Once upon a time... Digital Rights Ireland: The never-ending saga of data retention in the EU

LAW 2023/7
Department of Law

WORKING PAPER

Once upon a time... *Digital Rights Ireland*: The never-ending saga of data retention in the EU

Luisa Marin and Sarah Tas

European University Institute

Department of Law

Once upon a time... *Digital Rights Ireland*: The never-ending saga of data retention in the EU

Luisa Marin and Sarah Tas

LAW Working Paper 2023/7

ISSN 1725-6739

Published in December 2023 by the European University Institute.
Badia Fiesolana, via dei Roccettini 9
I – 50014 San Domenico di Fiesole (FI)
Italy
www.eui.eu

With the support of the Erasmus+ Programme of the European Union

The European Commission supports the EUI through the European Union budget. This publication reflects the views only of the author(s), and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Abstract

The aim of this chapter is to revisit and assess the data retention case law of the Court of Justice. After *Digital Rights Ireland*, the Court was requested by domestic courts to return to its doctrine on several occasions, and/so it took the chance to specify its view both in relation to the different typologies of data, and to the goals of retention. The result is a web of requirements and guarantees that defines a doctrine on the relationship between, on the one side, surveillance, and investigations, and, on the other side, privacy, and data protection. Its implications touch upon domestic criminal systems and on national security. In a first moment, this jurisprudence contributed to the emergence of a European narrative on counterterrorism. Nevertheless, new questions for preliminary reference continue to reach the Court and the political debate is dealing with an important legacy, which can also turn into an obstacle on the path of a new European legislative instrument.

The present piece is forthcoming as a chapter in M. Bergström, V. Mitsilegas, T. Quintel (eds.), 'Research Handbook on EU Criminal Law'.

Keywords

data retention – privacy – data protection – e-privacy directive – crime – national security - Court of Justice

Luisa Marin

Luisa Marin is a Marie Curie Fellow at the Law Department of European University Institute and Assistant Professor at the University of Insubria. Luisa acknowledges funding from the European Union’s Horizon 2020 research and innovation program, Marie Skłodowska-Curie grant agreement No 891762.

Sarah Tas

Sarah Tas is an Assistant Professor of European and Comparative Administrative Law at the University of Maastricht.

"We should not always rely on the courts to repair unsound laws that are the result of political opportunism"

Sophie in't Veld[1]

[1] The quote is reported in the article: The Parliament Magazine, "ECJ declares data collection rules illegal", at https://www.theparliamentmagazine.eu/news/article/ecj-declares-data-collection-rules-illegal

1. Data retention: at the intersection between surveillance and security vs. privacy and data protection

The Court of Justice's landmark judgment of April 8th 2014, *Digital Rights Ireland*,[2] which annulled the Data Retention Directive[3] (hereinafter: DRD) triggered a landslide of legislative reforms and preliminary references by domestic courts. The latter dealt with various issues ranging from domestic data retention law to the scope of the privacy and data protection rights provided for by EU instruments, and the notions of national security and criminal offences. Ever since, the Court has delivered a rich strand of case law,[4] which is still vivid. The last cases concern the scope of the e-privacy Directive[5] inasmuch it implements fundamental rights enshrined in the Charter, as well as on the scope of the notions of prosecuting serious crimes and of the national security clause provided for in Art. 4(2) TEU.[6]

This case law is highly salient for several reasons. First, it is central for the elaboration of a fundamental rights doctrine on privacy and data protection. These rights are enshrined in the Charter and are getting relevance in the EU legal order, both internally and in their external dimension. They have been used to assess the legality of European legislation which has been instrumental to the fight against terrorism. It should be recalled that *Digital Rights Ireland* had been delivered less than a year after the beginning of the Snowden revelations, which unveiled illicit mass surveillance programs carried out by the US National Security Agency and by the British intelligence Government Communications Headquarters (GCHQ) to fight terrorism.[7] The clandestine data mining scheme PRISM collected stored internet communications from requests made to Google, Yahoo, Microsoft, AOL, Facebook, Skype, Apple, and other companies. The future seems dominated by the emergence of big data, AI and machine learning technologies that will be integrated in policing and justice administration: the scope of fundamental rights as emerging from this case law will have a meaning in the future.

---

[2] Court of Justice of the EU (Grand Chamber), 8 April 2014, joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Ireland*, ECLI:EU:C:2014:238.

