# Fundamental rights in CJEU data retention case law:

# A refined regime in response to Member States' concerns, or compensating for the lack of legislative intervention in the digital age?

by **Evangelia Psychogiopoulou** *

**Abstract:** Data retention laws in the EU Member States entered a state of flux following Digital Rights Ireland and the annulment of Directive 2006/24/EC as a violation of the fundamental rights to respect for private life and the protection of personal data. For many Member States, it remained unclear what impact the invalidation of the directive should have on domestic data retention regimes. In subsequent case law, the CJEU sought to clarify the requirements deriving from EU law for national data retention legislation. While the CJEU has ruled that EU law in principle precludes national rules that prescribe a general and indiscriminate retention of traffic and location data by providers of electronic communications services and networks, it has also carved out exceptions that may justify interference with fundamental rights. Relevant cases have attracted much attention, with many national governments reaching out to the CJEU through observations submitted on what is admittedly a particularly complex and sensitive field of law. This article studies CJEU data retention case law and its evolution, examining the ways in which the CJEU has positioned itself vis-à-vis Member States' arguments on the balance to strike between fundamental rights' protection on the one hand and safeguarding national security and fighting (serious) crime on the other. The analysis shows how the CJEU has progressively refined and recalibrated its jurisprudence to acquiesce in part with Member States' demands. It also attests to the important role played by the CJEU in digital governance and the protection of fundamental rights in the absence of legislative intervention that addresses the particularities of the digital realm: the CJEU interprets the existing norms afresh, shaping the fundamental rights requirements applicable to Member States' data retention regimes.

Keywords: Court of Justice of the European Union (CJEU), data retention, access to data retained, fundamental rights, national security, combatting (serious) crime, e-Privacy Directive, e-Privacy Regulation, digital governance



Recommended citation: Evangelia Psychogiopoulou, Fundamental rights in CJEU data retention case law: A refined regime in response to Member States' concerns, or compensating for the lack of legislative intervention in the digital age?, 15 (2024) JIPITEC 194 para 1.

## A. Introduction

**1** The story of the European Union (EU)'s attempt to establish a data retention regime at the EU level has been well covered. Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services, or of public communications networks, sought to harmonize Member States' laws concerning the data retention obligations imposed on providers of electronic communications services and networks with a view to enabling access by the competent national authorities for the purpose of investigating, detecting and prosecuting serious crime.[1] In *Digital Rights*

* Assistant Professor, Department of Political Science and International Relations, University of the Peloponnese, e.psychogiopoulou@go.uop.gr; Senior Research Fellow, Hellenic Foundation for European and Foreign Policy, epsychogiopoulou@eliamep.gr. ORCID ID: 0000-0002-5326-6772

*Ireland*,[2] Directive 2006/24/EC was invalidated by the Court of Justice of the EU (CJEU) on the grounds that it breached Articles 7 and 8 of the Charter of Fundamental Rights (CFR) of the EU on the right to respect for private and family life and the right to protection of personal data, respectively.[3]

**2** Directive 2006/24/EC was adopted after the enactment of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (the e-Privacy Directive).[4] The latter sought to harmonize Member States' laws in order to ensure an equivalent level of protection for privacy and personal data with regard to the processing of personal data in the electronic communications sector, translating the principles laid down with regard to the processing of personal data and the free movement of such data in what was then Directive 95/46/EC (the Data Protection Directive,[5] the predecessor to the General Data Protection Regulation – GDPR[6]) into specific rules for the electronic communications sector. *Inter alia*, the e-Privacy Directive established the principle of the *confidentiality of communications*, prohibiting the storing of traffic data without the consent of the user. However, it also allowed for certain derogations by Member States.[7] Directive 2006/24/EC reflected this: it sought to cope with the variation in national provisions concerning the retention of data specifically for the purpose of preventing, investigating, detecting and prosecuting criminal offences. As held by the CJEU, it did so in a manner that was not compliant with fundamental rights. In fact, Directive 2006/24/EC had several flaws.[8] Most importantly, the general and indiscriminate retention of data it envisaged was viewed as a particularly serious interference with fundamental rights, given that it was insufficiently circumscribed to ensure respect for the principle of proportionality.[9]

**3** The CJEU declared Directive 2006/24/EC invalid as a result. Significantly, however, it neither outlawed data retention in general, nor addressed national legislation transposing Directive 2006/24/EC into Member States' national legal orders. National legislators could draw lessons from the CJEU ruling in *Digital Rights Ireland* regarding the compliance of rule-making with fundamental rights, but any privacy and data protection standards established by the CJEU in principle targeted only the EU legislator. This put domestic data retention regimes (enacted to transpose Directive 2006/24/EC but also adopted after its annulment) in a state of flux, which acted in turn as the catalyst for a wave of preliminary references made to the CJEU concerning national data retention laws and their compatibility with EU law, in the absence of EU secondary legislation on data retention. In this context, the focus has mostly been on the e-Privacy Directive in conjunction with general data protection law. Whereas the Data Protection Directive was intrinsically linked to the right to privacy,[10] the e-Privacy Directive states that national legislative measures regarding data retention should respect fundamental rights.[11] With the CFR acquiring binding legal effect with the Treaty of Lisbon,[12] references from national courts

1 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L 105/54 (no longer in force).

2 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and others* ECLI:EU:C:2014:238.

3 Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

4 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201/37.

5 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.

6 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 (General Data Protection Regulation) [2016] OJ L 119/1.

7 See Article 15(1) of Directive 2002/58/EC.

8 Marie-Pierre Granger and Kristina Irion, 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection' (2014) 39 European Law Review 835; Federico Fabbrini, 'Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S.' (2015) 28 Harvard Human Rights Journal 65; and Stefan Thierse and Sanja Badanjak, *Opposition in the EU Multi-Level Polity. Legal Mobilization against the Data Retention Directive* (2021 Palgrave Macmillan) 11, at 19.

9 See *Digital Rights Ireland*, paras 57-59 and 65.

10 See in particular recitals 2, 7, 9-11 and Article 1 of the Data Protection Directive.

11 According to Article 15 of the e-Privacy Directive, which was enacted before the CFR acquiring binding legal effect, any national measure concerning data retention should be in accordance with the general principles of EU law, including those referred to in Article 6(1) and (2) of the Treaty on European Union (TEU) and thus respect human rights and fundamental freedoms, which amounts to a general principle of the EU legal order. On this now see Art. 6(3) TEU [2012] OJ C326/13.

12 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community

for a preliminary ruling increasingly revolved around compliance with the CFR provisions.

