main dilemmas of contemporary liberal democratic constitutionalism: how to define the equilibrium between the individual and the collectivity in the data era, where digital technologies have allowed the collection, retention, processing and analysis of huge masses of personal data for predictive purposes? The indiscriminate collection of personal data and the use of digital technologies by public authorities can give birth to a digital panopticon, that is to say, a government which watches everything without being watched. However, European constitutionalism—national and supranational—with the central place conferred to the individual and its freedoms, puts an important barrier to the advent of a mass surveillance society, especially after the recognition of the fundamental rights to privacy and data protection. To which extent, however, can this barrier be set without seriously undermining certain fundamental interests of society, such as those previously mentioned for example, which may yet have constitutional ties? We are at the heart of the question of the relationship between the individual and the collectivity in a digital society. This is a question which necessitates, on the one hand, the search for and the implementation of subtle equilibria between the interests of the collectivity and individual rights, starting from the absolute importance of the latter in the European constitutional heritage, and, on the other hand, the setting of safeguards against abuses. We are here as well, as part of the contemporary version of a classical theme of constitutionalism, because, as mentioned by Advocate General Pitruzzella in his opinion on *Ligue des droits humains* with reference to the *Federalist no. 51*, men are not angels, and this is why legal mechanisms are necessary to limit and control government.[79] The following section turns to the CJEU's findings on controlling a seemingly emergent surveillance power—that is, automated analysis of personal data.

4 | WHITHER AUTOMATED ANALYSIS OF PERSONAL DATA?

As the volumes of metadata have grown exponentially, security and intelligence services have resorted to sophisticated tools of automated analysis, which have been developed thanks to increasing computational powers to enhance their abilities to process data. As mentioned earlier, the CJEU considered in *La Quadrature du Net and Others* one form of such automated analysis in connection with the processing of traffic and location data in pursuing the interests of national security. The Court delivered its findings on the type of automated analysis that was challenged in *La Quadrature du Net and Others* largely based on its earlier observations on the use of automated analysis in border controls. This section thus considers the state of play of the CJEU case-law on automated analysis before the

[77]Case C-817/19, *Ligue des droits humains* (pending).

[78]Case C-817/19, *Ligue des droits humains*, Opinion of Advocate General Pitruzzella delivered on 27 January 2022, ECLI:EU:C:2022:65. In his opinion in *Ligue des droits humains*, the Advocate General was satisfied with how automated analysis was drafted in the EU PNR Directive because it contained sufficient guarantees and safeguards and met with the requirements observed previously by the CJEU in Opinion 1/15. For a brief commentary of the opinion of Advocate General, see: C. Thönnes, 'A cautious green light for technology-driven mass surveillance' (*Verfassungsblog*, 28 January 2022), https://verfassungsblog.de/green-light/.

[79]Case C-817/19, *Ligue des droits humains*, Opinion of Advocate General Pitruzzella delivered on 27 January 2022, ECLI:EU:C:2022:65, para. 2, translated from French by the authors.

Court delivered its *La Quadrature du Net and Others* decision, before describing the circumstances under which the automated analysis of traffic and location data was found to be permissible.

4.1 | Opinion 1/15: A glimpse into the automated analysis of personal data

La Quadrature du Net and Others was not the first time the CJEU recognised the implications of automated analysis of personal data on individuals' fundamental rights. Three years earlier, the Court had the opportunity in Opinion 1/15 to engage with this question in a different context. At stake was the legality of automated decision-making that involved processing of personal data as part of Canada's border control pre-screening program. The latter involves automated cross-checking and analysis of information about everyone who buys a flight ticket to Canada. The premise of that automated process is to identify supposedly high-risk travellers, who would then be subjected to secondary screening to be admitted to the country.[80] As part of this operation, airline companies, regardless of where they are based, are obliged by law to share passenger information with the Canadian border control authority.

When initially imposed, this obligation caused a backlash in the EU, whose data protection laws restrict data transfers outside the EU. So far as EU-based companies were concerned, the legality of the sharing of data was ensured through the conclusion of an agreement between the EU and Canada.[81] Upon the expiration of that agreement, a lengthy negotiation process ensued to replace it. The new draft Agreement faced a legal challenge by the European Parliament whose approval is required to render it effective under EU law.[82] The occasion thus arose for the CJEU to make some initial observations on the automated processing of passenger information as part of Canada's border control pre-screening operation.[83] The CJEU's findings received different reactions, from commending its detailed analysis of the draft Agreement to more sceptical commentaries that were wary about the CJEU's approval of indiscriminate transfer and collection of information.[84] In hindsight, the CJEU's considerations on the automated processing of passenger information were very influential in its later deliberation on the permissibility of the automated analysis of traffic and location data in *La Quadrature du Net and Others*.

The requirements that the CJEU set forth in Opinion 1/15 regarding the permissibility of the automated analysis of passenger information can be summarised as follows. First, the pre-established models and criteria according to which the automated analysis is carried out should be 'specific and reliable' to target individuals who might be under a reasonable suspicion of participating in the commission of serious crimes or terrorist offences, and should be 'non-discriminatory'.[85] Second, if the automated analysis involves cross-checking of other databases, those databases should be reliable, up-to-date and limited to their use in connection with the fight against terrorism and serious crime.[86] Third, based on the evidence presented during the proceedings on the margin of error regarding the identification of high-risk travellers, any positive results following the automated analysis must be re-examined by non-automated means.[87] On this point, the CJEU recognised that the draft Agreement itself contained a provision prohibiting sole automated decision-making, and interestingly, it did not list it among the requirements mentioned in

[80]On general information on Canada's passenger pre-screening, see D. Lyon, 'Airport Screening, Surveillance, and Social Sorting: Canadian Responses to 9/11 in Context' (2006) 48(3) *Canadian Journal of Criminology and Criminal Justice*, 397; P. Hobbing, 'Tracing Terrorists: The EU-Canada Agreement in PNR Matters' (CEPS Special Report, September 2008).

[81]Council Decision 2006/230/EC of 18 July 2005 on the conclusion of an Agreement between the European Community and the Government of Canada on the Processing of API/PNR data [2006] OJ L82/14; Agreement between the European Community and the Government of Canada on the Processing of Advance Passenger Information and Passenger Name Record data [2006] OJ L 82/15, 21.3.2006.

[82]European Parliament, 'MEPs Refer EU-Canada Air Passenger Data to the EU Court of Justice' (25 November 2014), http://www.europarl.europa.eu/news/en/press-room/20141121IPR79818/meps-refer-eu-canada-air-passenger-data-deal-to-the-eu-court-of-justice.

[83]Opinion 1/15, paras. 190–211.

[84]C. Docksey, 'Opinion 1/15: Privacy and Security, Finding the Balance' (2017) 24(6) *Maastricht Journal of European and Comparative Law*, 768; A. Vedaschi, 'The European Court of Justice on the EU-Canada Passenger Name Record Agreement' (2018) 14 *European Constitutional Law Review*, 410; E. Celeste, 'The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios' (2019) 15(1) *European Constitutional Law Review*, 134.

[85]Opinion 1/15, para. 172.

[86]Ibid.

[87]Ibid., para. 173.

its *ratio decidendi*. Finally, the joint review that was anticipated by the draft Agreement itself should cover the review of the pre-established models and criteria, as well as relevant databases, to make sure that they exhibit the features listed above.[88] Similar to the CJEU's finding on the prohibition on the sole automated decision, this requirement was not later mentioned in its *ratio decidendi*.

4.2 | *La Quadrature du Net*: Amping up the restraints on automated analysis

In *La Quadrature du Net and Others*, the CJEU further endorsed certain requirements set out in Opinion 1/15, despite the fact that the context in which the autonomous analysis took place as well as the data against which that analysis was carried out differed.[89] Here, the automated analysis involved applying algorithms to traffic and location data of users of electronic communications services to detect suspicious patterns and behaviours in pursuance of safeguarding national security, as opposed to information about whoever bought a flight ticket to Canada in Opinion 1/15. Once a pattern or behaviour is detected, the Prime Minister can authorise that the relevant data be de-anonymised and collected and that it should be used within 60 days of collection. Such authorisation did not exist in the case of the pre-screening procedure in Opinion 1/15. The automated processing was implemented right away as a primary inspection to target those who must undergo secondary screening.[90]

In assessing the legality of automated analysis of traffic and location data, the CJEU first had to address if this practice triggered fundamental rights protections under the Charter, namely Article 7 on the right to privacy and Article 8 on the right to protect personal data. As a starting point, even though the automated analysis did not involve data *collection*, the Court observed that this technique provided the possibility of de-anonymising the traffic and location data, which could allow the individual concerned to be indirectly identified and as such would involve processing of *personal data*.[91] This data processing also triggered a question pertaining to the confidentiality of communications, in relation to the right to privacy, which encompasses the right to respect communications.[92] The CJEU further noted that this data processing amounted to a *serious* interference based on two factors. Firstly, it involved the monitoring of the metadata of everyone who uses the service.[93] Secondly, the processing may reveal the information consulted online.[94] In simpler terms, those two factors indicated the expansive scope of the automated analysis. According to the Court, this was not a reason to conclude automatically to a violation of the rights enshrined in the Charter. However, as explored below, the seriousness of that interference was a factor in determining the parameters for its permissibility.

In setting out the permissibility conditions for the automated analysis under Article 52(1) of the Charter,[95] the CJEU first recalled its findings in the earlier paragraphs on the strict necessity test for generalised and indiscriminate collection of traffic and location data for national security purposes.[96] It reiterated that automated analysis is not ruled out due to its general and indiscriminate nature. It can be justified if it meets the strict necessity test.[97] Based

[88]Ibid., para. 174.

[89]In *Privacy International*, the UK surveillance regime that was subject of the preliminary ruling set out a 'selective' operation to filter through the retained data, but the legality of that operation in and of itself was not disputed.

[90]*La Quadrature du Net and Others*, para. 43.

[91]Ibid., paras. 170–171. Anonymous data only eschew the scope of application of EU data protection law (and thus Article 8 of the Charter) if the data can never relate to the individual or there is no reasonable likelihood that it can make the individual identifiable. See Recital 26 and Art 4, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1, 4.5.2016 (GDPR). On the 'identifiability' requirement, see Opinion 1/15, para. 122; C-582/14 *Breyer v. Bundesrepublik Deutschland* [2016] EU:C:2016:779.

[92]*La Quadrature du Net and Others*, para. 173.

[93]Ibid., para. 174.

[94]Ibid.

[95]Article 52(1) of the Charter reads as '[a]ny limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others'.

[96]Ibid., para. 175. See Section 3.

[97]*La Quadrature du Net and Others*, para. 176.

on these strict parameters, the CJEU recalled that automated analysis should be conducted in order to safeguard against serious national security threats including terrorism.[98] In other words, the gravity of "serious" national security threats, including terrorism, could serve as a legitimate aim to justify the infringement. In line with its findings in the earlier paragraphs on mass data retention regimes for national security purposes, the CJEU also noted that a national security threat must be genuine and present or foreseeable.[99]

A time limit for automated analysis could also be inferred from the CJEU's findings. It mentioned that the analysis for 'a strictly limited period, may be justified', presumably suggesting that the automated analysis in this context must be restricted to a strict time period.[100] Further, the decision of the body authorising the automated analysis must be subject to an effective review by a body whose decision is binding.[101] The review must verify that a serious threat to national security exists and 'the conditions and safeguards' that must be laid down are observed.[102]

The CJEU further unpacked the automated decision-making itself. Using Opinion 1/15 as a precedent,[103] it engaged with 'pre-established models and criteria'—which can be simplified as algorithms—the use of which would flag up suspicious patterns of behaviour. Accordingly, steps should be taken to make sure that those pre-established models and criteria are specific and reliable to allow individuals who might be under a reasonable suspicion to participate in terrorist activities to be identified. Those models and criteria should also be non-discriminatory.[104] Regarding the latter, the CJEU noted the discriminatory effect of pre-established models and criteria that are designed on the premise that individuals' protected characteristics may be relevant for the prevention of terrorism.[105] For this reason, the models or criteria to execute an automated analysis cannot be based on sensitive data *in isolation*.[106] Moreover, the Court recognised the need to regularly re-examine the algorithms and the databases used to ensure that they are reliable and up-to-date and, consequentially, in practice, are non-discriminatory and limited to what is strictly necessary to achieve the purpose of preventing a terrorist activity that amounts to a serious threat to national security.[107] Lastly, the CJEU held that because of the margin of error that may result from the automated analysis, there has to be an individual non-automated re-examination of a positive result that flags the metadata before adopting a measure that may have an adverse effect on the person concerned.[108]

4.3 | The future of automated analysis and open questions

On initial observation, the Court's findings on automated analysis are a step in the right direction. The Court considered this type of analysis, in and of itself, as constitutive of a fundamental rights intrusion. This entailed conditioning its permissibility upon the observance of a series of requirements pertaining to the EU fundamental rights framework. At the same time, the CJEU's reasoning may raise novel issues, some of which partially relate to the CJEU's reference (solely) to Opinion 1/15.