[3] 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, OJ L 105, 13.4.2006, p. 54-63.

[4] Joined cases C-203/15 and C-698/15, *Tele2 Sverige AB and Watson* [2016] ECLI: EU: C:2016:970; Case C-207/16, *Ministerio Fiscal* [2018] ECLI:EU:C:2018:788; Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others* [2020] ECLI:EU:C:2020:791; Case C-746/18, *H.K. v Prokuratuur* [2021] ECLI:EU:C:2021:152.

[5] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning processing of personal data and protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47.

[6] Case C-140/20, *G.D. v The Commissioner of the Garda Síochána and Others* [2022] ECLI:EU:C:2022:258; Joined Cases C-793/19 and C-794/19, *Bundesrepublik Deutschland v SpaceNet AG* (C-793/19) and *Telekom Deutschland GmbH* (C-794/19) [2022] ECLI:EU:C:2022:702.

[7] The Guardian, NSA Files: Decoded. What the revelations mean for you, at

https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded

A second reason why this balance is crucial for our democracies intersects with the dividing line between protection of the private sphere and legitimate limitations on it, which are a state prerogative. This monopoly entails a legitimate space for surveillance, here represented by data retention, which involves collection and storage of personal data from private companies and, consequently, access by law enforcement authorities. The complex architecture of data retention boils down to these two layers of interferences with the private dimension, one by private actors and one by public ones, but conversely, it also limits the powers of law enforcement agencies to deploy effective means to combat crimes. It is not by chance that governments have on multiple occasions defended the necessity of data retention practices, which amounts to a third reason.[8]

Thirdly, this case law is also relevant in a criminal justice perspective, since it defines the equilibria between data subjects, including suspects of crimes and crime perpetrators, public authorities, and victims of crimes. Furthermore, elaborating on the dividing line between serious crimes and national security, the 'data retention saga' intersects the delicate question of division of competences between EU and Member States, first, on the definition of the national security exception of Art. 4(2) TUE, and second, on Member States' prerogatives in policing and investigations. Along this line, the case law of the Court indirectly influences the legal framework adopted for EU Agencies (such as Europol).

All this considered, this case law will have relevance in the political debate for some years ahead. Indeed, the reform of the European legislation on privacy and data protection with the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED), alongside the recast of the e-privacy directive proposed back in 2017, will keep privacy and data protection concerns at the center of the political debate for some years to come. Furthermore, this 'saga' sets clear boundaries that a future European data retention framework must respect. Lastly, the development of artificial intelligence (AI) technologies, and their potential for criminal justice deployments, will have to reckon with these boundaries and positive prescriptions given by the Court of Justice.

The chapter will revisit this saga through its milestones, starting from *Digital Rights Ireland*. It will further explore the *Tele2/Watson* and *Ministerio Fiscal* cases, before proceeding to the judgments in *La Quadrature du Net/Privacy International* and *H.K. v. Prokuratuur*. The latest progenies of this stream of cases are *G.D. v. The Commissioner of An Garda Síochána and Others* and *SpaceNet*. In the following sections, the chapter will examine the legacy of this case law, focusing, firstly, on the judicial dimension: it will elaborate on the complex reception of the Directive and of the Court of Justice's case law; secondly, it will reflect upon its political heritage, focusing on the data matrix case of Europol, and on the debates for future legal instruments, the e-privacy directive and a future data retention framework, before concluding.

2. The data retention 'saga': the Court of Justice at the center of the scene

[8] The Data Protection Office (DPO) of Europol had conducted a study on the data retention regime applying in the Member States, released on 22.8.2016 and circulated from the General Secretariat of the Council to the DAPIX, Friends of the Presidency. It is here stated that "Member States unanimously confirm that data retention has a positive impact on the prevention, investigation and prosecution of serious crimes and terrorism" and that it helps directing investigation, and also supports other forms of evidence, or enables construction of trails of evidence leading up to an offence, as well as supporting the judicial authority in the decision-making process. The quote is from p. 4 of the document.

2.1. Setting the scene: the *Digital Rights Ireland* case and invalidation of the Data Retention Directive

The first case of the saga, which led straight to the annulment of the data retention directive, is the answer to two joint cases submitted in 2012, one presented by the NGO Digital Rights Ireland, and the second one, from the Government of Carinthia and 11,130 individual applicants in a complaint for constitutional review before the Austrian Constitutional Court. In its referral, for example, the Austrian Court stressed that the Directive allowed storage of 'so many types of data in relation to an unlimited number of persons for a long time' and concerned 'almost exclusively persons whose conduct in no way justifies the retention of data relating to them'. This raised doubts as to the adequacy and the proportionality of the interference between data retention and fundamental rights, notably the right to privacy, the right to data protection and freedom of expression.