**4** In its case law, the CJEU has sought to clarify the requirements deriving from EU law for national data retention rules. In *Tele2 Sverige*,[13] it ruled that EU law precludes national legislation that prescribes general and indiscriminate data retention.[14] However, in subsequent rulings, covering seminal cases like *Privacy International*, *La Quadrature du Net*, *Prokuratuur*, *Commissioner of An Garda Síochána* and *SpaceNet*,[15] it carved out exceptions that may justify interference with fundamental rights.[16] Relevant cases have attracted much attention, prompting national governments to submit observations, mostly arguing that the collection and analysis of electronic communications data by domestic authorities such as intelligence bodies and law enforcement services is an essential means for upholding national security and fighting serious crime. This article seeks to untangle the CJEU data retention case law by examining the ways in which the CJEU has positioned itself on Member States' claims and the balance to strike between fundamental rights' protection on the one hand and the public interest objectives advocated by Member States with regard to surveillance measures on the other. It shows that the CJEU has both sought to ensure a high level of protection of fundamental rights and taken Member States' concerns on board, providing some policy space for data retention measures at national level. The analysis starts with a discussion of key points in the CJEU's reasoning rejecting mass surveillance in *Tele2 Sverige* (section B). It then focuses on how the CJEU has treated the "national security card" played by Member States seeking to evade their fundamental rights obligations under the e-Privacy Directive vis-à-vis generalized surveillance (section C). The next section examines those CJEU pronouncements that create permissible exceptions for lawful surveillance at the national level in an attempt to respond to the desire of Member States to maintain (or introduce) data retention schemes (section D). What follows sheds light on the efforts of the CJEU to provide the Member States with more leeway, while at the same time setting forth substantive and procedural requirements (section E), which also take the form of safeguards for review by courts or independent administrative bodies (section F). The article then situates the CJEU's evolving case law in the context of the legislative reform of the e-Privacy Directive (section G), which has reached a standstill due to the conflicting views on the issue of data retention. It argues that against this backdrop of political (and legal) controversy, the CJEU's jurisprudence has a strong bearing on the rules and fundamental rights standards applicable to Member States' data retention schemes. The final section offers some concluding remarks on the CJEU's willingness to heed Member States' surveillance demands through its jurisprudence, and highlights the CJEU's crucial role in digital governance and the protection of fundamental rights in the digital age (section H).

## B. Setting limitations on national legislation relating to data retention and access thereto: Rejecting mass surveillance

**5** Two cases deriving from preliminary questions put by national courts in Sweden and the UK allowed the CJEU in *Tele2 Sverige* to provide guidance on the compatibility with EU law of domestic regimes on data retention and access thereto, ruling (and reiterating its stance in the wake of *Digital Rights Ireland*) on the non-permissibility of mass surveillance. Swedish legislation provided for the general and indiscriminate retention by providers of electronic communications services of the traffic and location data of all subscribers and registered users, with respect to every means of electronic communication, for the purpose of fighting crime. The UK legal rules at issue empowered the Secretary of State for the Home Department to adopt a general regime requiring public telecommunications operators to retain all data relating to any telecommunications service for a maximum period of 12 months, if it was deemed necessary and proportionate on grounds of national security or for the purpose of preventing or detecting crime or preventing disorder.

**6** In reviewing the relevant legislation, the CJEU

[2007] OJ C 306/1.

13 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* ECLI:EU:C:2016:970.

14 On bulk state surveillance, see Paul Bernal, 'Data Gathering, Surveillance and Human Rights: Recasting the Debate' (2016) 1(2) Journal of Cyber Policy 243; and Alena Birrer, Danya He, Natascha Just, 'The State is Watching You—A Cross-National Comparison of Data Retention in Europe (2023) 47(4) Telecommunications Policy.

15 See Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* ECLI:EU:C:2020:790; Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and others* ECLI:EU:C:2020:791; Case C-746/18 *Prokuratuur* ECLI:EU:C:2021:152; Case C-140/20 *Commissioner of An Garda Síochána* ECLI:EU:C:2022:258; and Joined Cases C-793/19 and C-794/19 *SpaceNet and Telekom Deutschland* ECLI:EU:C:2022:702.

16 On the CJJEU's evolving case law, see Adam Juszczak and Elisa Sason, 'Recalibrating Data Retention in the EU. The Jurisprudence of the CJEU – Is this the End or the Beginning?' (2021) 4 eucrim 238; Marcin Rojszczak, 'The Uncertain Future of Data Retention Laws in the EU: Is a Legislative Reset Possible?' (2021) 41(1) Computer Law & Security Report.

followed a two-pronged approach, distinguishing rules on data retention and rules on access to the data retained, considering these to be closely interrelated activities. Domestic legislation was assessed with reference to the e-Privacy Directive, which was interpreted in line with the CFR. The CJEU started its reasoning from the premise that, pursuant to Article 15(1) of the e-Privacy Directive, Member States could derogate from the principle of the confidentiality of communications laid down in Article 5(1) of the directive.[17] They could do so on a number of grounds, such as safeguarding national security (understood as state security), defence, public security and preventing, investigating, detecting and prosecuting criminal offences and the unauthorized use of electronic communications systems.[18] This list of objectives, the CJEU stated, was exhaustive. Member States should not depart from the confidentiality of communications on other grounds,[19] and any national measures derogating on the grounds set forth should respect fundamental rights,[20] and in particular the right to privacy (enshrined in Article 7 CFR), the right to protection of personal data (enshrined in Article 8 CFR) and the right to freedom of expression (enshrined in Article 11 CFR).[21]

**7** The Swedish regime under review provided for the general and indiscriminate retention of traffic and location data, imposing on providers of electronic communications services an obligation to retain the data systematically and continuously, without exceptions.[22] The CJEU found that the data retained[23] enabled "very precise conclusions" to be drawn regarding the private lives of the persons concerned: their "everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the[ir] social relationships [...] and the social environments [they] frequented".[24] The "profile" of individuals could thus be established.[25] Against this background, the CJEU held that the ensuing interference with the fundamental rights of Articles 7 and 8 CFR was "very far reaching" and likely to make the persons concerned feel "under constant surveillance".[26] Moreover, although national legislation did not target the content of communication as such, it could affect the use of electronic communications and consequently the exercise of freedom of expression.[27]

**8** Given such a "particularly serious" interference with fundamental rights, the CJEU ruled that only fighting *serious* crime (such as organised crime or terrorism) should be considered capable of justifying it.[28] However, while the effectiveness of the fight against serious crime could greatly depend on the use of "modern investigation techniques", such an objective of general interest could not in itself justify national legislation providing for the general and indiscriminate retention of all traffic and location data.[29] Indeed, the Swedish legislation imposed a general and indiscriminate data retention obligation with "no differentiation, limitation or exception",[30] it affected all persons using electronic communications services without requiring a link between their conduct and serious crime,[31] and contained no restrictions regarding the retention of data for a particular time period, geographical area or group of persons likely to be involved in serious crime.[32]

**9** Importantly, the CJEU did not rule out data retention in general and affirmed that, interpreted in accordance with the CFR, Article 15(1) of the e-Privacy Directive did not preclude the *targeted* retention of traffic and location data as a preventive measure in the fight against serious crime. This meant that data retention should be limited to what is strictly necessary regarding the data categories to be retained, the means of communication affected, the persons concerned and the retention period adopted;[33] in addition, the CJEU offered guidance on how these proportionality requirements could be satisfied.[34]

**10** Regarding access to the data retained by competent national authorities, an issue of relevance for both the Swedish and UK legislation under review, the

17 See *Tele2 Sverige*, para. 85.
18 Ibid, para. 90.
19 Ibid.
20 Ibid, para. 91.
21 Ibid, para. 93.
22 Ibid, para. 97.
23 The retained data made it possible to trace and identify the source of a communication and its destination, the date, time, duration and type of a communication, the users' communication equipment and the location of mobile communication equipment. They also included data such as the name and address of the subscriber or registered user, the telephone number of the caller, the number called and the IP address for internet services, and enabled the identification of the person with whom a subscriber or registered user had communicated, the relevant means and time of communication, the place from which communication had taken place and its frequency. See ibid, para. 98.
24 Ibid, para. 99.
25 Ibid.
26 Ibid, para. 100.
27 Ibid, para. 101.
28 Ibid, paras 100, 102-103.
29 Ibid, 103.
30 Ibid, para. 105.
31 Ibid.
32 Ibid, para. 106.
33 Ibid, para. 108.
34 Ibid, paras 109-111and 115-116.