The first issue is the Court's attempt to consider the discriminatory effects of the automated analysis in question. The reference to Opinion 1/15 to support its finding that sensitive data must be excluded from the pre-established models is interesting because the Court did not explicitly set out that condition in the Opinion to address

[98]Ibid., para. 177.
[99]Ibid.
[100]Ibid., para. 178.
[101]Ibid., para. 179. See Section 5.
[102]Ibid. The meaning of the 'conditions and safeguards' mentioned in the relevant paragraph are not detailed by the Court so far as the Charter right infringement by automated analysis is concerned. It is unclear whether the Court refers to the requirements it considers later in terms of those requirements that need to be observed to enable that pre-established models and criteria are non-discriminatory, accurate and up to date, because observing those requirements seems to be tied into regular assessment of the systems as opposed to reviewing the authorisation of the system per se.
[103]See Section 4.1.
[104]*La Quadrature du Net and Others*, para. 180.
[105]Ibid.,
[106]Ibid., para. 181. Emphasis added.
[107]Ibid., para. 182.
[108]Ibid.

the potentially discriminatory effect of the automated analysis challenged before it. Rather, it considered that transferring data, from which sensitive data of arriving passengers may be inferred, would not be permissible unless a legitimate ground to justify that transfer existed.[109] Clearly, once transfer of information containing sensitive data were to be discontinued, those data would not be included in the automated analysis process. This, however, may not necessarily impede the discriminatory effect of the automated data processing activity.[110]

Excluding sensitive data from the dataset to be fed into the criteria that make up the algorithm may prevent discriminatory treatment resulting from automated analysis, but only to an extent. An algorithmic analysis may, for example, have an "indirect" discriminatory effect on people. Although it may not be conducted by reference to a protected characteristic, it may nevertheless have a discriminatory effect on a group of people sharing the same protected characteristic by putting them at a particular disadvantage.[111] More broadly, the ongoing debate on algorithmic bias and its legal treatment shows the complexity of addressing the issue.[112] There are, then, reasons to be wary of the phrase 'in isolation' that the Court uses when qualifying the exclusion of sensitive data from the criteria and profiles to execute automated analysis. A potential interpretation of this finding might be that sensitive data could be included in the dataset as long as it is introduced with non-sensitive data. The Court's numerous references to the principle of non-discrimination indicates that this kind of limited reading might not have been its intention, not least because to argue otherwise would still raise problems in relation to potentially "indirect" differential treatment.[113] Arguably, by relying solely on Opinion 1/15, the CJEU may have prevented, or at least hindered, further clarifications on the requirements that the models or criteria must meet with. There is therefore scope for the CJEU to re-evaluate and reformulate its interpretation of the discriminatory effect of automated decision-making when the occasion arises.

The second issue is the Court's insistence on ongoing revision of algorithmic models that may resonate with the lively debate on algorithmic transparency and unboxing the proverbial "Black box" by auditing algorithms.[114] There is, however, not a single line of authority on the best practices of algorithmic auditing.[115] As far as EU data protection law is concerned, discussions unfolded as to the extent to which the relevant national law may comprise aspects of algorithmic analysis, despite not explicitly requiring it.[116] Some mechanisms, which have sprung from the privacy

[109]Opinion 1/15, para. 172.

[110]Vedaschi, above, n. 84, 422 [criticising that the finding in Opinion 1/15 is a limited solution against the differential treatment].

[111]A. Romei and S. Ruggieri, 'Discrimination Data Analysis: A Multi-disciplinary Bibliography', in B. Custers et al. (eds.), *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases* (Springer, 2013), 109; EU Agency for Fundamental Rights (FRA), 'Big Data: Discrimination in Data-Supported Decision Making' (Fundamental Rights Agency, 2018), https://fra.europa.eu/en/publication/2018/bigdata-discrimination-data-supported-decision-making; F. Zuiderveen Borgesius, 'Discrimination, Artificial Intelligence, and Algorithmic Decision-Making' (Council of Europe, Directorate General of Democracy, 2018), https://rm.coe.int/discrimination-artificial-intelligence-and- algorithmic-decision-making/1680925d73.

[112]We do not claim to present a typology of algorithmic bias. In broad terms, there may be different causes of algorithmic bias, for example due to issues with the data (bias in the training data or inaccuracy of the data) or the algorithmic design (reflecting bias or being poorly designed). Algorithmic bias is thus addressed in the initiatives to provide an ethical framework for AI, the soft-law, guidelines and recommendations on the use of AI. See: High-Level Expert Group on Artificial Intelligence, 'Ethics Guidelines for Trustworthy AI (April 2019); Council of Europe, Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes, Decl(13/02/2019)1. The proposed EU Artificial Intelligence Act (AIA) bids to address algorithmic bias, too. Recital 38 reads 'Actions by law enforcement authorities involving certain uses of AI systems are characterised by a significant degree of power imbalance and may lead to surveillance, arrest or deprivation of a natural person's liberty as well as other adverse impacts on fundamental rights guaranteed in the Charter. In particular, if the AI system is not trained with high quality data, does not meet adequate requirements in terms of its accuracy or robustness, or is not properly designed and tested before being put on the market or otherwise put into service, it may single out people in a discriminatory or otherwise incorrect or unjust manner.'

[113]Note here that under the ECHR and EU law, treatments that constitute indirect discrimination is not prima facie a violation of the right to enjoy fundamental rights without discrimination based on a number of protected characteristics because the relevant treatment may be justified subject to requirements. For a brief description, see Zuiderveen Borgesius, above, n. 111, 18–20.

[114]T. Zarksy, 'The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making' (2016) 41(1) *Science, Technology, & Human Values*, 118; J. Cobbe and J. Singh, 'Reviewable Automated Decision Making' (2020) 39 *Computer Law & Security Review*, 1. Algorithmic transparency is considered as a requirement of 'trustworthy' AI in ethics guidelines, soft-law instruments and (draft) legislation. See: High-Level Expert Group on Artificial Intelligence, above, n. 112; Council of Europe, above, n. 113; European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM(2021) 206 final (21 April 2021) [imposes different degrees of transparency obligations for the risk categories because it envisages only minimum transparency obligations for low-risk AI systems].

[115]'Examining the Black-Box: Tools for Assessing Algorithmic Systems' (Ada Lovelace Institute, 29 April 2020), https://www.adalovelaceinstitute.org/report/examining-the-black-box-tools-for-assessing-algorithmic-systems/.

[116]B. Goodman, 'Discrimination, Data Sanitisation and Auditing in the European Union's General Data Protection Regulation' (2016) 2(4) *European Data Protection Law Review*, 493.

impact assessment policies and practices,[117] such as a Data Protection Impact Assessment, do, however, involve algorithmic auditing but only before commissioning the algorithmic systems.[118] They may potentially be useful but may not require an ongoing assessment once the system is commissioned. In endorsing the ongoing revision of algorithmic systems based on a number of factors, the CJEU may be partially addressing what internal audits of surveillance regimes that are based on algorithmic models may comprise.[119]

The third issue relates to the endorsement of the prohibition of automated *decision-making* when assessing the compatibility of the specific automated *analysis* method with the Charter. Prohibition of *solely* automated decision-making has always found a place in EU data protection law[120] and more recently has received utmost attention as the field of artificial intelligence and machine learning has advanced.[121] Two main legal sources that impose prohibitions on solely automated decision-making are Article 22 of the General Data Protection Regulation (GDPR) and Article 11 of the Law Enforcement Directive (LED). A similar prohibition can also be found in other EU legislation, such as Article 7(6) of Directive 2016/681 (EU Passenger Name Records (PNR) Directive).[122] Each of these sources merits further consideration and has indeed attracted attention though we do not here claim to contribute to the discussions on their scope or disputed (in)effectiveness.[123]

Nevertheless, this legal context might help to disentangle the Court's reference to human intervention and its legal footing in the Charter. Except the EU PNR Directive, the GDPR and the LED provide a *qualified* prohibition against fully automated decision-making. As a matter of exception, they allow for solely automated decision-making in their respective contexts if certain conditions are fulfilled.[124] In *La Quadrature du Net and Others*, however, the Court's insistence on 'non-automatic intervention' seems to be absolute.[125] In its findings on non-automatic intervention, the CJEU endorses its dicta in Opinion 1/15, where the draft agreement actually contained an absolute prohibition on automated decision-making.[126] There is thus room for clarification as to the basis on which such absolute prohibition ('non-human intervention') is endorsed by the CJEU, considering that not all fully automated decisions would be directly incompatible with the Charter since the GDPR and the LED allow exceptions to the prohibition.[127]

[117]See, for example, P. de Hert, 'A Human Rights Perspective on Privacy and Data Protection Impact Assessments', in D. Wright and P. de Hert (eds.), *Privacy Impact Assessment* (Springer 2021), at 33–76.

[118]For the obligation to carry out a data protection impact assessment under EU data protection law, see: Art 35, GDPR. Also see Art 27, Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89, 4.5.2016 (Law Enforcement Directive, LED). On the application of a data protection impact assessment to algorithmic accountability and transparency, see M.E. Kaminski and G. Malgieri, 'Algorithmic Impact Assessments under the GDPR: Producing Multi-layered Explanations' (2021) 11(2) *International Data Privacy Law*, 125.

[119]For an example of good practices regarding safeguards against the automated decision making to meet the GDPR requirements, see Article 29 Data Protection Working Party, 'Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679' (3 October 2017), https://ec.europa.eu/newsroom/article29/redirection/document/49826.

[120]L.A. Bygrave, 'Article 22. Automated Individual Decision Making including Profiling', in C. Kuner, L.A. Bygrave and C. Docksey (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020), 522.

[121]I. Mendoza and L.A. Bygrave, 'The Right Not to Be Subject to Automated Decisions Based on Profiling' (University of Oslo Faculty of Law Research Paper No. 2017–20, 8 May 2017), https://ssrn.com/abstract=2964855 [discussing the evolution of the prohibition on fully automated decisions under EU law]; O. Lynskey, 'Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing' (2019) 15 *International Journal of Law in Context*, 162 [discussing the prohibition on fully automated decisions under EU law when those decisions are rendered in the context of predictive policing]. The proposed EU AIA Act provides a definition of AI systems in its Article 3(1) and the techniques and approaches to AI systems in Annex I.

[122]Directive 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJ L 119/132, 4.5.2016 (EU PNR Directive).

[123]Mendoza and Bygrave, above n. 121; S. Wachter, B. Mittelstadt and L. Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7(2) *International Data Privacy Law*, 91; M. Brkan 'Do Algorithms Rule the World? Algorithmic Decision-Making and Data Protection in the Framework of the GDPR and Beyond' (2019) 27 *International Journal of Law and Information Technology*, 91.

[124]Art 22(2), GDPR; Art 11(1), LED.

[125]*La Quadrature du Net and Others*, para. 182.

[126]Opinion 1/15, para. 173.