Although it recognized that the Directive might also have an impact on freedom of expression, namely in the form of an inhibiting effect,[9] the Court of Justice focused its review on privacy and data protection, which are conceptualized as two distinct interferences.[10] The Court has reframed data retention into, first, retention of a broad set of meta-data concerning communications by telecommunications providers, and, secondly, access to data collected by the competent national authorities, waiving the (then applicable) Data Protection Directive and the e-Privacy Directive.[11] The criticism on data retention is not radical and does not preclude a future legislation. Instead, it demolishes the precise arrangements approved in the Directive. In the view of the Court, privacy and data protection have not been violated in their essence.[12] Instead, the reasoning focuses around the justification and proportionality of the interference, which is founded on the objectives of general interests of the fight against serious crime and the enhancement of public security, recalling its case law on *Kadi and Al Barakaat* and *Tsakouridis*.[13]

Mass surveillance is rejected on the ground of its necessity. This is key because it states the Court's position on the normalization of a state of exception and of a state of emergency: the highest court of the EU legal order considered that the fight against serious crime, namely organized crime and terrorism, did not in itself justify extensive surveillance of the whole population in the EU.[14] Respect for both rights to privacy and data protection is anchored to the principle of strict legality:[15] cases and conditions for their limitation must be specified by

[9] See also *Digital Rights Ireland*, para. 28 and 70.

[10] *Digital Rights Ireland*, para. 24 ff. See also para. 34-35.

[11] Digital Rights Ireland, para. 34-35.

[12] *Digital Rights Ireland*, para. 39-40. Privacy has not been violated because the content of the communication is not the object of retention. Data protection has not been violated because Member States were to ensure that appropriate technical and organizational measures were adopted against accidental or unlawful destruction, accidental loss or alteration of the data. See also Maja Brkan, 'The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning', *German Law Journal*, (2019), 20, pp. 864-883.

[13] *Digital Rights Ireland*, para. 42.

[14] *Digital Rights Ireland*, para. 51.

[15] Since the Court has interpreted the right to data protection as functional to protection of privacy, it stated that the right to data protection must also involve the same guarantees as privacy, namely, the principle of strict legality.

law, and such limitations must be subject to judicial scrutiny.[16] In substantiating these requirements, the EU legislation must lay down 'clear and precise rules governing the scope and application of the measures in question and imposing minimum safeguards' in the form of guarantees granting effective protection in case of abuse of, unlawful access to, and use of those data.[17]

The first problem is the lack of differentiation, limitation, or exception in light of the objective of fighting against serious crime and the lack of connection, even indirect, with a situation which was liable to give rise to a criminal prosecution.[18] The 'one size fits all' approach to retention did not pass the scrutiny of the Court. The second issue is the lack of an objective criterion by which to determine the limits of access of law enforcement agencies to retained data and their use,[19] with substantive and procedural conditions relating to access of the competent national authorities to data and their use. Third, a form of judicial scrutiny on the access by national authorities should be in place.[20] Additional grounds are the length of retention, which does not distinguish between categories of data; the lack of safeguards for data security against the risk of abuse of the retained data; a last concern relates to the external dimension, which might imply breach of control by an independent authority as required by the Charter.[21] On these grounds, the Court motivated the annulment of the Directive, rejecting the pre-emptive logic which has animated many of the counter-terrorist measures. The rationale of *Digital Rights Ireland* echoes the *Kadi* judgment, in the sense that the Court rejected the necessity of an EU legal instrument derogating from the principles of the constitutional state based on the rule of law. The Court clearly rejected the 'panopticism' underlying this measure.

Looking beyond the case, the relevance of *Digital Rights Ireland* is key because in finding legal grounds for declaring the annulment of the Directive, the Court sowed all the seeds which should generate a future data retention framework. In other words, the *pars destruens* of the reasoning is also the *pars construens* of requirements and guarantees that a future legal instrument must respect. Additionally, the collapse of the European legislation has triggered more seismic waves, to which the next sections are devoted.