CJEU followed the same rationale, considering only the objective of fighting *serious* crime capable of justifying the seriousness of the interference at hand.[35] To ensure respect for the principle of proportionality,[36] the national legislator should determine substantive and procedural conditions governing access to the retained data.[37] Taking note of the jurisprudence of the European Court of Human Rights (ECtHR) in this respect,[38] the CJEU held vis-a-vis substantive conditions that national authorities should only be granted access to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in serious crime,[39] though in particular situations where vital national interests are threatened (e.g. by terrorism), access can also be granted to other persons' data if there is objective evidence that the data can effectively contribute to combating the detected threats.[40] Concerning procedural requirements, the CJEU required prior review by a court or an independent administrative body (except in cases of validly established urgency[41]) and the notification of the persons affected, once the notification no longer jeopardizes the investigations undertaken.[42] It also cautioned against risks of misuse and unlawful access: providers of electronic communications services should guarantee a particularly high level of protection for the retained data, and national legislatures should ensure that the data is retained within the Union and irreversibly destroyed at the end of the retention period.[43] Whether the Swedish and UK laws satisfied such requirements was left to the referring courts to determine.

**11** *Tele2 Sverige* reflects the CJEU's efforts to establish a fundamental rights-compliant framework for examining the compatibility of national data retention laws with the e-Privacy Directive. It is also important for having clarified that national legislation on both data retention and access to the retained data comes within the scope of the e-Privacy Directive. Member States which submitted written observations to the CJEU had different views on this. Whereas the Belgian, Danish, German, Estonian and Dutch governments argued in the affirmative, the UK government claimed that only legislation relating to data retention should fall within the scope of the directive.[44] Crucially, the Czech government advanced the argument that national legislation whose aim is to combat crime should not come within the scope of the directive at all.[45]

**12** Determining the scope of application of the e-Privacy Directive was indeed a contentious issue, since the directive proclaims in Article 1(3) that "activities of the state" in the fields of public security, defence, state security and criminal law are excluded from its scope.[46] According to the CJEU, legislative measures derogating from the principle of the confidentiality of communications should not be deemed to be activities within the scope of Article 1(3) of the directive, as this would have deprived Article 15(1) of the e-Privacy Directive of its very *raison d'être*.[47] By enabling derogation from the principle of the confidentiality of communications, Article 15(1) of the directive necessarily presupposed that the national measures it authorized fell within the scope of the directive.[48] As both data retention and access to the retained data involved the processing of data,[49] the CJEU concluded that the e-Privacy Directive covered national measures on both.

## C. Clarifying the scope of application of the e-Privacy Directive

**13** In Tele2 *Sverige*, the CJEU rejected mass surveillance and unambiguously brought data retention and access thereof within the scope of EU law, despite the fact that secondary EU law on data retention no longer existed. *Ministerio Fiscal* confirmed the applicability of the e-Privacy Directive, interpreted in accordance with the CFR, with reference to domestic legislation in Spain which allowed the police to seek judicial authorization to access the subscriber data retained by providers of electronic communications services in connection with a criminal investigation.[50] In *Privacy International*,

35 Ibid, para. 115.
36 Ibid, paras 116 and 118.
37 Ibid, para. 118.
38 See ECtHR, 4 December 2015, *Zakharov v. Russia*, CE:ECHR:2015:1204JUD004714306.
39 See *Tele2 Sverige*, para. 119.
40 Ibid.
41 Ibid, para. 120.
42 Ibid, para. 121.
43 Ibid, para. 122.
44 Ibid.
45 Ibid, para. 65.
46 Ibid, para. 69.
47 Ibid, paras 72-73.
48 Ibid.
49 Ibid, paras 75 and 78.
50 In *Ministerio Fiscal*, the Spanish government, supported by the UK government, argued to no avail that the request for access to the data at issue on the grounds of a judicial decision in connection with a criminal investigation, fell within national authorities' exercise of *jus puniendi*, which constituted an activity of the State in the area of criminal law and therefore fell under the exception provided for in Article 1(3) of Directive 2002/58/EC (along with the exception laid down in the first indent of Article 3(2) of Directive 95/46/EC concerning *inter alia* processing operations on grounds of public security, defence, State

the CJEU reiterated the applicability of EU law, countering arguments put by Member States seeking to evade their obligations under the e-Privacy Directive, this time on national security grounds.

**14** This case originated in proceedings between Privacy International, a non-governmental organisation, and public authorities in the UK concerning the legality of domestic legislation enabling the acquisition and use of bulk communications data by the country's security and intelligence agencies for the purpose of safeguarding national security. According to the referring court, the databases compiled by these agencies, which should be as comprehensive as possible, sought to identify unknown threats to national security and were essential in the fields of counter-terrorism, counter-espionage and counter-nuclear proliferation.[51] Accordingly, the issue for the referring court was whether national legislation fell within the scope of the e-Privacy Directive, given that pursuant to Article 4(2) of the Treaty on European Union (TEU) and Article 1(3) of the e-Privacy Directive, national security remains a responsibility of the Member States.

**15** The UK, Czech, Estonian, Irish, French, Cypriot, Hungarian, Polish and Swedish governments argued, through observations, against the application of the e-Privacy Directive. They claimed that the purpose of the national legislation at issue was to safeguard national security and that the activities of the security and intelligence agencies, as essential state functions relating to the maintenance of law and order and safeguarding national security and territorial integrity, were the sole responsibility of Member States in line with Article 4(2) TEU.[52] Also, by means of Article 1(3), the e-Privacy Directive expressly excluded from its scope activities concerning public security, defence and state security, meaning that national measures in those fields were not required to meet its requirements.[53]

**16** The CJEU rebuffed these arguments. The disclosure of bulk communications data amounted to processing of personal data by providers of electronic communications services,[54] and *all* processing carried out by such providers should be seen as falling within the scope of the e-Privacy Directive, including processing which results from obligations imposed by public authorities.[55] Article 4(2) TEU did not alter this. In the CJEU's view, only measures *directly implemented* by Member States in the fields of Article 4(2) TEU (i.e. without the imposition of data processing obligations on private operators) should be seen as falling outside the scope of the e-Privacy Directive.[56]

**17** By endorsing such a narrow interpretation of Article 4(2) TEU, leaving "very little outside the scope of EU law",[57] the CJEU brought national measures on national security within the scope of the e-Privacy Directive (and its own jurisdiction[58]) and further developed the line of reasoning it adopted in *Tele2 Sverige*: a general and indiscriminate transfer of traffic and location data, and thus bulk access to traffic and location data, for the purpose of safeguarding national security was not congruent with EU law.[59] Still, the CJEU did acknowledge the importance of safeguarding national security which, as noted, went beyond that of the other public interest objectives referred to in Article 15(1) of the e-Privacy Directive, such as combating crime or safeguarding public security, and could therefore justify measures entailing more serious interference with fundamental rights.[60] The primary interest vis-à-vis state security, the CJEU explained, lay in protecting the "essential functions of the State and the fundamental interests of society", encompassing "the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities".[61] Nevertheless, the UK legislation exceeded the limits of what was strictly necessary, pursuant to Article 15(1) of the e-Privacy Directive interpreted in line with the CFR.[62] In particular, it did not rely on objective criteria to define the circumstances and conditions under which domestic authorities were to be granted access to the data concerned.[63]

security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law. See Case C-207/16 *Ministerio Fiscal* ECLI:EU:C:2018:788, paras 29-30.