[127]Article 22(2) of the GDPR reads: '[p]aragraph 1 shall not apply if the decision: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent.' Article 13 of the LED reads as '[m]ember States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited *unless* authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller'. Emphasis added.

One assumption could be to limit the Court's findings to the facts of the case. The automated analysis in question amounted to a derogation from the principle of confidentiality of communications for national security purposes, as set out in Article 15 of the e-Privacy Directive because of the obligations imposed upon electronic communications service providers (lex specialis) and, by extension, the Charter applied. This interpretation, however, may raise an issue as to the relationship between lex specialis and lex generalis data protection law to the extent that the respective derogations constitute personal data processing.[128] In fact, the Court recognised in *La Quadrature du Net and Others* the relationship between the e-Privacy Directive and the GDPR when it considered the legality of the retention of subscriber information.[129] In particular, it referred to Article 23 of the GDPR, which allows Member States to restrict the application of obligations and individual rights based on a number of grounds, one of which is to safeguard national security, defence and public security.[130] Considering that the right not to be subjected to solely automated decision-making is one such right, fully automated decisions are, in theory and as a matter of exception, allowed by virtue of Article 23 of the GDPR, subject to the qualifications set out in that Article. Member States are limited as to the extent to which they may resort to the exceptions under Article 23, as they may only be exercised for a purpose specified in the Article, without interfering with the essence of fundamental rights and in accordance with the requirements of necessity and proportionality. In a way, the prohibition against solely automated decision-making under secondary legislation is still not an absolute prohibition as the Court portrayed it in its analysis on automated analysis of personal data in *La Quadrature du Net and Others*. Clarity in terms of the reasoning of the Court in upholding a prohibition as such is necessary to understand the implications of the ruling in automated decision systems beyond this case, as—at least in theory—the secondary legislation allows for a derogation from the prohibition, albeit it must be scrutinised in light of fundamental rights protection.

Overall, with *La Quadrature du Net and Others*, the CJEU upheld its approach in Opinion 1/15 in considering automated analysis and decision-making in light of the overall objective of safeguarding fundamental rights. The questions that have arisen from its latest finding on the topic implicate the profound importance of upholding fundamental rights protection against the use of mass surveillance practices that draw on AI-based technologies. In fact, these questions resonate with the questions raised in the preliminary ruling requests on the compatibility of the EU's own PNR system with the Charter.[131] As we wait for the CJEU's latest deliberations on these requests, the ongoing legislative debate surrounding the adoption of the proposed EU AI Act signals even further debate on the future of automated analysis, especially on the compatibility of mass surveillance practices with the EU fundamental rights framework.[132] The proposed Act prefaces the need to ensure 'consistency with the EU Charter of Fundamental Rights and the existing secondary Union legislation on data protection, consumer protection, non-discrimination and gender equality'.[133] That said, it might compound the existing patchwork of EU instruments on mass surveillance and data retention. The international agreements for law enforcement and judicial co-operation, which provide for the use of automated systems, are excluded from the scope of the proposed Act.[134] Furthermore, it does not apply to the existing legislation establishing EU databases for security and border management purposes and their

[128]On the relationship between the e-Privacy Directive and the GDPR, see EDPB, 'Opinion 5/2019 on the Interplay between the e-Privacy Directive and the GDPR, in Particular Regarding the Competence, Tasks and Powers of Data Protection Authorities' (12 March 2019), https://edpb.europa.eu/our-work-tools/our-documents/styrelsens-yttrande-art-64/opinion-52019-interplay-between-eprivacy_en.

[129]*La Quadrature du Net and Others*, para. 202.

[130]Ibid., para. 209.

[131]Case C-817/19, *Ligue des droits humains* (pending); Cases C-148/20, C-149/20 and C-150/20, *Deutsche Lufthansa* (pending).

[132]One of the prominent debates following the release of the proposed EU AI Act has been the ongoing issue on the use of facial recognition systems in EU Member States. While a number of actors called for the outright ban of these systems, the proposed Act only partly prohibits 'real-time' remote identification systems into which facial recognition may fall. See: F. Ragazzi et al., 'Biometric and Behavioural Surveillance in EU Member States', (Report for the Greens/EFA, 2021), http://extranet.greens-efa-service.eu/public/media/file/1/7297. See, for other criticisms on the EU AI Act, T. Krupiy, 'Why the Proposed Artificial Intelligence Regulation Does Not Deliver on the Promise to Protect Individuals from Harm' (*Europeanlawblog.eu*, 23 July 2021) https://europeanlawblog.eu/2021/07/23/why-the-proposed-artificial-intelligence-regulation-does-not-deliver-on-the-promise-to-protect-individuals-from-harm/; A. Circiumaru, 'Three Proposals to Strengthen the EU Artificial Intelligence Act' (Ada Lovelace Institute, 13 December 2021), https://www.adalovelaceinstitute.org/blog/three-proposals-strengthen-eu-artificial-intelligence-act/.

[133]Explanatory Memorandum, 1.2, the proposed EU AI Act.

[134]Article 2(4), the proposed EU AI Act.

interoperability, which have raised grave fundamental rights concerns.[135] In this evolving complex mosaic of legislative landscape, the crucial role of the CJEU in safeguarding fundamental rights becomes all the more profound. A key aspect of protecting rights is the oversight of law enforcement and security services' powers found in this mosaic. The following section considers the role of oversight mechanisms as it has evolved in the CJEU's case-law on data retention.

5 | 'OVERSIGHT WITH TEETH'

As set out in Section 3, generalised and indiscriminate retention of personal data is permissible only where a Member State is facing a serious threat to national security (including terrorism[136] and serious crime[137]) that proves to be genuine and present or foreseeable. This applies not only to retention of data, but also to access to real-time collection and sharing of traffic and location data, as well as automated analysis (see above). The Court held that when a Member State makes such a claim regarding a serious threat to national security, this claim must be verified by means of an effective review by a court or an independent administrative body[138] either ex post, in most cases, or a priori, when the interference is particularly grave. It is the nature of this effective review that is the subject of this section.

It is true that not all the Court's judgments on data retention have been welcomed by some state authorities, security services in particular, which have been accustomed to a fairly free hand under national rules. Because some of these services, in several Member States, do not have a history of strict external and independent control of their surveillance activities, including in the electronic world, *La Quadrature du Net and Others* helpfully sets out in substantial detail what kind of oversight and powers are necessary for lawful surveillance of electronic communications. In the Court's view, control over the way in which Member States use the exceptions to the rights to privacy and data protection is central to ensuring that the relationship of rights to exceptions remains intact and that rights clearly and substantively take priority over exceptions. It was thus incumbent on the Court to provide detailed rules on oversight mechanisms to guarantee the primacy of rights over exceptions. In other words, the Court recognised that the security services themselves could not be left responsible for determining whether their actions were compatible with EU law. An external body, an oversight mechanism, is necessary to make such judgment on whether a serious threat to national security (including terrorism and serious crime) exists and whether it is both genuine and present or foreseeable on the basis of evidence. This must include the power for the reviewing body to oblige security services to provide evidence on the basis of which they claim to justify the interference with fundamental rights. It is then for that body to make the assessment whether the justification provided is sufficiently robust and in accordance with the law to justify the actions either taken, or, where ex ante, to be taken.

In light of the centrality of the role of an oversight mechanism to ensure the lawfulness of the interference, a similarly robust definition is required. For that reason, rules on the characteristics and the powers of an oversight mechanism takes up a substantial portion of the judgment in *La Quadrature du Net and Others*. The Court provides extensive (and binding) guidance on what kind of oversight is obligatory, by what kind of body and with which

[135]Article 83(1), the proposed EU AI Act. On the compatibility of the databases with EU law, see N. Vavoula, *Immigration and Privacy in the Law of the EU: The Case of Information Systems* (Brill Nijhoff, forthcoming 2022). On this argument, see N. Vavoula, 'Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism' (2021) 23(4) *European Journal of Migration and Law*, 457.

[136]*La Quadrature du Net and Others*, para. 179, which reads: 'That being said, in order to guarantee that such a measure is actually limited to what is strictly necessary in order to protect national security and, more particularly, to prevent terrorism, in accordance with what was held in paragraph 139 of the present judgment, it is essential that the decision authorising automated analysis be subject to effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that a situation justifying that measure exists and that the conditions and safeguards that must be laid down are observed'.

[137]Ibid., para. 166, which reads: 'However, in accordance with the principle of proportionality, as mentioned in paragraph 131 above, access to data retained for the purpose of combating serious crime may, provided that the substantive and procedural conditions associated with such access referred to in the previous paragraph are observed, be justified by the objective of safeguarding national security'.

[138]This phrase has remained constant in the case-law; see *Tele2 and Watson*.

powers. It also addresses the question of a priori and ex post oversight and which applies to what decisions. Of particular importance, as discussed below, is that the Court set out how an oversight body must authorise, a priori, any decision for real-time traffic and location data retention and sharing, and ex post, at the very least, any decision allowing providers of electronic communications to carry out general and indiscriminate retention of data, traffic and location data, automated analysis and any national rules authorising automated analysis.

The term "oversight" is only loosely defined and not yet legally limited in EU law. It became a catch-all word to describe ways of controlling the activities of security services by the Church Committee in the United States (US) in the 1970s.[139] At that time, the advantage of using this term rather than judicial review, or some other more overtly legal phrase, was to achieve a compromise with the services, which were very strongly opposed to any whiff of judicial interference. Since then, however, the term has been used in increasingly diverse contexts—by some to include strict judicial review and by others to describe even whistle-blowers and non-governmental organisations (NGOs). In the European context, the 2013 Snowden revelations of US mass surveillance of electronic communications[140] led to two authoritative reports on "oversight" by the European Parliament in 2013[141] and the Commission for Human Rights of the Council of Europe in 2015.[142] Both strongly endorsed democratic oversight carried out by bodies with real and visible independence from the services themselves, and which have binding powers. The first recommendation of the Commission's report related to the independence of such bodies. These bodies must be fully independent both from the executive and the security services and hold powers to oversee all aspects of security service regulations, policies, operations and administration. To strengthen the independence of such bodies, the report recommended that a designated parliamentary committee have a role in the appointment of members and the possibility for the bodies' members to take part in parliamentary hearings. The scope of oversight is also the subject of recommendations: oversight must include all aspects and phases of the collection, processing, storage, sharing, minimisation and deletion of personal data. Equally, the oversight body must not only have powers to review the lawfulness of activities which interfere with privacy and data protection but also with the rights of freedom of expression, assembly, association and religion, thought and conscience. These recommendations are useful as a prelude to the Court's judgment.

In *La Quadrature du Net and Others*—and earlier case-law on issues related to the processing of personal data—the Court *never* uses the term "oversight". Instead, it requires an effective *review* by *a court or by an independent administrative body*. This language is close to that of the ECtHR, the decisions of which must be taken into account when determining the scope of rights that appear in both the Charter and the ECHR.[143] Section 8 considers the ECtHR's vision of oversight, but the following observations can be made in terms of the independence requirement that both courts seek. The Strasbourg Court has frequently been required to determine the characteristics necessary for an effective review. It has avoided accepting the title given by states to bodies charged with reviewing security services in favour of a functional definition based on the body's composition, powers and scope of action. Whether an entity is called a court or an independent administrative body is not determinative of its status. Instead, independence is a key requirement, which means both independence from the executive and independence from the parties.[144] It must be impartial, which denotes the absence of prejudice or bias.[145] Key to determining whether a body is independent is the manner of appointment of its members, their terms of office, the existence of guarantees against outside pressures and the question whether the body presents an appearance of independence. Lack of independence is apparent where the role or duties of the members make them vulnerable to outside pressure, where

[139]T. Young, '40 Years Ago, Church Committee Investigated Americans Spying on Americans' (*Brookings*, 4 May 2015), https://www.brookings.edu/blog/brookings-now/2015/05/06/40-years-ago-church-committee-investigated-americans-spying-on-americans/.