2.2. *Tele2 Sverige/Watson* and *Ministerio Fiscal*: domestic legislations through the prism of the Charter of Fundamental Rights

After *Digital Rights Ireland* and the annulment of the Directive, legal doubts appeared as to its implications on the validity of domestic legislation transposing the Data Retention Directive. The ambiguities relate to the validity of the transposing national laws, as well as the position of the Court on data retention, and in particular the compatibility of generalized data retention with EU law. Thus, this opened the door to multiple preliminary references by Member States.

[16] The Court, while it considered privacy and data protection as two distinct legal frameworks, nevertheless seemed to interpret the latter as functional to protection of privacy. On the relation between the two rights, see Orla Linksey, Deconstructing Data Protection: The Added-Value of a Right to Data Protection in the EU Legal Order, (2014) 63(3) *International and Comparative Law Quarterly*, p. 569.

[17] *Digital Rights Ireland*, para. 56.

[18] Digital Rights Ireland, para. 56 ff.

[19] Digital Rights Ireland, para. 60 ff.

[20] *Digital Rights Ireland*, para. 60 ff. x

[21] Namely Art. 8(3) of the Charter. *Digital Rights Ireland*, para. 64-68.

The first cases came from Sweden and the United Kingdom in *Tele2 Sverige AB and Watson* on legislation adopted for the fight against serious crime, passed in December 2016.[22] It was the first time that the Court had to decide, after *Digital Rights Ireland*, on the application of EU law to cases of national legislation on the retention of traffic and location data, and their access for the purpose of combating crime. The Court stated that these cases fall under EU law since the state activities involved providers of electronic communication services, regulated by the e-privacy directive.[23]

Drawing from *Digital Rights Ireland*, the Court followed a systemic approach to reviewing existing national laws, merging into one single act the two moments of the retention of metadata by providers and access to data by law enforcement authorities.[24] With regards to the compliance of the retention law, the Court confirmed its strong stance in favour of data protection and privacy, against state surveillance in Europe. In fact, it precluded generalised and indiscriminate retention of traffic and location data, where there is no link between the retained data and the threat and no restrictions on retention, and where it exceeds what is strictly necessary. The Court however, distinguished between bulk and preventive targeted data retention. Whereas the former does not comply with EU law, the latter is not as such precluded when backed up by appropriate safeguards. These include respect for the necessity criteria and the existence of minimum safeguards, of clear and precise rules, and of an objective link with a *serious* criminal offense.[25] As to compliance of access to retained data, similar rules may apply with the addition of procedural rules of prior review by a court or an independent administrative body of the request for access, and notification obligations.[26]

In these joined cases the Court followed the line laid down in the previous case law but went a step further by offering an extensive interpretation of the statutory law in place, namely the e-Privacy Directive (Art. 15) read conjunctively with the Charter.[27] Two aspects can be noted here. The first is the introduction of the procedural safeguard of prior authorization by a Court or an independent administrative authority. In contrast, the e-Privacy Directive merely requires establishment of an independent supervisory authority and does not provide for *ex ante* authorization.[28] Secondly there is the condition of combating serious crime to legitimate data retention. Once again, this criterion does not emerge from statutory law but from interpretation of the principle of proportionality. The criterion was initially also part of the Data Retention Directive. Paradoxically, the Court offers an interpretation of the issue at stake that in some respects resembles the rules of the annulled legal instrument. Taken in conjunction with *Digital Rights Ireland*, the Court developed a high threshold for data retention, without ever dismissing

[22] Joined cases C-203/15 and C-698/15, *Tele2 Sverige AB and Watson* [2016] ECLI: EU: C:2016:970.

[23] Joined cases C-203/15 and C-698/15, *Tele2 Sverige AB and Watson* [2016] ECLI: EU: C:2016:970, paras. 78-81.

[24] Oreste Pollicino, Marco Bassini, 'La Corte di Giustizia e una trama ormai nota: la sentenza Tele 2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico', in *Diritto Penale e Contemporaneo*, 9.1.2017.

[25] Joined cases C-203/15 and C-698/15, *Tele2 Sverige AB and Watson* [2016] ECLI: EU: C:2016:970, paras. 108-112.

[26] Joined cases C-203/15 and C-698/15, *Tele2 Sverige AB and Watson* [2016] ECLI: EU: C:2016:970, para. 125.

[27] Joined cases C-203/15 and C-698/15, *Tele2 Sverige AB and Watson* [2016] ECLI: EU: C:2016:970, para.