51 See *Privacy International*, paras 25 and 29.

52 Ibid, para. 32.

53 Ibid, para. 33.

54 Ibid, para. 41.

55 Ibid, paras 44 and 46.

56 Ibid, para. 48.

57 Iain Cameron, 'Metadata Retention and National Security: Privacy International and La Quadrature du Net' (2021) Common Market Law Review 1433, at 1458.

58 On the CJEU asserting authority over national security with Privacy International, see Monika Zalnieriute, 'A Struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of European Union' (2021) 85(1) The Modern Law Review 198.

59 See *Privacy International*, paras 80-81.

60 Ibid, para. 75.

61 Ibid, para. 74.

62 Ibid, para. 81.

63 Ibid, para. 76.

## D. Carving out exceptions for national legislative measures

**18** *Tele2 Sverige* and *Privacy International* made it clear that data processing for the purpose of combatting (serious) crime and safeguarding national security comes within the scope of the e-Privacy Directive and is generally prohibited. However, while it did rule in *Privacy International* that national measures adopted with the aim of protecting national security are still subject to EU law, the CJEU appeared to provide Member States with some leeway for surveillance by underscoring the importance of national security as a public interest objective that may justify particularly intrusive interference in the exercise of fundamental rights, subject to strict proportionality constraints. In *La Quadrature du Net*, which originated in two references for a preliminary ruling by the French Council of State and the Belgian Constitutional Court respectively, the CJEU, in response to Member States' wanting to uphold data retention schemes, took steps to *qualify* their powers in doing so by carving out specific exceptions according to different sets of public interest objectives pursued at the national level. Each of these public interest objectives was judged capable by the CJEU of justifying distinct data retention activities in terms of their nature, breadth and ultimately seriousness in terms of interference with CFR rights.[64] Thus, in adjusting its position, the CJEU distinguished between measures concerning national security, measures designed to combat serious crime and prevent serious threats to or attacks on public security, and measures to combat less serious crime and attacks on public security. Underlying the CJEU's reasoning was the recognition, which chimes with the ECtHR jurisprudence, that besides *negative obligations* of non-interference, *positive obligations* to secure the *effective* enjoyment of fundamental rights may also derive from the CFR, in particular Article 3 on the right to the integrity of a person, Article 4 on the prohibition of torture and inhuman or degrading treatment or punishment and Article 7 CFR on the right to respect for family and private life.[65]

## I. The case for national security

**19** Adopting reasoning akin to that in *Privacy International*, the CJEU first confirmed that the more far-reaching permissible exception is the one which relates to the safeguarding of *national security*.[66] The CJEU ruled that national legislation which allows an order mandating general and indiscriminate data retention by providers of electronic communications services is compatible with the e-Privacy Directive, on condition that: there are sufficiently solid grounds for considering that the Member State concerned is confronted with a serious threat to national security, which is genuine, present or foreseeable;[67] the data retention takes place for a limited period of time[68] (which can, however, be extended if the serious threat persists[69]); the data retention is not systematic[70] and is subject to limitations and strict safeguards against the risk of abuse;[71] and that provision is made for effective review by a court or independent administrative body with a view to verifying that all the necessary conditions and safeguards are actually observed.[72]

**20** Importantly, the CJEU also accepted that intelligence gathering techniques enabling automated analysis and the real-time collection of traffic and location data can also be justified on national security grounds. The automated analysis at issue took the form of providers screening all the traffic and location data retained at the request of domestic authorities with a view to verifying correspondence matching certain parameters set by the latter.[73] This, the CJEU held, entailed a general and indiscriminate processing of the data of persons using electronic communications services,[74] which amounted to a particularly serious interference with CFR rights. For such measures to be justified, Member States should be facing a serious threat to national security which is shown to be genuine, present or foreseeable; the retention period should be limited;[75] and any authorizing decision should be subject to effective review by a court or independent administrative body.[76] Regarding the screening parameters used, the CJEU stated that these should be specific and reliable, making it possible to identify individuals who might be under a reasonable suspicion of participation in terrorist offences;[77] that they should be non-discriminatory; that they should not be based solely on data such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or information about a person's health or sex life;

64 Valsamis Mitsilegas, Elspeth Guild, Elif Kuskonmas, Niovi Vavoula, 'Data Retention and the Future of Large-Scale Surveillance: The Evolution and Contestation of Judicial Benchmarks' (2023) 29 European Law Review 176.

65 See *La Quadrature du Net*, paras 126 and 128.

66 Ibid, para. 136.

67 Ibid, para. 137.

68 Ibid.

69 Ibid, para 138.

70 Ibid.

71 Ibid.

72 Ibid, para. 139.

73 Ibid, para. 172.

74 Ibid, para. 174.

75 Ibid, para. 177.

76 Ibid, para. 179.

77 Ibid, para. 180.

and that they should be re-examined on a regular basis.[78] The CJEU added that any positive matches should be subject to an individual re-examination by non-automated means before the person concerned becomes adversely affected by a subsequent measure such as the real-time collection of his/her traffic and location data.[79]

**21** Concerning the latter, the CJEU observed that it should only be authorized individually for a person previously identified as potentially having links to a terrorist threat and persons in the same circle. The real-time collection of traffic and location data, the CJEU explained, is particularly intrusive, given that it provides a means of accurately and permanently tracking the movements of mobile telephone users.[80] Such an interference could only be justified in respect of persons for whom "there is a valid reason to suspect that they are involved in one way or another in terrorist activities".[81] An authorization decision should thus be based on objective and non-discriminatory criteria[82] and be subject to prior review carried out by a court or an independent administrative body.[83] Moreover, the competent national authorities should notify the persons concerned, provided that the notification does not jeopardize their tasks.[84]