[140]Z. Bauman et al., 'After Snowden: Rethinking the Impact of Surveillance' (2014) 8(2) *International Political Sociology*, 121.

[141]European Parliament, 'Report on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs' (2013/2188(INI), 21 February 2014.

[142]Council of Europe—Commission for Human Rights, 'Democratic and Effective Oversight of National Security Services' (2015).

[143]Article 6, TEU.

[144]*Zand v. Austria* (1978) 15 DR 70.

[145]*Piersack v. Belgium* (1983) 5 EHRR 169.

there are insufficient legal guarantees of their independence and if they can be removed or their terms ended, or their tasks and duties changed substantially by the body which appointed them.[146] In the field of oversight of secret surveillance by security services, the ECtHR has been particularly sensitive to the gravity of the risk of serious human rights violations and required states to ensure the independence of all oversight bodies.[147]

The CJEU reviewed the requirements of independence of the court or independent administrative body in *HK*. It highlighted that where there is a requirement of a prior review (mainly in relation to traffic and location data; see below), even in cases of urgency, this must take place before the collection of the data.[148] The court or body entrusted with carrying out the review must have all the powers and provide all the guarantees necessary in order to reconcile the various interests and rights in question, which leads directly to the requirements of the status of the court or body. The CJEU differentiated between courts and independent administrative bodies, which might suggest that its confidence is greater as regards the former than the latter. As regards independent administrative bodies, they must have a status which enables them to act objectively and impartially and for this purpose must be free of any external influence.[149] The CJEU further clarified that the independence of a body carrying out a prior review means that it must be a third party in relation to the authority which is requesting access to the data. This is necessary to ensure that the review is carried out objectively and impartially and free from any external influence. In particular (as was at the centre of the facts of the case), independence entails that the authority entrusted with the prior review must not be involved in the conduct of the criminal investigation and must be neutral in regard to the parties to the proceedings. These mandatory characteristics for independence mean that administrative bodies within the hierarchy of the security services cannot qualify as permissible oversight bodies. The arm's length relationship which the CJEU requires to establish independence is not only structural but must also be effective and real in practice. The lack of independence of the body carrying out a prior review cannot be remedied by the independence of the body carrying out a subsequent review. Interestingly, the CJEU made no reference to the ECtHR case-law in its reasoning.

Considering these essential elements of independence, it is now time to examine what duties the Court assigns to the court or independent administrative body regarding decisions on national security grounds of agencies to require electronic services providers to retain, share and analyse electronic communication data. The Court is very clear about what it requires from this court or body: it is an effective examination of whether the state is actually facing a serious threat to national security that proves to be genuine and present or foreseeable. It is for the court or body to require evidence from the security services that there is such a threat. Thus, the burden of proof is on the services. The first element is whether the threat is serious: this requires the services to prove that this is not marginal or insignificant. There is no indication of what the standard of proof should be, but it must at least be that of administrative or civil law, a balance of probabilities. The judgment indicates that the gravity of the threat must be determined in relation to the seriousness of the interference with fundamental rights which the services request (proportionality and necessity).[150] This implies a sliding scale: the more serious the (validated) threat, the wider the

[146] *Luka v. Romania*, [2000] ECHR 192.

[147] See *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, [2012] BHRC 193. Its para. 98 reads: 'The Court has indicated, when reviewing legislation governing secret surveillance in the light of Article 8, that in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge [...]. However, [...] the Court was prepared to accept as adequate the independent supervision available. In *Klass and Others*, this included a practice of seeking prior consent to surveillance measures of the G-10 Commission, an independent body chaired by a president who was qualified to hold judicial office and which moreover had the power to order the immediate termination of the measures in question [...]. In *Kennedy v. UK* [...] the Court was impressed by the interplay between the Investigatory Powers Tribunal ("IPT"), an independent body composed of persons who held or had held high judicial office and experienced lawyers which had the power, among other things, to quash interception orders, and the Interception of Communications Commissioner, likewise a functionary who held or had held high judicial office [...] and who had access to all interception warrants and applications for interception warrants [...]'.

[148] *HK v. Prokuratuur*, para. 51.

[149] Ibid., para. 53.

[150] *La Quadrature du Net and Others*, para. 121, which reads: 'Indeed, as can be seen from Article 52(1) of the Charter, that provision allows limitations to be placed on the exercise of those rights, provided that those limitations are provided for by law, that they respect the essence of those rights and that, in compliance with the principle of proportionality, they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others'.

justification for a fundamental rights interference and vice-versa. The threat must be to national security (which includes terrorism and serious crime) which means that the term must be defined in law and justiciable. Most importantly, the threat must be genuine and present or foreseeable. As far as genuine is concerned, this means the threat must not be vague or illusory. There must be real elements, which the security services can show to the court or body to convince it of the reality of the threat. As regards present or foreseeable, this is less easily determined. On the one hand, a present threat has an immediate temporality, the threat must be in the here-and-now—something that could happen in current time. The word foreseeable is less clearly definable as something in the future can be foreseeable but not necessarily imminent. The field in which this word has been subject to the most discussion and judicial consideration is climate change. It may be foreseeable but is it imminent?[151] It will be for the court or independent administrative body to determine the parameters of foreseeability, but always with the option of referring the question to the Court if it is in doubt as to what the correct meaning should be.

Most importantly, the court or independent administrative body must determine whether there is a sufficiently important threat to justify the surveillance measures sought or implemented. Its job is not to check whether the request for a decision or the determination of an appeal against a decision of surveillance is in accordance with national law, which is a simple legality test. It must have the power to order the provision of evidence on the reality and nature of the threat itself and the impact on fundamental rights. This means the court or body needs substantive powers to investigate the nature of the threat, not simply legal verification powers to check that the procedures by which the security services' decision was made are in accordance with national law.

Throughout the judgment, there are six main categories of decisions of security services which must be subject to the court or independent administrative body's jurisdiction. These are:

i. a decision that requires an information society service provider to transmit all user data (para. 52);
ii. a decision giving an instruction to providers of electronic communication services to carry out general and indiscriminate retention of data (para. 139);
iii. decisions on national security grounds requiring services to retain (and share) general and indiscriminate traffic and location data (para. 168);
iv. decisions authorising automated analysis (para. 179);
v. the sharing of real-time traffic and location data (para. 189); and
vi. national rules which authorise automated analysis (para. 192).

Two types of decisions must be subject to an a priori review by a court or independent administrative body. The first is access to real-time traffic and location data. Here the court or body must ensure that this data is limited to that of persons with a link to terrorism on the basis of objective and non-discriminatory criteria (though see the discussion in Section 4 above). This means the court must examine the strength of evidence that the targeted person(s) in fact has a link with terrorism sufficiently evidenced by the security services to justify the measure. Further, this real-time collection must be authorised only within the limits of what is strictly necessary to counter the threat which has been established as genuine and present or foreseeable. Secondly, the use of automated analysis, both decisions and rules, must be subject to an a priori review by the court or body. This review must verify whether this analysis is justified in light of the situation, in particular the national security threat, and whether it is strictly necessary. Finally, all decisions of the court or body must be binding on the national authorities. They are not advisory.

From the existing studies on oversight of national security services across the Member States, in particular the report of the EU Agency for Fundamental Rights of 2015 which maps the existing powers and characteristics of Member States' services,[152] few ostensibly comply with the Court's standards set out in *La Quadrature du Net and*

[151]A. Anderson, M. Foster, H. Lambert and J. McAdam, 'A Well-Founded Fear of Being Persecuted … But When? (2020) 42 *Sydney Law Review*, 155.
[152]EU Agency for Fundamental Rights (FRA), 'Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU: Mapping Member States' Legal Frameworks' (6 November 2015), https://fra.europa.eu/en/publication/2015/surveillance-intelligence-services-volume-i-member-states-legal-frameworks.

Others. For instance, ten Member States do not have judicial oversight for approval of targeted surveillance measures and two have no oversight at all.[153] Clearly, a number of Member States will need to update their national law to take into account the Court's judgments. They will need to review their national legislation with a view to ensuring firstly, that their courts or independent administrative bodies are indeed sufficiently independent to fulfil the Court's strictures; secondly, that the scope of review which these courts or bodies are charged to carry out is consistent with the task that the Court has assigned them—the assessment of the seriousness of the threat; thirdly, that they have the necessary powers as determined by the Court to carry out their tasks; and fourthly, that national law is clear where there must be an a priori determination by the court or body of a surveillance measure and where an ex post review is sufficient.

6 | THE RECEPTION OF THE CJEU RULINGS IN EU MEMBER STATES: THE FRENCH CONSEIL D'ÉTAT AND THE BELGIAN CONSTITUTIONAL COURT LITIGATION

Indicative of state concerns over the fundamental rights limitations imposed by the Court of Justice on generalised surveillance has been the recent litigation before the French Conseil d'État[154] and the Belgian Constitutional Court.[155] Interestingly, each court headed down different paths on the CJEU's observations in *La Quadrature du Net and Others*. While the latter annulled the incompatible provisions of the Belgian legislation on data retention, the former followed a calculated approach in upholding the French data retention scheme.

Before the French Conseil d'État, the French Government argued against the applicability of the CJEU rulings, particularly *La Quadrature du Net and Others*, at national level, by playing the constitutional identity card: arguing that security considerations are integral to the French constitutional identity which trumps the applicability of EU law. The French Government argued in the proceedings that this securitised approach is linked with the constitutional objectives of safeguarding the fundamental interests of the nation, the prevention of attacks on public order, investigating individuals committing criminal offences and the fight against terrorism, which must be reconciled with constitutionally enshrined liberties.[156] The French Government treated these security objectives as matters falling within the national identity clause in Article 4(2) of the TEU, as functions remaining within the exclusive or main responsibility of Member States—and which thus do not benefit, as a matter of EU law, from a protection which is equivalent to that guaranteed by the French Constitution.[157]

This intervention is significant and unprecedented in EU law, as it is the first time that arguments related to national constitutional identity are not linked with the protection of fundamental rights (which are deemed to require protection from the uncritical reach of EU law),[158] but rather with the protection of national security (to which EU law-led fundamental rights protection poses an obstacle).[159] The French Government has in essence argued that the prioritisation of security considerations reflects national constitutional identity and must prevail over EU law and any fundamental rights safeguards the EU legal order has developed in the field.

[153]Ibid., 52.

[154]Conseil d'État, Judgment of 21 April 2021, Decision no. 393099.

[155]Belgian constitutional court, decision no. 57/2021, 22 April 2021, https://www.const-court.be/public/f/2021/2021-057f-info.pdf.

[156]Ibid., para. 9.

[157]Ibid., para. 10.

[158]In the field of European criminal law, see in this context the judgment of the BVerG on the European Arrest Warrant. BVerfG, Order of the Second Senate of 15 December 2015–2 BvR 2735/14. For a commentary, see F. Meyer, '"From Solange II to Forever I": The German Federal Constitutional Court and the European Arrest Warrant (and how the CJEU responded)" (2016) 7 *New Journal of European Criminal Law*, 283. For an analysis of fundamental rights concerns as triggering constitutional identity and mutual trust concerns, see V. Mitsilegas, 'Judicial Dialogue, Legal Pluralism and Mutual Trust in Europe's Area of Criminal Justice', *European Law Review*, forthcoming.

[159]The approach by the Conseil d'État has been characterised as a 'Securitarian Solange'. See S. Vallée and G. Genevoix, 'A Securitarian Solange. France has launched a cluster bomb on the EU's legal and political order' (*Verfassungsblog*, 25 April 2021), https://verfassungsblog.de/a-securitarian-solange/.