[28] Marcin Rojszczak, 'The uncertain future of data retention laws in the EU: Is a legislative reset possible?' [2021] *Computer Law & Security Review* 41.

the need of retaining data.[29] Whereas the Court clarified the safeguards needed to lawfully retain metadata, doubts remain on the exact meaning of the judgment. Thus, preliminary questions continued to be addressed to Luxembourg, for example by Spain in the *Ministerio Fiscal* case of October 2018.[30] Spain precisely questioned the criteria of *seriousness* developed by the Court. The Court developed a relation between infringement of privacy and data protection and criminal offenses.[31] Access to retained data can be allowed for fighting crime, not considered *serious* crime, when the interference with fundamental rights is not considered *serious*. In the same strain, if the interference is *serious*, meaning where access to the data makes it possible to reach precise conclusions on an individuals' private life, it can only be justified by the fight against *serious* crime. This somewhat clarifies the position of the Court on the criteria of *seriousness*.

This case adds another milestone in the saga: it completes the perspective developed in *Tele 2*, by dealing specifically with the aspect of access by authorities to retained data. This can seem to contradict its position in *Ireland v. Parliament and Council*, where it stated that the Data Retention Directive did not deal with the issue of access to data, but was concerned with retention.[32] Though this case concerned the e-Privacy Directive, one has to observe that this systemic or integrated reading of data retention is fraught with consequences, in the sense that it broadens the scope of the scrutiny of the Court of Justice toward domestic laws concerning public authorities' access to data in the context of crime.[33] In another perspective, the case builds a proportionality doctrine in the relation between interferences with fundamental rights and the types of crimes justifying them, by distinguishing between categories of data (identification data, or traffic data or location data) and the seriousness of the interferences.

However, these two more cases did not mean the end of the judicial saga: instead, they paved the way for more cases and references dealing with domestic laws on intelligence activities and national security.[34]

2.3. Taking a step aside? *La Quadrature du Net/Privacy International* and the limited carving of a national security exception

The never-ending saga of data retention involved another episode in 2020, this time to clarify data retention for national security purposes. The Court decided on this long-debated issue in

[29] Adam Juszczak and Elisa Sason, 'Recalibrating Data Retention in the EU' (2021) Eucrim < https://eucrim.eu/articles/recalibrating-data-retention-in-the-eu/ > accessed 9 December 2021.

[30] Case C-207/16, *Ministerio Fiscal* [2018] ECLI:EU:C:2018:788.

[31] Case C-207/16, *Ministerio Fiscal* [2018] ECLI:EU:C:2018:788, paras. 56 and 57.

[32] Cf. CJEU, *Ireland v. Parliament and Council*, para. 83. See also Giulia Formici, Tutela della riservatezza delle comunicazioni elettroniche: riflessioni (ri)partendo dalla pronuncia *Ministerio Fiscal*, in Osservatorio costituzionale AIC, 3/2018, 26.11.2018, p. 466.

[33] Giulia Tiberi, Il caso Tele2 Sverige/Watson: una iconica sentenza della Corte di Giustizia nella saga sulla data retention, in *Quaderni costituzionali*, 2017, pp. 434-438.

[34] David Fennelly, Data retention: the life, death and afterlife of a directive, in ERA Forum, Springer, 25.6.2018; Lorna Woods, Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber), EU Law Analysis, 21.12.2016.

the cases *Privacy International*,[35] brought (again) by the United Kingdom, and *La Quadrature du Net*, which joined cases from France and Belgium.[36] It started by clarifying and extending the scope of EU law. In principle, the founding Treaty excludes national security from the scope of EU law.[37] However, within the e-Privacy Directive, two articles seem to conflict. On the one hand, Article 1(3) excludes national security from the scope of the instrument and, on the other hand, Article 15(1) states that it is possible to restrict the principle of confidentiality to safeguard national security.[38] Thus, doubts arose in these two cases, as to whether EU law applies to national measures taken for the purposes of protecting national security.[39] While nine Member States argued that the Directive shall not apply to activities of security and intelligence agencies,[40] the Court decided otherwise. According to the Court, national law which requires providers of electronic communications services to retain metadata for the purposes of protecting national security falls within the scope of the e-Privacy Directive.[41] The mere fact that processing and retention of data is conducted by a private entity makes it fall under EU law.