## II. The case for combatting serious crime (and serious attacks on public security)

**22** Regarding data retention measures taken in respect of the second level in the hierarchy of objectives, namely *combatting serious crime and preventing serious threats or serious attacks on public security*, the CJEU asserted, in light of *Tele2 Sverige*, that compliance with any positive obligations deriving from Articles 3, 4 and 7 CFR should not translate into legislation giving the green light to the general and indiscriminate retention of traffic and location data without differentiation, limitations or exceptions,[85] and without the requirement of a link between the data of the persons concerned and the objective pursued.[86] This line of reasoning was confirmed in *Prokuratuur*, in reference to Estonian legislation enabling law enforcement authorities to gain *access* to traffic and location data which related to fixed and mobile telephone services and had been generally and indiscriminately retained. In *La Quadrature du Net*, the CJEU found that compliance with positive obligations under Articles 3, 4 and 7 CFR permitted *targeted* data retention for the purpose of combatting serious crime and preventing serious threats or attacks on public security (and *a fortiori*, national security),[87] with proportionality safeguards set for the data categories to be retained, the means of communication affected, the persons concerned and the retention period.[88]

**23** As several governments pointed to the difficulties surrounding the detection of offences committed online, especially child pornography,[89] the CJEU also accepted the compatibility with the e-Privacy Directive, read in the light of Articles 7, 8 and 11 CFR, of legislative measures providing for the general and indiscriminate retention of *IP addresses* with a view to combatting serious crime and preventing serious threats to public security (along with national security), subject to conditions.[90] The fact that IP addresses relate to the *source of connection* (and not to the recipient of communication) was deemed by the CJEU to make them less sensitive than other traffic data, on the grounds that no information is disclosed about the third parties with which communication is made.[91] Nonetheless, the ensuing interference with the CFR rights was considered to be serious, given that the IP addresses can reveal a user's clickstream and thus the user's entire online activity.[92] This led the CJEU to stress the importance of requirements limiting the retention period and substantive and procedural conditions restricting the uses to which the data are put.[93]

**24** Noting that it might prove necessary to retain data beyond the time period laid down in domestic legislation for legitimate purposes (for instance, for marketing and billing communication services or for purposes under Article 15(1) of the e-Privacy Directive), the CJEU also recognized that Member States may provide for the *expedited* retention of traffic and location data (also known as *quick freeze*), for a specified period of time and subject to effective judicial review, in order to fight serious crime (and attacks on national security).[94] To comply with the principle of proportionality, the retention obligation, the CJEU held, should only relate to traffic and location data that may shed light on serious

78 Ibid, paras 180-181.
79 Ibid, para. 182.
80 Ibid, para. 187
81 Ibid, para. 188.
82 Ibid, para. 189.
83 Ibid.
84 Ibid, para. 190.
85 Ibid, para. 143.
86 Ibid, para. 145.
87 Ibid, para. 146.
88 Ibid, para. 147.
89 Ibid, para. 154.
90 Ibid, paras 155-156.
91 Ibid, para. 152.
92 Ibid, para. 153.
93 Ibid, paras 155-156.
94 Ibid, paras 161 and 163-164.

criminal offences or acts adversely affecting national security, while the retention period should be limited to what is strictly necessary, although an extension should be possible where the circumstances and objective pursued justify it.[95] Notably, the CJEU ruled that the expedited data retention need not be limited to the data of persons suspected or having committed a criminal offence (or acts adversely affecting national security); it can also cover the data of victims and their social or professional circle, and data concerning specified geographical areas such as the place where the offence or act at issue was committed or prepared.[96] The CJEU also clarified that the public interest objective that guides *access* to the retained traffic and location data should be the same as the public interest objective justifying the *retention* of data.[97] However, it should be possible to access, on national security grounds, data originally retained to fight serious crime.[98] Contrariwise, access to data whose retention was justified by the objectives of combatting serious crime or safeguarding national security should not be granted for the purpose of prosecuting and punishing ordinary crime.[99]

## III. The case for combatting ordinary crime (and safeguarding public security)

**25** In *La Quadrature du Net*, the third level of public interest objectives reviewed, namely the objective of preventing, investigating, detecting and prosecuting criminal offences and safeguarding public security, was found capable of justifying only legislative measures concerning the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems, namely their addresses.[100] As such data only allows for the users' identification, without disclosing any information concerning the communications made and thus the users' private lives,[101] the CJEU held that its retention constitutes a 'non-serious interference' with the rights safeguarded in Articles 7 and 8 CFR[102] and can thus be accepted, even without a specific time limit.[103]

95 Ibid.
96 Ibid, para. 165.
97 Ibid, para. 166.
98 Ibid.
99 Ibid.
100 Ibid, paras 158-159.
101 Ibid, para. 157.
102 Ibid.
103 Ibid, para. 159.

## E. Refining the exceptions for national legislative measures

**26** In more recent case law, the CJEU has not departed from this graduated approach whereby specific public interest objectives justify particular data retention activities. In *VD*,[104] for instance, in which the CJEU dealt with French legislation providing for the general and indiscriminate retention of traffic data for one year, the CJEU confirmed that the public interest objective of fighting common crime, that is crime which does not qualify as "serious" (here, market abuse offences), cannot justify it.

**27** In *Commissioner of An Garda Síochána*, which stemmed from domestic proceedings concerning the validity of Irish data retention legislation, the CJEU reiterated, in the light of *La Quadrature du Net*, that Article 15(1) of the e-Privacy Directive, interpreted in line with the CFR, allows legislative measures that enable, for the purpose of safeguarding national security, a general and indiscriminate retention of traffic and location data, as long as the Member State concerned is confronted with a serious threat to national security which is genuine and present or foreseeable, coupled with other conditions. However, criminal behaviour, even of a particularly serious nature, should not be treated in the same way as a threat to national security.[105]

**28** The CJEU thus discarded claims put forward by Ireland and France that serious crime cannot be combatted effectively in the absence of a general and indiscriminate data retention.[106] It also refused arguments advanced by the Danish government that the competent national authorities should be able to access, for the purpose of fighting serious crime, traffic and location data retained in a general and indiscriminate way to address a serious threat to national security that is genuine and present or foreseeable. In the light of the hierarchy of public interest objectives outlined in CJEU judgments, access to the retained data should in principle be justified by the same public interest objective for which the data retention was ordered, unless the importance of the public interest objective pursued through access is greater than that of the objective justifying the retention of data.[107] As a result, authorizing access for the purpose of fighting serious crime (the second-level public interest objective envisaged) to traffic and location data retained in order to safeguard national security (the first-level public interest objective identified)

104 CJEU, Joined Cases C-339/20 and C-397/20 *VD* ECLI:EU:C:2022:703.
105 See *Commissioner of An Garda Síochána*, para. 63.
106 Ibid, para. 68.
107 Ibid, para. 98.

would be contrary to the classification of public interest objectives made.[108] This is arguably a more constrained interpretation than the one provided in *La Quadrature du Net*, where the CJEU appeared to accept that access to traffic and location data for the purpose of combatting serious crime *or* safeguarding national security is allowed on condition that the data is generally considered to have been retained in a manner compatible with the e-Privacy Directive.[109] In *Spacenet*, which focused on the conformity of data retention legislation in Germany with EU law, the CJEU employed the exact same reasoning it applied in *Commissioner of An Garda Síochána*, and stated, in response to similar arguments made by the Danish government, that only when access to the retained data is in pursuit of an objective whose importance is greater (i.e. safeguarding national security) than the one for which the data was retained (e.g. fighting serious crime) can the public interest objective pursued by data retention and access to the retained data differ.[110]