In its response, the Conseil d'État attempted to accommodate to the extent possible the arguments of the French Government regarding the prioritisation of security considerations and their importance within the internal constitutional order, while at the same time seeking to avoid a direct clash with EU law and the CJEU. The Conseil d'État did not engage in interpreting Article 4(2) of the TEU as per the French Government's argumentation. In so doing, it avoided falling into the "*Weiss* trap".[160] However, it did rule that in the event that the application of a European Directive or Regulation, as interpreted by the CJEU, would have the effect of depriving of effective guarantees one of the constitutional requirements in question, which will not benefit, in Union law, from equivalent protection, the administrative judge must set it aside to the strict extent that respect for the Constitution so requires.[161] The Conseil d'État accepted the link between national data retention mechanisms and the protection of national security,[162] but did not declare EU law invalid or inapplicable. Rather, it attempted to set the parameters and limits of the national data retention schemes by a security-driven interpretation of the case-law of the CJEU.

The Conseil d'État applied the case-law of the CJEU, in particular the ruling in *La Quadrature du Net and Others*, to find that the generalised retention of certain categories of what is considered as less sensitive data, such as civil status, IP address, accounts and payments data, is permitted.[163] Generalised retention of traffic and location data for national security purposes is also justified, but the Government has a duty to assess the existence of a grave, real and actual or predictable threat to national security periodically.[164] On the other hand, generalised retention of traffic and location data for purposes other than those of national security, in particular the prosecution of criminal offences and the protection of public order, is unlawful.[165] The Conseil d'État further emphasised the need for ex ante independent review of the use of retained data for intelligence purposes, and found the French system wanting in view of the non-binding character of the opinion of the National Commission for the Control of Intelligence Techniques (CNCTR), which must be given prior to any authorisation for such use.[166]

In this way, the Conseil d'État avoided a direct clash with the CJEU and at the same time used the case-law of the CJEU to interpret broadly the powers of the executive to retain personal data in a generalised manner and thus to back up the French Government's security agenda. Generalised data retention for national security purposes *as such* is expressly justified and limits the overreach of the executive centre mainly around procedural safeguards regarding automated processing,[167] real-time access[168] and the existence of independent and legally binding ex ante authorisation regarding real-time access to data[169] and subsequent use. The case-law of the CJEU has thus been translated, by the Conseil d'État, as providing little resistance to the system of domestic generalised surveillance on the basis of data retention for national security purposes, with the exception of the introduction of a number of specific procedural safeguards.

The Belgian Constitutional Court, on the other hand, adopted the CJEU's reasoning in *La Quadrature du Net and Others* in quashing the Belgian legislation on data retention. The Court did not hesitate to note that the relevant legislation allowed for a generalised and undifferentiated obligation for telecommunications providers to store personal data of their customers for broader objectives than the fight against serious crime and the protection of public security.[170] According to the Court, the CJEU's decision in *La Quadrature du Net and Others* required a change in the perspective of the national legislator: the obligation to retain personal data must be the exception, not the rule.[171] It

[160]For a more EU-friendly analysis of the judgment, see J. Ziller, 'The Conseil d'Etat Refuses to Follow the Pied Piper of Karlsruhe' (*Verfassungsblog*, 24 April 2021), https://verfassungsblog.de/the-conseil-detat-refuses-to-follow-the-pied-piper-of-karlsruhe/.
[161]Conseil d'État, Decision no. 393099, para. 5.
[162]Ibid., paras. 21–26.
[163]Ibid., paras. 35–36.
[164]Ibid., paras. 43–46.
[165]Ibid., paras. 48 *et seq*.
[166]Ibid., para. 74. The Conseil d'État referred expressly to the CJEU rulings in *Tele2 and Watson* and *HK*. See para. 68.
[167]Ibid., para. 77.
[168]Ibid., para. 78.
[169]Ibid., para. 80.
[170]Belgian constitutional court, decision no. 57/2021, point B.17.
[171]Ibid., point B.18.

also called on the national legislator to draw up legislation that follows the CJEU case-law and meets the Charter requirements.[172]

As more preliminary requests on the subject are in the pipeline,[173] intense discussions on the compatibility of data retention practices with EU law ensue. The different interpretations by national courts point to the crucial role of the CJEU in avoiding a fragmented fundamental rights protection. At the same time, the Conseil d'État litigation is the tip of the iceberg in unravelling the contestation over the CJEU's rulings on mass surveillance regimes. In the next section, we will explore the other episode of contestation that takes place at the legislative level.

7 | BYPASSING THE CJEU IN THE NEGOTIATIONS OF THE E-PRIVACY REGULATION?

The pronouncements of the CJEU are central also in relation to the negotiations for the adoption of an e-Privacy Regulation,[174] which will replace Directive 2002/58/EC on privacy and electronic communications. The Commission proposal left this matter outside its scope, so that Member States would be free to keep or create national data retention laws, provided that they are "targeted" and that they comply with the case-law of the CJEU and its interpretation of the e-Privacy Directive and the Charter. In particular, Article 11 of the proposal, which broadly corresponds to Article 15 of the e-Privacy Directive, enables the EU and Member States to restrict by way of a legislative measure the scope of the obligations and rights provided for in the proposal where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23(1)(a)–(e) of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests.

Member States have been dissatisfied with this approach. They considered that the proposed rules are stricter than those laid down in Directive 2002/58/EU, thus potentially further limiting the possibilities of retaining data for law enforcement purposes in criminal proceedings.[175] In a non-paper issued on 14 February 2019, eight delegations to the Council proposed that the e-Privacy Regulation should allow for 'the possibility for existing and future data retention regimes'.[176] A new Article 7(2a) was proposed to be added to the draft e-Privacy Regulation, which would provide that:

> Union or national law may impose an obligation on the providers of the electronic communication services to retain metadata for a longer period of time, where such an obligation respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard the prevention, investigation, detection or prosecution of criminal offences.[177]

Further concerns have been raised by a number of digital rights groups led by EDRi, challenging the exception for national security and public order in Article 2(2)(a) of the proposal, according to which the Regulation would not

[172]Ibid., point B.19.

[173]C-140/20, *G.D. v. The Commissioner of the Garda Síochána, Minister for Communications, Energy and Natural Resources* (pending); Joined Cases C-339/20 and C-397/20, *VD* (C-339/20) and *SR* (C-397/20) (pending).

[174]Commission, 'Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' COM(2017) 10 final.

[175]Council, Document 6358/19 (14 February 2019) 2. For an analysis, see X. Tracol, 'The Two Judgments of the European Court of Justice in the Four Cases of *Privacy International*, *La Quadrature du Net and Others*, *French Data Network and Others* and *Ordre des Barreaux francophones et germanophone and Others*: The Grand Chamber is Trying Hard to Square the Circle of Data Retention' (2021) *Computer Law & Security Review*, 1, 12.

[176]Council, Document 6358/19, above, n. 175, 2.

[177]Ibid., 5.

apply to 'activities which fall outside the scope of Union law, and in any event *to processing operations* concerning national security *and defence, regardless of the person carrying out those operations*'.[178] That provision aimed at bypassing the case-law of the CJEU on data retention, and digital rights groups thus requested the telecoms working party of the Council to reject it.[179] Nevertheless, in the Council mandate for negotiations with the European Parliament, processing for national security and defence purposes is excluded from the scope of the proposed Regulation 'regardless of who is carrying out those activities whether it is a public authority or a private operator acting at the request of a public authority'.[180] Furthermore, Recital 26 states that:

> this Regulation should not affect the ability of Member States to carry out lawful interception of electronic communications, including by requiring providers to enable and assist competent authorities in carrying out lawful interceptions, or take other measures, such as legislative measures providing for the retention of data for a limited period of time, if necessary and proportionate to safeguard the public interests mentioned above, in accordance with the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the European Union and of the European Court of Human Rights.[181]

In addition, Article 7(4) provides that:

> Union or Member State law may provide that the electronic communications metadata is retained, including under any retention measure that respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society, in order to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the safeguarding against and the prevention of threats to public security, for a limited period. The duration of the retention may be extended if threats to public security of the Union or of a Member State persists.[182]

This provision reflects the aforementioned non-paper as well as the wishes of the French delegation expressed in a working document of 12 January 2021, but reference to the need for targeted retention schemes in line with the analysis in the previous section is completely missing.[183] Essentially, the negotiations within the Council have been a battlefield between, on the one hand, efforts to enhance privacy safeguards and, on the other, attempts to enable mass surveillance and transform the e-Privacy Regulation into a 'surveillance toolkit' with Article 7(4) essentially signifying that the latter side 'got its way'.[184] However, it is imperative that the e-Privacy reform is not used to legalise data retention regimes and overall water down the pronouncements of the CJEU in its line of case-law. Echoing the aforementioned concerns, on 9 March 2021, the European Data Protection Board (EDPB) issued statement 03/2021 on the e-Privacy Regulation.[185] The EDPB reiterated the need that legislative measures requiring providers of electronic communications services to retain electronic communication data comply with the ECHR and the Charter, and the relevant CJEU case-law, 'which notably provides that Articles 7, 8, 11 and 52(1) of the Charter must be interpreted as precluding legislative measures, which would provide, as a preventive measure, the general

[178]Council, Document 5008/21 (5 January 2021) 58.
[179]'Strengthening Privacy and Confidentiality of Communications' (*EDRi*, 25 January 2021), https://www.euractiv.com/wp-content/uploads/sites/2/2021/01/20210125-ePrivacy-letter-EDRi.pdf.
[180]Council, Document 6087/21 (10 February 2021) 42.
[181]Ibid., 31.
[182]Ibid., 59.
[183]Council, WK 390/2021.
[184]'France "Got its Way" as Portugal Ends e-Privacy Seadlock' (*eurobserver*, 12 February 2021), https://euobserver.com/science/150904.
[185]EDPB, 'Statement 03/2021 on the e-Privacy Regulation' (9 March 2021), https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-032021-eprivacy-regulation_en.

and indiscriminate retention of traffic and location data'.[186] Importantly, the EDPB expressed concerns about retention of electronic communication data for the purposes of law enforcement and safeguarding national security stressing that:

> providing a legal basis for anything else than targeted retention [...] is not allowed under the Charter, and would anyhow need to be subject to strict temporal and material limitations as well as review by a Court or by an independent authority.[187]

As the trialogues with the European Parliament are underway, it remains to be seen how this issue can be resolved so that the pronouncements of the CJEU do not become dead letter in lieu of retaining national mass surveillance regimes. There is, however, another set of requirements for the legal limitations of large-scale surveillance measures that can be derived from Member States' obligations under the ECHR. It is thus important to turn our attention to the ECHR protections as interpreted by the ECtHR in its case-law and the dialogue between the CJEU and the ECtHR on the topic.

8 | LIMITATIONS TO SURVEILLANCE UNDER THE ECHR: AN EVERLASTING TANGO BETWEEN THE ECTHR AND THE CJEU

With its case-law going back almost four decades, the ECtHR is no stranger to the legal challenges against states' surveillance powers. When the CJEU released its *Digital Rights Ireland* decision, the question on the cross-fertilisation between the CJEU and the ECtHR arose. The *Big Brother Watch* and *Centrum för Rättvisa* decisions delivered by the Grand Chamber (GC) of the ECtHR has piqued the interest in that cross-fertilisation or fragmentation—if there is one—to determine the legal limitations of security and intelligence services in conducting surveillance operations under the Charter and the ECHR. The decisions are rich in possible discussions on the future of mass surveillance and there has been a mixture of initial reactions.[188] This section considers the latest ECHR developments on surveillance in light of three main points: (a) the future of data retention under the ECHR; (b) the permissibility of automated analysis of personal data; and (c) the ECHR-compliant oversight system.

8.1 | Acquisition of related communications data: A dual system for rules governing access to data?