On the data retention issue, the Court followed the same line of arguments taken in its previous case law. While in national security cases, the Court admits that more intrusive measures could be adopted, the strict scrutiny test still applies with regards to proportionality.[42] This means that the measures must be strictly necessary and rely on objective criteria. In both cases, the Court found that general and indiscriminate data retention of traffic and location data by security and intelligence agencies for the purpose of safeguarding national security is in principle incompatible with EU law. It did, however, open the door to several exceptions.

The first exception concerns general and indiscriminate data retention.[43] This type of retention may be allowed if the Member State is confronted with a *serious* threat to national security, which is genuine and foreseeable. However, this retention cannot be systematic and must be limited in time. Effective review shall be conducted by a court or an independent administrative body, to ensure that the conditions and safeguards are respected. The second exception deals with targeted retention authorised for *serious* crimes, *serious* threats to public security and safeguarding national security. The following conditions must be met: it must be limited to what is strictly necessary and based on objective and non-discriminatory factors.

---

[35] Case C-623/17, *Privacy International* [2020] ECLI:EU:C:2020:790.

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

[37] Treaty of the European Union, Article 4(2).

[38] Council and European Parliament Directive 2002/58/EC of 12 July 2002 on processing of personal data and protection of privacy in the electronic communications sector [2002] OJ L 201, Articles 1(3) and 15(1).

[39] Marcin Rojszczak, 'The uncertain future of data retention laws in the EU: Is a legislative reset possible?' [2021] *Computer Law & Security Review* 41.

[40] United Kingdom, Czech Republic, Estonia, Ireland, France, Cyprus, Hungary, Poland and Sweden.

[41] Case C-623/17, *Privacy International* [2020] ECLI:EU:C:2020:790, para. 49; Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others* [2020] ECLI:EU:C:2020:791, para. 104.

[42] Case C-623/17, *Privacy International* [2020] ECLI:EU:C:2020:790, paras. 75-76; Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others* [2020] ECLI:EU:C:2020:791, paras. 136-137.

[43] Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others* [2020] ECLI:EU:C:2020:791, para. 139.

The third exception relates to retention of IP addresses, on the one hand, and of civil identity, on the other hand.[44] General and indiscriminate retention of IP addresses must be subject to strict compliance with substantive and procedural conditions. The rules on civil identity are looser, due to the little information it gives on someone's personal life. The retention may concern any type of crime and does not need a specific time limit or a link between the retained data and the objective. The fourth limit discusses the "quick freeze", meaning the expedited retention of metadata for combating *serious* crime and safeguarding national security.[45] This type of retention can comply with EU law, when it is proportionate and limited to what is strictly necessary and where the offense has already been established or may reasonably be suspected. Finally, the Court stated that real-time retention and automatic detection and analysis of data to fight crime and discover security threats are compatible with EU law.[46] This is the case when the security threat to national security is *serious*, genuine, and present or foreseeable, and where the duration is limited to what is strictly necessary.

Through these two cases, the Court attempted to clarify further the scope of data retention legislations and provide guidelines on their admissibility for national security purposes. Opening up to bulk data retention for national security purposes, the Court has nevertheless put boundaries to it, broadening the scope of European data privacy rights against security concerns. It nevertheless decided not to go beyond the threshold of targeted data retention, thus rejecting the requests emerging from domestic authorities, such as governments, courts, and law enforcement authorities, to shift toward a more viable form of data retention for domestic actors. Despite the detailed judgment, the Court did not manage to clarify some aspects: first, the definition of national security is left to Member States, which therefore enjoy some discretion. Precisely, it is left to them to define the actual circumstances which represent a serious, real and actual threat to national security. Therefore, even these landmark judgments did not put an end to the saga. The new preliminary references meanwhile raised have not been withdrawn by the referring courts.[47] This seems to be the result of a process in which a clarification of the Court triggers uncertainty on a connected issue, which therefore pushes for some questions to be submitted to the Court. This highlights the extent of the uncertainty emerging from the decisions taken by the Court, and the persistent fragmentation within the Member States.

2.4. The data retention saga in perpetual motion? H.K. v Prokuratuur, G.D. v The Commissioner of An Garda Síochána and others and SpaceNet

While the number of cases decided by the Court would have suggested requests for preliminary references by domestic courts would come to an end, the practice showed otherwise. As recognized by Advocate General Sánchez Bordona, the new references "highlight once again the concern raised in some Member States by the case law of the Court

[44] Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others* [2020] ECLI:EU:C:2020:791, paras. 156-159.