**29** *In Commissioner of An Garda Síochána*, however, the CJEU took steps to explain in more detail and to codify lawful forms of data retention, shedding more light on the permissible exceptions allowing data retention for combatting serious crime and preventing serious threats on public security (and by default, safeguarding national security, as this constitutes the highest public interest objective in the scaling system established). The list of measures that Member States can lawfully adopt in pursuit of these public interest objectives – which, as stressed by the CJEU, can also be combined and applied concurrently[111] – covers: a) the *targeted retention* of traffic and location data, which is limited on the basis of objective and non-discriminatory factors regarding the categories of persons concerned, or by geographical criterion, for a period that respects what is strictly necessary (which can, however, be extended); b) the general and indiscriminate retention of *IP addresses* assigned to the source of an internet connection for a limited period; c) the *expedited retention* of traffic and location data lawfully possessed by service providers for a specified period by means of the decision of a competent authority subject to effective judicial review;[112] and d) the general and indiscriminate retention of data relating to the *civil identity of users* of electronic communications systems. Relevant measures must all ensure, by means of clear and precise rules, that the retention of data is subject to compliance with the applicable substantive and procedural conditions, and that the persons concerned have effective safeguards against risks of abuse.[113] The same list of measures under the rubric of combatting serious crime, preventing serious threats to public security and *a fortiori* safeguarding national security was also sanctioned in *Spacenet*.

**30** Notably, *Commissioner of An Garda Síochána* offered additional guidance on some of these exceptions, refining their characteristics and scope. The CJEU explained, for instance, that the *targeted retention* of traffic and location data does not require that the persons suspected of being involved in an act of serious crime be known in advance.[114] It can also pertain to persons who are the subject of an investigation or other surveillance measures, or who are referred to in the national criminal record in relation to an earlier conviction for serious crimes and as highly likely to re-offend.[115] In a similar vein, the CJEU declared that, in the case of a geographical criterion being used to indicate a high risk of the preparation or commission of a serious crime, the areas covered can include places with a high incidence of serious crime, as well as places which are particularly vulnerable to serious crime, such as places with a high volume of visitors or places in strategic locations (i.e. airports, stations, maritime ports, tollbooth areas, etc.),[116] with Member States being able to use the average crime rate in a geographical area as a relevant criterion.[117] Offering more room for manoeuvre, the CJEU also held that non-personal or geographical criteria can be considered by Member States, as long as they are objective, non-discriminatory and help establish a connection, even of an indirect nature, between serious crime and the persons whose data are retained.[118]

**31** Along the same lines, the CJEU ruled that there is no requirement for an *expedited retention* of data to be limited to suspects identified in advance.[119] A national legislative measure may thus provide for the expedited retention of the traffic and location data of persons with whom a victim was in contact prior to a serious threat to public security arising or a serious crime being committed.[120] An expedited retention of data may also extend to specific geographic areas related to the commission of or preparation for the offence or attack in question,[121] a place or a person, including the victim of a serious crime

108 Ibid, para. 99.
109 See *La Quadrature du Net*, para. 167.
110 See *SpaceNet*, paras 128-130.
111 See *Commissioner of An Garda Síochána*, para. 92.
112 Ibid, para. 67.
113 Ibid, paras. 67 and 92
114 Ibid, para. 75.
115 Ibid, para. 78.
116 Ibid, para. 79.
117 Ibid, para. 80.
118 Ibid, para. 83.
119 Ibid, para. 75.
120 Ibid, para. 89.
121 Ibid, para. 90

who has disappeared,[122] and can be ordered when domestic authorities begin an investigation into a serious threat to public security or a possible serious crime.[123] As for the retention of data relating to the *civil identity of users* of electronic communications systems, the CJEU accepted that Member States may enact legislation for the purpose of combatting serious crime which makes the purchase of a means of electronic communication, such as a pre-paid SIM card, subject to the purchaser's identity being checked and that information being registered, with the seller being required, should the case arise, to give the competent national authorities access to that information.[124]

**32** The CJEU may have provided some extra policy space for Member States' data retention measures, but this did not eradicate the legal constraints on the latter stemming from EU law. Thus, in *Spacenet*, the CJEU did not accept the German government's argument that the data retention obligation at issue amounted to targeted retention.[125] Here, the referring court had raised doubts about the incompatibility of domestic data retention legislation with EU law, given that the data retention obligation concerned a relatively short period of time and a smaller amount of data[126] which excluded the content of communications along with data relating to the visited websites, data from electronic mail services and data concerning communications of a social or religious nature in the form of telephone assistance provided to people in distress. According to the CJEU, regardless of the length of the retention period and the quantity or nature of the data retained, the German legislation mandated the general retention of what remained a "very broad set of traffic and location data" which practically covered the entire population, without providing a reason and without drawing any distinction in terms of personal, temporal or geographical factors.[127] Such data provided the means for drawing "very precise conclusions" concerning the private lives of the persons concerned[128] (e.g. their everyday habits, their permanent or temporary places of residence, their daily or other movements, the activities they carried out, their social relationships and the social environments frequented),[129] and therefore for establishing their profile.[130] For the CJEU, the safeguards built into the legal framework to protect the retained data against risks of abuse and unlawful access could not remedy the serious interference resulting from the generalized data retention at issue.

## F. Review by courts and independent administrative bodies

**33** In its case law, the CJEU has also consistently held that data retention activities and access thereof shall be made dependent, as a general rule, on review by a court or an independent administrative body, mandating *prior r*eview (as opposed to *ex post* review) in certain instances. In *Prokuratuur*, the CJEU took steps to clarify the requirements for such a review, particularly from the perspective of the independence of the body entrusted with oversight duties. The Estonian legislation under dispute conferred upon the public prosecutor's office the power to authorize public authorities to access traffic and location data for the purposes of a criminal investigation. The CJEU ascertained that in the context of criminal investigations, such prior review should be entrusted to a court or body that is able to strike a fair balance between the needs of the investigation and combatting crime on the one hand, and the fundamental rights to privacy and protection of personal data on the other. This should essentially translate into a status which enables objective and impartial action, is free of external influence, and is thus a third party.[131] In the case at hand, the independence requirement was not satisfied: the investigation procedure was directed by the public prosecutor's office, which also conducted the public prosecution; it did not therefore have a neutral stance vis-à-vis the parties.[132] The CJEU employed similar reasoning in subsequent rulings. In *Commissioner of An Garda Síochána*, for instance, it held that national legislation which assigned a police officer the power to centrally process requests for

122 Ibid.

123 Ibid, para. 91.

124 Ibid, para. 71.

125 See *Spacenet*, para. 84.

126 In the context of the provision of telephone services, the retention obligation laid down covered, *inter alia*, the data required to identify the source of a communication and its destination, the date and time of the start and end of the communication or – in the case of communication by SMS, multimedia message or similar message – the time of dispatch and receipt of the message and, in the case of mobile use, the designation of the cell sites used by the caller and the recipient at the start of the communication. In the context of the provision of internet access services, the retention obligation covered, *inter alia*, the IP address assigned to the subscriber, the date and time of the start and end of the internet use from the assigned IP address and, in the case of mobile use, the designation of the cell sites used at the beginning of the internet connection. The data enabling the identification of the geographical location and the directions of maximum radiation of the antennas serving the cell site in question were also retained.