The first time that the ECtHR was asked to determine the permissibility of public authorities' access to communications data dates to 1984. In *Malone*,[189] concerning the practice of the British Post Office to hand over the automatic recording of the applicant's metering information, which showed the dialled numbers and the duration of the calls, the Court noted that this practice amounted to an Article 8 interference along with the interception itself.[190] Since

[186]Ibid., 1–2.
[187]Ibid., 2.
[188]M. Milanovic, 'The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in *Big Brother Watch* and *Centrum för Rättvisa*' (*EJIL: Talk!*, 26 May 2021), https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/; L. Ni Loideain, 'Not So Grand: The Big Brother Watch ECtHR Grand Chamber judgment' (*infolawcentre*, 28 May 2021), https://infolawcentre.blogs.sas.ac.uk/2021/05/28/not-so-grand-the-big-brother-watch-ecthr-grand-chamber-judgment/; M. Klamberg, 'Big Brother's Little, More Dangerous Brother: *Centrum för Rättvisa*' (*Verfassungsblog*, 1 June 2021), https://verfassungsblog.de/raettvisa; M. Zalnieriute, 'Procedural Fetishism and Mass Surveillance under the ECHR: *Big Brother Watch v UK*' (*Verfassungsblog*, 2 June 2021), https://verfassungsblog.de/big-b-v-uk/.
[189]*Malone v. UK* (1985) 7 EHRR 14. Note here that, although the 1974 *Klass* decision was the ECtHR's first decision on communications interception, the Court's analysis on the permissibility of the challenged operation focused on the system of oversight. For an early analysis of the evolving case-law of the ECtHR on the interception of communications in connection with national security interest on one hand, and in connection with ordinary criminal investigations, see S. Sottiaux, *Terrorism and Limitation of Rights: The ECHR and the US Constitution* (Hart, 2008).
[190]*Malone v. UK*, para. 84.

then, the Court has started to weave the legal requirements for permissible interception of communications and information collection in connection with national security interests into its case-law. Notably, in connection with the latter form of surveillance, the ECtHR has affirmed that the collection of the information and its subsequent use by authorities amounted to separate Article 8 interferences.[191] It has taken a similar approach for the former form of surveillance, particularly in *Weber and Saravia*, where it held that 'transmission of data and its use by authorities … constitutes a further separate interference with the applicants' rights under Article 8'.[192]

In *Digital Rights Ireland*, the CJEU relied on the ECtHR's pronouncements in finding that obliging communications service providers to retain communications data of their users and provide subsequent access to that data to public authorities constituted separate interferences with the Charter rights (namely the right to privacy enshrined in Article 7).[193] It thus has started to lay down the requirements to justify the interference stemming from public authorities accessing the data, limiting the purpose of access to preventing or detecting serious crime.[194] The ECtHR responded with references to the CJEU case-law, for example in *Zakharov*, where, among others, it considered the permissibility of Russian law allowing for a direct access to communications data, without any prior authorisation, in light of the existing oversight system.[195] This was followed with references in *Szabó*, where the Court found an Article 8 violation against an EU Member State's law on interception of communication.[196] It criticised the lack of a priori involvement of an independent authorising body and an individual suspicion to target individuals whose communications might be intercepted.[197] This came as a relief for some commentators who noted that the ECtHR and the CJEU were showing signs of following similar approaches, which meant that there would not be two dissimilar requirements that intelligence and security services of EU Member States have to follow.[198]

The journey of this judicial exchange between the ECtHR and the CJEU took a different turn following *Big Brother Watch* and *Centrum för Rättvisa*.[199] Both cases involved legal challenges against bulk interception of communications in the UK and Sweden, respectively. *Big Brother Watch* also involved a challenge against the UK law data retention scheme—which since has undergone change[200]—that assigned certain UK security and intelligence service authorities the power to request communications data from communication service providers, albeit in a targeted manner.[201] On the question of the power of public authorities to access communications data, there was no denying that the Chamber followed the CJEU's approach. Based on the references to the CJEU's findings in *Digital Rights Ireland* and *Tele2 and Watson* on access to the retained communications data, as well as the following UK High Court decision on the incompatibility of a data retention regime with EU law,[202] the Chamber found an Article 8 violation with ease. Two—very brief—pronouncements for the Chamber's decisions were: first, public authorities' access to the data was not limited to the purpose of combating serious crime, and second, the access regime was not subject to a priori independent review.[203] When the applicants appealed the Chamber's decision, they did not make further

[191] *Leander v. Sweden* (1987) 9 EHRR 433, para. 48; *Amann v. Switzerland* (2000) 30 EHRR 843, para. 69; *Rotaru v. Romania* (2000) 8 BHRC 43, para. 46.
[192] *Weber and Saravia v. Germany* (2008) 46 EHRR SE5, para. 79.
[193] *Digital Rights Ireland*, para. 35.
[194] Ibid., para. 61; *Tele2 and Watson*, paras. 118–119.
[195] *Roman Zakharov v. Russia*, paras. 270–271.
[196] *Szabó and Vissy v. Hungary (2016) 63 EHRR 3*.
[197] Ibid., para. 71. However, on the point of contention that the ECtHR departed from *Zakharov*, see: *Szabó and Vissy v. Hungary* (Pinto de Albuquerque J concurring), point 20.
[198] M.D. Cole and A. Vandendriessche, 'From Digital Rights Ireland and Schrems in Luxembourg to Zakharov and Szabo/Vissy in Strasbourg' (2016) 2 (1) *European Data Protection Law Review*, 121; F. Böhm, 'Assessing the New Instruments in EU–US Data Protection Law for Law Enforcement and Surveillance Purposes', (2016) 2 *European Data Protection Law Review*, 178.
[199] *Big Brother Watch and others v. UK*, Appl Nos. 58,170/13, 62,322/14 and 24,960/15 (25.05.2021); *Centrum för Rättvisa v. Sweden*, Appl No. 35252/08 (25.05.2021).
[200] UK law on interception communications and data acquisition has been changed by the Investigatory Powers Act (IPA) 2016. See S. McKay, *Blackstone's Guide to the Investigatory Powers Act 2016* (Oxford University Press, 2017).
[201] For a brief description of the law, see I. Walden, 'United Kingdom', in U. Sieber and N. von zur Mühlen (eds.), *Access to Telecommunication Data in Criminal Justice: A Comparative Analysis of European Legal Orders* (MPIS, 2016), 705.
[202] *Liberty v. Secretary of State for the Home Department and Others* [2018] 3 WLR 1435. For critical analysis of this decision, see M. White, 'Is the Incompatibility of UK Data Retention Law with EU Law Really a Victory?' (2021) 41(1) *Legal Studies*, 130.
[203] *Big Brother Watch and Others v. UK*, para. 467.

submissions on its finding on the data acquisition by UK security and intelligence services. Nor did the Government contest that finding, which led the Grand Chamber to uphold the Chamber's decision.[204]

On initial observation, the Grand Chamber in *Big Brother Watch* seems to accept the CJEU's findings unquestioningly, which may indicate a consensus or at least an absence of disagreement on the issue. A comprehensive reading of the Grand Chamber's findings together with *Centrum för Rättvisa* might sway some to concerns that the ECtHR may be sidestepping what commentators believe to be the high standards of the CJEU.[205] As mentioned below on the system of oversight, the Grand Chamber considered the whole process of the untargeted interception regime of the UK, from the initial interception of communications to the retention of the intercepted communication and the related data and to the access by an analyst.[206] The operation thus involved varying scales of Article 8 interferences as it progressed.[207] Ni Loideain observed that in this way the Grand Chamber departed from its established case-law, where, as mentioned at the beginning of this section, access to the data constituted a separate and further Article 8 interference.[208] What is interesting here, in terms of data retention schemes, is the Grand Chamber's findings on the applicant's claim in *Big Brother Watch* that the UK law breached Article 8 ECHR by applying more lenient safeguards to the communications data captured during the interception than to the content of the intercepted communications.

Those communications data are called 'related communications data', which is, as its name suggests, communications data associated with those communications acquired by means of interception.[209] In *Centrum för Rättvisa*, the Grand Chamber noted that Swedish law did not differentiate between the contents of the interception and its related communications data once they were obtained because the same procedures and safeguards applied to both intercepted materials.[210] This includes a priori authorisation by the Foreign Intelligence Court, whose independence the GC was satisfied with.[211] The UK law, however, treated both the communications data and its content once they are obtained. The main point of contention was the fact that, while the contents of communications related to a person known to be in the British Isles could not be selected for examination, its communications data could be selected and was not destroyed immediately.[212] This would mean that access to communications data was not certified by the Secretary of State, although the analysts had to complete a record why it was necessary and proportionate to access the data.[213] The UK Government argued for a differential treatment between the content of communications and its data based on the temporal value of the latter, which a priori certification would hamper, and the lengthy analytic work required to decipher it.[214]

At the outset, the Grand Chamber refuted the claim that the collection of communications data occasioned by the bulk interception was less intrusive than the collection of the actual content.[215] However, once obtained, the Grand Chamber confirmed that they could be treated differently since they may have different uses for intelligence services.[216] The Grand Chamber was satisfied with the UK Government's argument and held that 'the storage provisions concerning related communications data were sufficiently robust, even though they differed in substance from the provisions relating to content.'[217] It was only unhappy with the secretive nature of the retention period for the

[204]Ibid., paras. 517–522.
[205]Ni Loideain, above, n. 188.
[206]Section 8.3.
[207]*Big Brother Watch and Others v. UK*, para. 325. *Centrum för Rättvisa v. Sweden*, paras. 239–245.
[208]Ni Loideain, above, n. 188.
[209]G. Smith, 'Big Brother Watch v UK—implications for the Investigatory Powers Act?' (*cyberleagle.com*, 13 September 2018), https://www.cyberleagle.com/2018/09/big-brother-watch-v-uk-implications-for.html. A concept of 'relevant communications data' appears in the IPA 2016, which comprises different categories of data including internet connection records and (to use the UK terminology) entity data, which could be simplified as subscriber information. See G. Smith, 'Never mind Internet Connection Records, what about Relevant Communications Data?' (*cyberleagle.com*, 29 November 2015), https://www.cyberleagle.com/2015/11/never-mind-internet-connection-records.html.
[210]*Centrum för Rättvisa v. Sweden*, para. 283.
[211]Ibid., paras. 295–296.
[212]Ibid., para. 419.
[213]Ibid., para. 420.
[214]Ibid., paras. 420 and 422.
[215]*Big Brother Watch and others v. UK*, para. 363.
[216]Ibid., para. 364.
[217]Ibid., para. 423.

intercepted communications data, which was unearthed during the proceedings.[218] Notably, the analysts wishing to access the communications data have to complete an auditable form explaining how the requested access was necessary and proportionate.[219] The Grand Chamber spoke approvingly of the internal authorisation procedure to access communications data, although access to the content of communications would require a certification by the Secretary of State.[220] The Grand Chamber reasoned here that the requirements that it put forward in terms of the initial bulk interception, that is a priori authorisation and designation of categories of selectors, would accommodate for excluding communications data from safeguards applicable to content of communications once they are obtained.[221] Arguably, this was because the Grand Chamber did not specify if the further access and use of the data constitute a separate Article 8 interference, according to which the Grand Chamber would have to determine its permissibility independently of the initial interception. In this way, access to communications data obtained through the bulk interception regime is not subject to a priori authorisation, and the question may remain whether the Grand Chamber's finding here is on par with the minimum safeguards that the CJEU observed for access to data. Surely, the CJEU did not consider those safeguards necessarily in connection with communications data obtained through interception of external communications, but there are compelling arguments not to treat internal and external communications separately, which unfortunately were not accepted by the Grand Chamber.[222]

8.2 | Automated analysis on the horizon

Up until its *Big Brother Watch* and *Centrum för Rättvisa* decisions, the general trend of the ECtHR in responding to states' use of new surveillance technologies has been relatively progressive.[223] In its highly popular dicta, the ECtHR has repeatedly mentioned that 'the need for […] safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned'.[224] The Grand Chamber's deliberations in *Big Brother Watch* and *Centrum för Rättvisa*, however, are rather polarising in terms of showing the ECtHR readiness in addressing concerns over surveillance regimes that operate using an automated selection process to "assign" risks to individuals to profile.