[45] Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others* [2020] ECLI:EU:C:2020:791, para. 161.

[46] Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others* [2020] ECLI:EU:C:2020:791, para. 181.

[47] OPINION OF ADVOCATE GENERAL CAMPOS SÁNCHEZ-BORDONA, delivered on 18 November 2021, Case C-140/20, *G.D. v. The Commissioner of the Garda Síochána*, ECLI:EU:C:2021:942, para. 25.

on the retention of, and access to, personal data generated in the electronic communications sector."[48]

The last cases in the saga, *H.K. v Prokuratuur*,[49] *G.D. v The Commissioner of An Garda Síochána and others*,[50] and *SpaceNet*,[51] dealt among others, with the guarantees of the authorization procedure in access to retained data by national authorities. Thus, these cases influence the criminal proceedings, and notably the admissibility of evidence and the role of public prosecutors and police officers.

In the first case, *H.K. v Prokuratuur*, the Court, building on its case law, reiterated that access to metadata, due to the major interference with the right to privacy, must be strictly limited to proceedings related to *serious* crime.[52] It went a step further by stating that the admissibility of evidence is an issue of national procedural autonomy. However, the principle of effectiveness requires national criminal courts to disregard information and evidence obtained through a breach of EU law if the person is not in a position to effectively comment on the information and the evidence is likely to have a preponderant influence on the decision.[53] The findings of the Court imply that this evidence has to be assessed at the stage of judicial proceedings. Therefore, *H.K.* affects not only the data retention debate, but also influences the rules on criminal proceedings. Moreover, the Court specified the requirement of independence to be met by the authority tasked with scrutiny on access to retained data, deciding that the public prosecutor does not meet the criterion of independence, being involved in the conduct of criminal investigations.[54]

The second case, *G.D. v The Commissioner of An Garda Síochána and others*, essentially confirmed its previous case law that EU law precludes, as a preventive measure, the general and indiscriminate retention of traffic and location data for the purposes of combating serious crimes.[55] It also repeated the exceptions that the Court mentioned in *La Quadrature du Net*,[56] with regards the limited targeted retention, the retention of IP addresses, the retention of data related to the civil identity of users and the quick freeze.[57] When it comes to the influence of the case-law on criminal proceedings, the Court essentially reiterated *H.K. v Prokuratuur* on

[48] OPINION OF ADVOCATE GENERAL CAMPOS SÁNCHEZ-BORDONA, Delivered on 18 November 2021(1), Joined Cases C-793/19 and C-794/19, *Bundesrepublik Deutschland v. SpaceNet AG, Telekom Deutschland GmbH*.

[49] Case C-746/18, *H.K. v Prokuratuur* [2021] ECLI:EU:C:2021:152.

[50] Case C-140/20, G.D. v The Commissioner of the Garda Síochána and Others [2022] ECLI:EU:C:2022:258.

[51] Joined Cases C-793/19 and C-794/19, *Bundesrepublik Deutschland v SpaceNet A*G (C-793/19) and *Telekom Deutschland GmbH* (C-794/19) [2022] ECLI:EU:C:2022:702.

[52] Case C-746/18, *H.K. v Prokuratuur* [2021] ECLI:EU:C:2021:152, para. 45.

[53] Case C-746/18, *H.K. v Prokuratuur* [2021] ECLI:EU:C:2021:152, para. 43.

[54] Case C-746/18, *H.K. v Prokuratuur* [2021] ECLI:EU:C:2021:152, paras. 54-56.

[55] Case C-140/20, G.D. v The Commissioner of the Garda Síochána and Others [2022] ECLI:EU:C:2022:258, para. 101.

[56] Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others* [2020] ECLI:EU:C:2020:791, paras. 136-161.