127 See *Spacenet*, paras 81-83.

128 Ibid, paras 87-88.

129 Ibid, para. 90.

130 Ibid, para. 87.

131 See *Prokuratuur*, paras 53-54.

132 Ibid, para. 54.

access to data by police services for the investigation or prosecution of serious criminal offences did not fulfil the requirements for independence.[133] This was so, despite the police officer being assisted by a police unit with a certain degree of autonomy, and the fact that the decisions issued could be subject to judicial review.[134]

**34** Clearly then, a body external to the authority seeking access to the retained data is necessary and should be made responsible for determining the lawfulness of the interference with the CFR rights deriving from access to the data. The independence requirement thus entails that administrative bodies embedded in the law enforcement and security hierarchy cannot constitute lawful oversight authorities. Importantly, the court or administrative body entrusted with the task of review should have all the necessary powers and provide all the guarantees required to reconcile the various interests and rights in question.[135] This implies that it has the capacity to carry out an *effective examination* of whether the surveillance measure at issue is justified, which extends to assessment of whether a situation justifying that measure exists and whether the various conditions and safeguards that must be laid down in domestic legislation are being observed.[136]

**35** In the light of the CJEU's case law to date, external and independent control is required of any requirement placed on providers of electronic communications services: a) to retain, generally and indiscriminately, traffic and location data[137] and to provide access to such data;[138] b) to undertake, for a specified period of time, the expedited retention of traffic and location data;[139] c) to carry out automated analysis of traffic and location data;[140] and d) to engage in real-time collection of traffic and location data.[141] *Prior* review by a court or independent administrative body is essential in the case of automated analysis,[142] in the case of the real-time collection of traffic and location data,[143] and regarding access to data generally and indiscriminately retained.[144]

133 See *Commissioner of An Garda Síochána*, para. 111.
134 Ibid, paras 111-112.
135 See *Prokuratuur*, para. 52.
136 On this see *La Quadrature du Net*, paras 139 and 168.
137 See *Commissioner of An Garda Síochána*, para. 58.
138 Ibid, para. 106.
139 Ibid, paras 67 and 86. See also *La Quadrature du Net*, para. 168.
140 See *La Quadrature du Net*, paras 179 and 192.
141 Ibid, paras 189 and 192.
142 Ibid, paras 179 and 192.
143 Ibid, paras 189 and 192.
144 See *Prokuratuur*, paras 50-51 and *La Quadrature du Net*, para. 106.

## G. Data retention case law and the CJEU's role in the digital age

**36** CJEU case law on the legal constraints on Member States' data retention regimes deriving from EU law reflects a clear effort by the CJEU to strike a balance between the different rights and interests involved. In light of the arguments presented by Member States in favour of upholding data retention regimes at the national level, the CJEU has progressively refined and recalibrated its jurisprudence to acquiesce in part with the Member States' demands. This shows a somewhat receptive court – that is, one that is willing to accept and assuage Member States' concerns by recognizing that certain forms of data retention and access thereof can still be regulated at the national level. However, it also reflects a court that is willing to solve the legal problems brought to its attention through novel rule-interpretation that clarifies and elaborates on how a norm should be interpreted henceforth so as to address the challenges posed by digitalisation and concurrently uphold fundamental rights. This has to be seen in the light of the difficulties the EU legislator has keeping pace with technological developments and updating the legislative framework established by the e-Privacy Directive, while at the same time refraining from using the legislative process to *legalize* mass data retention at the national level to the detriment of fundamental rights.

**37** When the European Commission (Commission) published its proposal in January 2017 for an e-Privacy Regulation to replace the e-Privacy Directive in light of the broad range of internet-based services enabling inter-personal communication, beyond traditional communication services, it did not deviate from the approach followed by Article 15 of the e-Privacy Directive. It confirmed that legislative measures on data retention that pursue public interest objectives should remain possible *under conditions*,[145] and declared that the principle

145 See Article 11(1) of the 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/2017/010 final, according to which "Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 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) to (e) of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests."

of confidentiality should apply to various means of communication, including "calls, internet access, instant messaging applications, e-mail, internet phone calls and personal messaging provided through social media".[146] However, when the Council agreed on the scope of its mandate to negotiate the e-Privacy Regulation with the European Parliament on 10 February 2021 after four years of stalled discussions between the Member States, it included data retention and diverted from CJEU case law.

**38** The Council's mandate is as follows: Article 2(2)(a) and (d) respectively exclude from the scope of the Regulation "processing activities and operations concerning national security and defence, 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" and "activities, including data processing activities, of competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".[147] Recital 26 then affirms that the e-Privacy 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 this is necessary and proportionate to "safeguard specific public interests, including public security and the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and other important objectives of general public interest".[148] More conspicuously, Article 7(4) states 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", adding that "[t]he duration of the retention may be extended if threats to public security of the Union or of a Member State persist".[149]

**39** Rules of this sort are not in line with CJEU case law.[150] They water down the safeguards and conditions crafted by the CJEU and give the Member States *carte blanche* to retain data by creating a concrete legal basis for it. Clearly, the institutional preferences of the Council differ from those of the European Parliament, which is keen to keep data retention as an exception and to not make it the rule.[151] It should thus come as no surprise that negotiations between the two institutions have reached a political stalemate.[152] While trilogues are reported to have begun on 20 May 2021, the legislative file stagnated under the Swedish Council Presidency (1/1/2023-30/6/2023),[153] while the subsequent Spanish (1/7/2023-31/12/2023) and Belgian Council Presidencies (1/1/2024-30/6/2024) did not consider the conclusion of the negotiations a priority.[154] This

146 Ibid, Recital 1.

147 See Council of the EU, 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) - Mandate for negotiations with EP, 6087/21, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=EN.

148 Ibid.

149 Ibid. Article 6(1)(d) of the Council's mandate adds that providers of electronic communications networks and services should be permitted to process electronic communications data if it is necessary *inter alia* to comply with "a legal obligation to which the provider is subject laid down by Union or Member State law, which respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society 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."

150 See Marcin Rojszczak (n 16); Maria Tzanou and Spyridoula Karyda, 'Privacy International and Quadrature du Net: One Step Forward Two Steps Back in the Data Retention Saga?' (2022) 28(1) European Public Law 123; and Gavin Robinson, 'Targeted Retention of Communications Metadata: Future-Proofing the Fight Against Serious Crime in Europe?' (2023) 8(2) European Papers 713.

151 Committee on Civil Liberties, Justice and Home Affairs, Report on the 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), 20.10.2017, Rapporteur: Marju Lauristin, https://www.europarl.europa.eu/doceo/document/A-8-2017-0324_EN.html.

152 See European Parliament, Legislative Train Schedule, Proposal for a regulation on privacy and electronic communications in "A Europe Fit for the Digital Age", https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-jd-e-privacy-reform.