On the one hand, the breakdown of the process of bulk interception regimes challenged in both decisions is a step in the right direction against the claims that the Article 8 interference occasioning from it only occurs at the stage of the selection process, which is argued to limit the initial interference of bulk interception of communications.[225] Crucially, in its admissibility decision on *Weber and Saravia*, the ECtHR considered strategic monitoring, whereby information was collected by intercepting telecommunications indiscriminately in order to avert serious dangers, or commission of international terrorist attacks in Germany.[226] This surveillance method, which did not require targeted individualised suspicion, was found to adhere to the requirements of proportionality as required under Article 8 ECHR on the basis that the intercepted communications were filtered in the later stage by using "keywords" that were capable of triggering an investigation into the dangers for which interception initially was implemented.[227] This meant that the legislation contained 'adequate safeguards against the arbitrary use' as it defined the categories of people who may be subjected to the strategic monitoring.[228] Based on the evolution of the ECtHR's case-law up until *Weber*, Murphy expressed caution on how an emphasis on selective operations may shift

[218]Ibid.
[219]Ibid., para. 418.
[220]Ibid., para. 421.
[221]Ibid.
[222]Milanovic, above, n. 188.
[223]N. Ni Loideain, 'The Approach of the European Court of Human Rights to the Interception of Communications' (13 November 2020), https://ssrn.com/abstract=3699386.
[224]*S and Marper v. UK* (2008) 48 EHRR 50, para. 103.
[225]*Big Brother Watch and Others v. UK*, para. 288.
[226]*Weber and Saravia v. Germany*, para. 4.
[227]Ibid., para. 32.
[228]Ibid., para. 97.

the focus from the expansive privacy intrusion caused by the indiscriminate retention to compensating for that intrusion with an automated selective process.[229] Thus, in recognising the interception of communications and communications data associated with it as the first stage of Article 8 interference and seeking a priori independent authorisation for it, the GC seems to deflate the rhetoric that the initial collection of communications and data only raises an Article 8 issue if it is later accessed or used.

On the other hand, as the automated analysis becomes more complex by incorporating sophisticated artificial intelligence (AI) based tools with the ability to self-adapt without human input, it may become harder to scrutinise the Article 8 interference occasioned by those tools using the analogy of automated filtering of the data using technical combinations of letters and numbers.[230] Undeniably, the oversight system as a safeguard to restrain surveillance powers of intelligence and security agencies imposes an ex post accountability.[231] Thus, the references in *La Quadrature du Net and Others*—in terms of reviewing algorithms to ensure they are non-discriminatory, up-to-date and limited to what is necessary to achieve the protection of national security interests—may be weaved into the supervision of the system that the ECtHR requires.[232] Notably, in addressing whether intelligence analysts request to access the intercepted material by selectors is subject to an oversight system, the GC considered whether there were internal audits.[233] Still, even if a system of oversight is accepted, subject to the considerations on its independence as well as technical and legal expertise, the question on the intrusiveness of the AI-based automated decision-making tools at the stage of their creation remains.[234]

A key point of contention here is that the complex algorithmic analysis to deduce otherwise unrecognisable patterns rests on the collection of very large databases because it is through the interrogation of the accumulated data from different sources that those patterns are deduced.[235] The profiling of air passenger travellers[236] and the use of facial recognition systems in public spaces[237] are examples of those practices, along with the bulk collection of intercepted communications and data associated with it.[238] Commentators thus called upon the ECtHR to conduct a more rigorous scrutiny of the unequivocally indiscriminate surveillance measures that incorporate AI tools.[239]

The two much anticipated decisions on bulk interception of communications might have revealed the ECtHR's self-restraint on the topic, to the dismay of its judges. While recognising the technological changes experienced in the last decade and the digitalisation of everyday life, the Grand Chamber chose not to revisit its case-law to require a pre-existing suspicion to conduct surveillance by deferring to the "preventive" nature of bulk surveillance operations, which would by nature rest on the absence of such suspicion.[240] Instead, as mentioned below, it attributed significant weight to the oversight of the system, which seems to be a compensation for its initial reaction to legitimise preventive mass surveillance. Moreover, the deferral to state discretion to determine what is necessary to achieve the objective of protecting national security interests may raise the question whether an update to the strict (er) scrutiny of mass surveillance occasioned by sophisticated algorithmic tools will ever be on the horizon.

[229] M.H. Murphy, 'Algorithmic Surveillance: The Collection Conundrum' (2017) 31(2) *International Review of Law, Computers & Technology*, 225.
[230] Ibid., 230.
[231] L. McGregor, D. Murray and V. Ng, 'International Human Rights as a Framework for Algorithmic Accountability' (2019) 68(2) *International Comparative Law Quarterly*, 309 [the authors use International Human Rights as a framework to develop substantive and procedural safeguards against automated decision-making procedures, which includes their monitoring and oversight].
[232] Section 4.2.
[233] *Big Brother Watch and Others v. UK*, para. 418.
[234] Murphy, above, n. 229, 230.
[235] National Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment* (The National Academies Press, 2008); M. de Zwart, S. Humphreys and B. van Dissel, 'Surveillance, Big Data and Democracy: Lessons for Australia from the US and UK' (2014) 37(2) *University of New South Wales Law Journal*, 713.
[236] D. Korff and M. Georges, 'Passenger Name Records, Data Mining & Data Protection: The Need for Strong Safeguards' (Consultative Committee of the Convention for the Protection of Individuals with regard to Automated Processing of Personal Data (T-PD) of the Council of Europe, June 2015), https://rm.coe.int/16806a601b.
[237] L. Houwing, 'Stop the Creep of Biometric Surveillance Technology' (2020) 2 *European Data Protection Law Review*, 174.
[238] Intelligence and Security Committee, Privacy and Security: A Modern and Transparent Legal Framework (HC 2015 1075) para. 30, https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf.
[239] Ni Loideain, 'The Approach of the European Court of Human Rights', above, n. 223; P. Vogiatzoglou, 'Mass Surveillance, Predictive Policing, and the Implementation of the CJEU and ECtHR Requirement of Objectivity' (2019) 10(1) *European Journal of Law and Technology*, 1.
[240] *Big Brother Watch and Others v. UK*, para. 348. See also *Centrum för Rättvisa v. Sweden*, para. 262.

8.3 | Prevalence of ex ante authorisation for oversight, but with reservations

Since *Klass*, the ECtHR has engaged with the question of ex ante or ex post oversight of surveillance powers of security services in adjudicating adequate safeguards against those powers.[241] The Court has mentioned in dicta its preference for entrusting the judiciary with "oversight" (or, in the Court's words, control or supervision) powers, while approving other types of systems of oversight in light of the permissibility requirements under Article 8 of the ECHR.[242] Since *Digital Rights Ireland*, some authors observed that the CJEU may have gone beyond the ECtHR case-law when it started to mandate a priori effective review by a court or an independent administrative body for retention of data, compared to the rather imprecise direction by the ECtHR.[243] The CJEU iterations of effective review in *La Quadrature du Net and Others* and more recently the GC's findings in *Big Brother Watch* and *Centrum för Rättvisa* may indicate an interesting crossover between the CJEU and the ECtHR.

The ECtHR's preference for judicial oversight has been couched in its observation that 'the rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subjected to an effective control which should normally be assured by the judiciary'[244] since it offers 'the best guarantees of independence, impartiality and a proper procedure'.[245] Still, the judicial involvement was not a prerequisite of the Article 8 requirements. Independence is a defining feature of an oversight body that the ECtHR accepts as an adequate safeguard under Article 8 ECHR.[246] Thus, the ECtHR has spoken approvingly of other forms of oversight bodies that were tasked with investigating the practices of security and intelligence services. As mentioned earlier, the Court has considered a number of factors such as the qualifications of their members, practice, powers to investigate surveillance operations, duration of their terms and any safeguards to protect them from coercion.[247] For example, in *Klass*, the ECtHR considered the supervision of the G10 Commission, whose members were qualified to hold judicial office, and whose prior consultation had to be sought to implement the surveillance measure, along with the ex post oversight provided by the Parliamentary Board, as an adequate safeguard.[248] This approach was the ECtHR's early sign of not only accepting non-judicial or quasi-judicial bodies, but also evaluating the oversight system as a whole.

A key case in this respect is *Kennedy*, where the Court considered the general oversight structure as a compensation for the absence of a priori authorisation.[249] It was asked to adjudicate on the permissibility of the UK surveillance regime. The oversight system disputed in *Kennedy* consisted of the Interception of Communications Commissioner (ICC) and the Investigatory Powers Tribunal (IPT). The former was tasked with overseeing the general functioning of the UK surveillance regime as well as the decisions authorising the surveillance in specific cases. By considering who may be qualified to be the Commissioner and how he reviews the surveillance regime, including his powers to access to closed materials, the Court was satisfied that this ex post oversight body was independent of the executive and legislator.[250] The IPT is a court specialised in hearing complaints against the UK surveillance

[241] *Klass and Others v. Germany* (1979–80) 2 EHRR 214.

[242] See, for a brief review, G. Malgieri and P. de Hert, 'European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but Not Necessarily by Judges', in D. Gray and S.E. Henderson (eds.), *The Cambridge Handbook of Surveillance Law* (Cambridge University Press, 2017), 509; T.J. McIntyre, 'Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective', in M. Scheinin, H. Krunke and M. Aksenova (eds.), *Judges as Guardians of Constitutional and Human Rights* (Edward Elgar Publishing, 2016), 136; E. Kosta, 'Surveilling Masses and Unveiling Human Rights—Uneasy Choices for the Strasbourg Court' (Tilburg Law School Research Paper No. 2018–10, 3 May 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3167723.

[243] Malgieri and de Hert, above, n. 242 [especially in relation to interception carried out for criminal investigations, the authors reason the ECtHR's approach with the differences among Signatory Parties legal systems]. McIntyre, above, n. 242, notes that the first iterations in *Digital Rights Ireland* for a priori authorisation by a court or an independent administrative body concerned the permissibility requirements of data retention measures under the Charter and in this way, it treats the relevant aspect of the permissibility question on a par with the interception of communications, as opposed to the ECtHR's approach in its earlier cases concerning data retention. That said, the ECtHR has not assigned the judiciary with the authorisation power in the interception cases until its GC decision in *Big Brother Watch*.

[244] *Szabó and Vissy v. Hungary*, para. 77.

[245] *Klass and Others v. Germany*, para. 55.

[246] Section 5.

[247] Ibid.

[248] *Klass and Others v. Germany*, paras. 54–56.

[249] *Kennedy v. UK* (2011) 52 EHRR 4.

[250] Ibid., para. 166.

regime, whose jurisdiction does not depend on notification to the subject of surveillance. Anyone who suspects that they may have been subject to surveillance can apply to the IPT. The ECtHR affirmed the independent nature of the IPT as required under Article 8 of the ECHR based on its extensive jurisdiction, own rules of procedures and the qualifications of the members to be appointed.[251]

Still, in certain cases, the ECtHR explicitly disapproved of the lack of a priori involvement by an independent body. For example, in *Telegraaf Media Nederland Landelikje Media*, the Court considered the permissibility of implementing targeted interception against journalists to discover their journalistic sources under Articles 8 and 10 of the ECHR.[252] This interception could be authorised by the Ministry of Interior or security services and thus the lack of a priori authorisation by an independent body would not provide sufficient safeguards against using the interception measure to coerce journalists.[253] The ex post facto oversight body could not remedy the level of intrusion that journalists may suffer when they are the subject of an interception measure.[254] Similarly, the ECtHR has been critical of the major flows in the oversight system of surveillance measures in connection with national security interests. In *Zakharov*, the ECtHR disapproved of the judicial authorisation based on the very limited powers of the judiciary to effectively supervise the implementation of interception and the ineffectiveness of the subsequent supervision arrangements.[255] In *Szabó*, having determined the ineffectiveness of the ex post oversight system, the Court sought whether a priori authorisation from an official qualified for judicial office could remedy that system. The case-law thus far indicates that the key is to determine what type of oversight is the best to restrain security services surveillance powers. The ECtHR thus evaluates the oversight system of a Signatory Party comprehensively, and may be persuaded more towards requiring a priori intervention by an oversight body, based on the invasiveness of the surveillance measure.

The GC of the ECtHR's explicit iterations for a priori authorisation in the much-anticipated *Big Brother Watch* and *Centrum för Rättvisa* decisions thus rest on the Court's contextual analysis of the systems of oversight. In their challenge before the Chamber in *Big Brother Watch*, the applicants asked the Chamber to find a violation based on the lack of a priori authorisation for a bulk interception warrant, whose authorisation was made by the Secretary of State.[256] The Chamber refused this request based on its earlier acceptance of the UK oversight system and the independent reviews conducted in light of the Snowden revelations, which the Court found to show no evidence of *deliberate* abuse of power.[257]The Grand Chamber, however, overturned the Chamber's finding. It divided the stages of the bulk interception process from the initial interception and retention of packets of electronic communication to be subsequently selected for examination by selectors to the retention of the data after being examined by analysts.[258] After finding that each stage triggers the Article 8 protection at different levels, the Court differentiated the bulk interception regime in question from targeted interception, and held that the possible targeted interception based on "selectors" is preceded by untargeted interception by intelligence services.[259] Upholding the Chamber's refusal of mandating a reasonable suspicion requirement to conduct bulk interception as it would hamper its preventative nature, the Grand Chamber turned its attention to the oversight of the regime.[260] It thus put great emphasis on the oversight system. In other words, the GC aimed to compensate the lack of reasonable suspicion to carry out the bulk interception with more stringent requirements for the oversight of that interception regime. It noted that to restrain the intelligence services, 'bulk interception should be subject to independent authorisation at the outset,

[251]Ibid., para. 167.
[252]*Telegraaf Media Nederland Landelijke Media BV and others v. Netherlands*.
[253]Ibid., para. 100.
[254]Ibid., para. 101.
[255]*Roman Zakharov v. Russia*, paras. 274–285.
[256]The UK surveillance regime has since been revised with the introduction of the Investigatory Powers Act 2014, and a new system of authorisation requires the Judicial Commissioner to approve the bulk interception warrant authorised by the Secretary of State. See M.H. Murphy, *Surveillance and the Law: Language, Power, and Privacy* (Routledge, 2020), 62–67.
[257]*Big Brother Watch and Others v. UK*, paras. 381–383. Emphasis added.
[258]Ibid., paras. 325–327.
[259]Ibid., para. 346.
[260]Ibid., para. 349.

when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent ex post facto review'.[261] With an emphasis on "authorisation", the Grand Chamber clearly distinguished the oversight requirements for bulk interception from its earlier findings in *Kennedy*, where the Secretary of State could authorise the interception warrant, but, as discussed above, the lack of a priori judicial authorisation was remedied by an ex post facto oversight body that the ECtHR deemed independent and a specialised court that is tasked with ex post facto oversight. Moreover, while upholding its earlier finding that the issue turned on the authorising body independent of the executive, the Grand Chamber further considered its practice and tasks. The authorising body 'should be informed of both the purpose of the interception and the bearers or communication routes likely to be intercepted'.[262] The selectors to be used must be included in the application for bulk interception to allow the authorising body to determine their necessity and proportionality.[263]

In *Centrum för Rättvisa*, the Swedish law incorporated a priori judicial authorisation to its bulk interception regime, but to ensure compatibility with the ECtHR requirements, the Grand Chamber focused on the dual role of the Foreign Intelligence Inspectorate, which was tasked with not only overseeing surveillance operations in general, but also reviewing individual claims.[264] Following its established case-law, the Grand Chamber considered the latter as an effective remedy against the surveillance powers of security and intelligence services.[265] The existence of this type of ex post facto oversight was particularly important where national law does not require the subject of a surveillance operation to be notified.[266] Thus, the Grand Chamber reiterated the importance of an independent ex post facto oversight body, whose decisions are binding.[267] As mentioned above, the Grand Chamber was satisfied that the IPT was such body as far as the UK law was concerned. However, the Inspectorate's second role of reviewing individual claims would mean that it might have to assess its own decisions in supervising surveillance operations, which, according to the Grand Chamber, would generate a conflict of interest.[268] The Grand Chamber also spoke disapprovingly of the absence of any reasoned decision produced by the Inspectorate following a claim by an individual.[269] That said, on the question of the Inspectorate's power to produce binding opinions as part of its general oversight task, the Grand Chamber was persuaded by its duty to report to competent authorities whose decision is binding, although some of its operation rested on opinions and recommendations that were not legally binding.[270]

The Grand Chamber's recent decisions thus show a mutual standing between the approaches of the ECtHR and the CJEU (as observed in *La Quadrature du Net and Others*) in relation to the systems of oversight for surveillance operations of security services. First, both courts give importance to the independence of the oversight body, rather than its status. Second, both courts seem to mandate a priori involvement by an independent body in light of the invasiveness of the surveillance practice. Interestingly, in designating different oversight systems for surveillance operations challenged before it, the CJEU does not explicitly mention a connection between a priori and ex post review in terms of continuity of that review, especially where an a priori independent body is involved. The ECtHR's vision of assessing the oversight system comprehensively might provide the minimum threshold in this regard.[271] Finally, both courts agree on seeking an oversight body with powers to issue binding decisions. On this point, however, the overall assessment of the Swedish system seems to have compensated this requirement in *Centrum för*

[261] Ibid., para. 350.
[262] Ibid., para. 352.
[263] Ibid., paras. 352 and 354.
[264] *Centrum för Rättvisa v. Sweden*, para. 356.
[265] Ibid., para. 273.
[266] Ibid.
[267] Ibid.
[268] Ibid., para. 359.
[269] Ibid., para. 361.
[270] Ibid., paras. 349–350.
[271] The President of the ECtHR, Robert Spano, spoke of 'end-to-end' safeguards in considering the GC decisions in *Big Brother Watch* and *Centrum för Rättvisa*. See 'Speech by Robert Spano', 7 October 2021, at the Third European Intelligence Oversight Conference: National Security and the Role of Oversight Bodies in European Jurisprudence, https://www.echr.coe.int/Documents/Speech_20211007_Spano_Conference_European_Intelligence_Oversight_ENG.pdf.

Rättvisa. Still, the mutual observations between the Courts on certain points could serve as a benchmark for the legislative developments where Member States contest the requirements set by the CJEU.

9 | CONCLUSION

The question of the legal constraints under EU law of State powers in relation to retention of telecommunications data has culminated in a series of legal challenges before the CJEU. *Privacy International* and *La Quadrature du Net and Others* are part of this tug of war between Member States' desire to maintain generalised and indiscriminate data retention schemes and the upholding of fundamental rights.

This article highlighted that the public–private partnership took centre stage when several Member States argued that national data retention schemes safeguarding national security were the sole responsibility and competence of Member States and thus were beyond the reach of EU law. The cardinal point in the Court's reasoning in rejecting this claim was the central role that the private sector has played in surveillance activities. If *all* private sector data processing activities fall within the scope of EU law, so would the activities that involve retaining traffic and location data and granting security and intelligence services access to said data. It is immaterial whether the relevant data processing activities were carried out for safeguarding national security. The message of the Court was straightforward: Member States cannot divest themselves of their fundamental rights obligations under EU law by outsourcing data retention to private sector operators and oblige them to transmit the data to security and intelligence services with a simple reference to national security exemption.

Furthermore, the article analysed how the Court reiterated and, on some occasions, re-evaluated the limits of the powers of intelligence services and law enforcement authorities to retain and access telecommunications data. In *La Quadrature du Net and Others* in particular, the CJEU accepted a grading scale of permissibility requirements for different types of personal data processing based on the purpose pursued and the type of personal data involved (e.g., traffic and location data, IP address). Three clusters of public interest objectives—safeguarding national security; combating serious crime and preventing serious threats or serious attacks on public security; and combating crime and safeguarding public security—have emerged and each public interest objective entails different permissible retention activities based on the differing seriousness of threats.

Following on from the national court's reaction to the CJEU's findings, and the reform to the e-Privacy Directive, two—rather opposite—interpretations of its recent decisions emerge. On the one hand, the CJEU's approval of indiscriminate data retention schemes and automated analysis of personal data in pursuit of national security interest subject to certain safeguards might be considered as a departure from its earlier observations on the subject inaugurated with *Digital Rights Ireland*. To the extent that national courts apply the CJEU's reasoning in the recent decisions to confirm the expansion of intelligence and security services' powers, the decisions might be used to turn the scales in support of those powers. On the other hand, this emphasis on subjecting data retention schemes to those safeguards meant that the CJEU maintained the Charter requirements as the stronghold against unlawful surveillance of electronic communications data. It did so through expanding (or reiterating) its jurisdiction on the permissibility of surveillance measures under EU law to a field to which Member States have resorted to escape its scrutiny.

Be that as it may, the Court's detailed findings on "oversight" and the time within which state agencies must act emerge as the key safeguards against large-scale surveillance powers. A comparison with the latest ECtHR developments indicates an agreement between the ECtHR and the CJEU on setting out the conditions for permissible oversight systems under the ECHR and EU law, respectively. The common thread across the permissibility requirements for each intrusive surveillance activity (e.g. transfer of data to security services; data retention; automated analysis of personal data; real-time access to traffic and location data) is the existence of an effective "review" by a court or an administrative body to ensure the lawfulness of the interference. There are several crucial points in the CJEU's pronouncements on the nature of the review. First, the independence of the body reviewing security service surveillance operations, which the Court had the opportunity to expand on in *HK*, is key. Second, the Court explicitly

mandated the tasks that must be assigned to the bodies, which include the determination of the existence of a genuine and foreseeable serious threat against national security. Thus, the review bodies must be entrusted with the necessary powers to carry out their tasks. Lastly, the Court specifically required a priori review of decisions for real-time traffic and location data retention and their real-time sharing. Similarly, through the judgments, the CJEU has upheld the principle that data must be destroyed when it has served its purpose unless specific grounds are presented (and tested by an oversight authority) for extended retention. Thus, the timescale for action by intelligence and security services is limited.

Overall, the CJEU case-law on large-scale surveillance of telecommunication data has evolved, whereby each judgment has been met with resistance by national governments, and translated into their resistance to maintain national data retention schemes. In its case-law, the CJEU has thus been given the opportunity to elaborate on its initial pronouncements in *Digital Rights Ireland* and to strike a balance between avoiding a direct full-on clash with national governments, on the one hand, and maintaining limits to large-scale surveillance and upholding fundamental rights, on the other. In striking that balance, the CJEU accepted in *Privacy International* and *La Quadrature du Net and Others* that bulk data retention is permissible on national security grounds under strict conditions, including oversight. The judicial acceptance of the permissibility of large-scale surveillance for national security purposes could be seen as a pragmatic approach of the CJEU to end the data retention saga through containing national data retention regimes by ensuring their subjection to significant safeguards and limitations so that large-scale surveillance is the exception rather than the rule. This stance appears to be confirmed by the ECtHR, which appears to be moving away from the high threshold of safeguards developed by the CJEU. Though both European courts are in principle in alignment, their interaction is much more complex, and it is hoped that the seemingly more lenient approach of the ECtHR will not lead to further downgrading of the standards of protection as elaborated by the CJEU. In this ongoing friction, also demonstrated by the negotiations on the reform of the e-Privacy Directive, it remains to be seen whether these judicial developments will manage to meet national concerns on maintaining large-scale surveillance while also upholding fundamental rights in the digital era. The cases pending at the CJEU on the automated analysis of passenger information and data retention indicate that there might not be an imminent end to the story of (and resistance to) the permissibility of mass surveillance. Despite the CJEU seemingly watering down the safeguards against indiscriminate data retention while infiltrating the national security stronghold of Member States, it is to be hoped that the Court will succeed in disregarding the polarisation trap and fostering the adoption and development of new technologies that are compliant with fundamental rights through stringent but innovative legal requirements on the permissibility of mass surveillance in exceptional cases.

How to cite this article: Mitsilegas V, Guild E, Kuskonmaz E, Vavoula N. Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks. *Eur Law J*. 2023;29(1-2): 176-211. doi:10.1111/eulj.12417