153 Ibid.

154 See EU23, Programme, Spanish Presidency of the Council of the European Union, Second half of 2023, Europe, closer, https://spanish-presidency.consilium.europa.eu/media/

is also the case with the current Hungarian Council Presidency (1/7/2024-31/12/2024).[155]

**40** In such a context of political (and legal) deadlock, the CJEU's case law has a strong bearing on the rules and standards applicable to Member States' data retention schemes. Through its case law, the CJEU revisits the interpretation of long-established norms at EU level, creating new understandings that seek to cater for the challenges posed by digitalisation and the proliferation of communication services online, in the light of Member States' concerns in pursuit of public interest objectives and the need to safeguard fundamental rights. From this perspective, the CJEU assumes a key role in digital governance and the protection of fundamental rights in the digital era: faced with the needs brought into being by the digital realm, coupled with the inertia of the EU legislator, the CJEU jurisprudence *adapts* EU law and *shapes* the fundamental rights requirements it sets for Member States' data retention regimes – inevitably on a case-by-case basis. This confirms arguments in the literature about courts (European courts in particular) having assumed a crucial role in addressing the challenges of the digital age through rule-interpretation that responds to present-day conditions and also compensates for the absence of legislative reform.[156]

## H. Conclusion

**41** CJEU case law on the legal constraints deriving from EU law for Member States' data retention regimes has been growing following *Digital Rights Ireland* and the annulment, on fundamental rights grounds, of Directive 2006/24/EC, which sought to harmonize Member States' laws concerning the data retention obligations of providers of electronic communications services and networks with a view to combatting serious crime. In a gradually evolving line of rulings, the CJEU has positioned itself, in what is admittedly a particularly complex field of law, on Member States' surveillance schemes and practices in pursuit of public interest objectives ranging from protecting national security and fighting terrorism to detecting and investigating crime. Relevant case law reflects a clear effort by the CJEU to strike a balance between the distinct rights and interests involved. In light of Member States' fervent arguments in favour of upholding data retention regimes at the national level, the CJEU has progressively refined and recalibrated its jurisprudence to acquiesce in part with Member States' demands. The CJEU held at an early stage that national data retention schemes are not beyond the reach of EU law and that Member States cannot escape their fundamental rights obligations by outsourcing data retention obligations to private operators that are required to provide access thereof to security, intelligence, law enforcement and other domestic authorities.[157] At the same time, the CJEU accepted early on that there is no absolute prohibition on data retention and that derogation from the confidentiality of communications is not unthinkable. Since then, finding itself in the delicate position of having to secure fundamental rights on the one hand and cope with Member States' sensitivities on the other, it has taken steps to create some room for state manoeuvre, while considering data retention and access to the retained data as separate interferences with the exercise of fundamental rights which must be justified separately.

**42** Cases like *Privacy International*, *La Quadrature du Net* and *Commissioner of An Garda Síochána* show the CJEU's willingness to recognize Member States' concerns by taking the view that they can still regulate certain forms of data retention and access thereof at the national level. The CJEU's responsiveness to Member States' calls for some leeway to be found for preserving national data retention schemes has gone hand in hand with graduation, respect for the principle of proportionality and keeping true to the basic rule that data retention should be the exception and not the rule in a democratic society, given the dissuasive effect it can have on the exercise of fundamental rights.[158] As regards the public

e4ujaagg/the-spanish-presidency-programme.pdf; and beEU, belgium24.eu, Programme, Belgian Presidency of the Council of the European Union, First half of 2024, https://belgian-presidency.consilium.europa.eu/media/3kajw1io/programme_en.pdf.

155 HU24EU, Programme of the Hungarian Presidency of the Council of the European Union in the Second Half of 2024, https://hungarian-presidency.consilium.europa.eu/media/32nhoe0p/programme-and-priorities-of-the-hungarian-presidency.pdf.

156 On the role of courts in the digital age, see Evangelia Psychogiopoulou and Susana de la Sierra, 'European Supranational Courts and Judicial Decision-Making in the Era of Digitalisation', in Evangelia Psychogiopoulou and Susana de la Sierra (eds), *Digital Media Governance and Supranational Courts. Selected Issues and Insights from the European Judiciary* (2022 Edward Elgar Publishing) 1; and Giovanni de Gregorio and Oreste Pollicino, 'Courts, Rights and Powers in the Digital Age', in Federica Casarosa and Evangelia Psychogiopoulou (eds), *Social Media, Fundamental Rights and Courts. A European Perspective* (2023 Routledge) 242.

157 On the private sector assuming tasks of generalized and indiscriminate data retention and the ensuing public-private surveillance partnership, see Valsamis Mitsilegas, 'The Privatisation of Surveillance in the Digital Age', in Valsamis Mitsilegas and Niovi Vavoula (eds.), *Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives* (2021 Hart Publishing) 101.

158 See *Tele2 Sverige*, para. 104.

interest objectives in particular that may justify data retention (and access to the data retained), it is clear from the CJEU's jurisprudence that in accordance with the principle of proportionality, a hierarchy exists which accords with the importance of the public interest objective to be attained, and that the seriousness of the interference introduced by the national surveillance measure must be proportionate to the importance of the public interest objective at issue. This means that each public interest objective permits different data retention activities based on the degree of seriousness of the specific threats, which also has implications for access to the data retained. Thus, the CJEU has ruled that the importance of the objective of safeguarding national security, read in the light of Article 4(2) TEU according to which national security remains the sole responsibility of Member States, supersedes that of the objectives of combatting crime – even serious crime[159] – and of safeguarding public security.[160] The objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights, such as general and indiscriminate data retention, automated analysis of personal data and real-time collection of traffic and location data, subject to stringent conditions and independent oversight.

**43** Overall, the CJEU's jurisprudence contains several key pronouncements concerning national surveillance measures, and has evolved to take on board national governments' concerns whilst elaborating protective standards for upholding fundamental rights. Along with the CJEU's readiness to adapt its case law in order to reach a compromise and give consideration to Member States' stated desire for data retention schemes at the national level, the system of requirements created exemplifies the CJEU's crucial role in digital governance and the protection of fundamental rights in the digital age. Indeed, the evolution of the CJEU's case law must be viewed in the light of the failure of the EU legislator to come up with a meaningful update to the e-Privacy Directive dating back to 2002, and thereby to keep pace with the development of electronic communications services and, importantly, do so in a fundamental rights-compliant way, without risking any downgrading of the protection afforded to fundamental rights. In such a context of political tension and legislative uncertainty, with inter-institutional negotiations on the e-Privacy Regulation essentially blocked, the CJEU offers some kind of solution to the data retention impasse. This lies in defining standards for fundamental rights protection pragmatically, on a case-by-case basis, without ignoring Member States' concerns relating to the pursuit of public interest objectives. Seen in this light, through its case law, the CJEU *creates* and *remoulds* understandings of the checks and balances that should accompany national schemes for and practices of data retention, and thus provides some direction where the EU legislator – having failed to date to modernize the e-Privacy legal regime in the digital economy – does not.

159 Note however that in certain instances, it can prove challenging to distinguish serious forms of criminality from threats to national security. On this, see Gavin Robinson (n 150), at 723 and Iain Cameron (n 57), at 1462-1463.

160 See *La Quadrature du Net*, para. 136.