[57] Case C-140/20, G.D. v The Commissioner of the Garda Síochána and Others [2022] ECLI:EU:C:2022:258, para. 101.

the admissibility of evidence and the requirement of independence. First, the Court stated that the admissibility of evidence obtained through retention schemes, is a matter of national procedural autonomy, that is solely limited by the obligation of compliance with the principles of equivalence and effectiveness.[58] Second, the Court emphasized the importance of a prior review by a court or an independent administrative body, to access retained data. In this regard, it concluded that a police officer does not constitute a court and does not have all the guarantees of independence and impartiality required to qualify as an independent administrative body.[59] This position has been reiterated in *SpaceNet*.[60] These cases show the impact that the Court of Luxembourg can have on domestic criminal proceedings. The Court tries to clarify the data retention saga and the limitations on access to traffic and location data by law enforcement authorities. However, doubts remain, for example on what constitutes a *serious* crime.[61]

This section has presented the milestones of the judicial saga on data retention, which started with the annulment of the data retention directive, and later, though the medium of the interpretation of the e-Privacy Directive, displayed consequences on the legislations of the Member States. Analysing them altogether allows us to clarify the complex legacy left by the Court in this long-standing debate. In fact, since *Digital Rights Ireland*, the Court has been the sole European actor able to influence the discussion and develop European standards to be respected within each of the EU Member States. In this connection, the Court of Justice developed a set of criteria for data retention in the fight against crime and safeguarding of national security. When it comes to the fight against crime, the Court repeatedly stated that generalised and indiscriminate retention of traffic and location data is not compliant with EU law. Preventive targeted data retention and access to it may be authorized solely for serious crimes, if it contains sufficient safeguards (necessity, objective link, clear and precise rules). For access to data by law enforcement agencies, additional procedural safeguards apply, namely the notification duty and prior review by a court or independent administrative body. When it comes to national security purposes, the Court has made concessions, accepting more intrusive measures, but still applying a strict scrutiny test (necessity, appropriateness, proportionality and objective criteria). Several exceptions have been introduced, when the threat to national security is serious, genuine, present, or foreseeable.

Overall, the Court has offered interesting clarifications on the data retention debate as well as criteria to be taken into account when developing new national or European data retention legislation. However, some aspects remain in the hands of the Member States, such as the definition of a serious crime and the scope of national security.[62] While the activism of the Court of Justice cannot be denied, it is now time to turn our attention to the reception of this case law in domestic legal orders, in order to study its implementation.

[58] Case C-140/20, G.D. v The Commissioner of the Garda Síochána and Others [2022] ECLI:EU:C:2022:258, para. 127.

[59] Case C-140/20, G.D. v The Commissioner of the Garda Síochána and Others [2022] ECLI:EU:C:2022:258, para. 111.

[60] Joined Cases C-793/19 and C-794/19, *Bundesrepublik Deutschland v SpaceNet AG* (C-793/19) and *Telekom Deutschland GmbH* (C-794/19) [2022] ECLI:EU:C:2022:702.

[61] Sophia Rovelli, 'Case *Prokuratuur*: Proportionality and the Independence of authorities in data retention' [2021] European Papers 6 No. 1 199.

[62] Sophia Rovelli, 'Case *Prokuratuur*: Proportionality and the Independence of authorities in data retention' [2021] *European Papers* 6 No. 1 199, 207.

3. Reception of the saga in domestic legal orders: a chronicle of uncertainty and fragmentation

The judicial heritage of the data retention saga is characterized by fragmentation and uncertainties emerging in the Member States' legal orders. This started even before the annulment of the Directive and remains true nowadays. Though a comprehensive overview on all the Member States would fall outside the scope of this work, both because of the geographical and temporal dimension of this comparison, we can nevertheless give some perspectives based on assessments of some reactions triggered by this case law.

3.1. Contestation and uncertainty: the scenario before and after *Digital Rights Ireland*

As highlighted in the first edition of this chapter,[63] the data retention directive has been a contested instrument and has triggered several reactions in Member States' legal orders since the early days. First, it has met resistance in the transposition. Ireland has for example launched an action for annulment against the Directive,[64] and several Member States (notably Austria, the Netherlands, Sweden, Greece, and Ireland) have delayed its transposition. Initially, the European Commission kept its role as an active enforcer of EU law and initiated several infringements proceedings against Member States that failed to transpose the Directive in the prescribed period.[65] In that regard, Sweden was fined – for the first time – for failing to fulfil its obligations under the Directive.[66] Another form of contestation appeared soon after legislators transposed the Directive within the national legal orders. The transposition met strong judicial opposition at domestic level. The German *Bundesverfassungsgericht* (the Federal Constitutional Court) entirely invalidated the national transposing law,[67] and the Commission subsequently initiated an infringement procedure against the German position.[68] Before *Digital Rights Ireland*, other national higher courts challenged, either partially or totally, the national implementing provisions for breach of constitutional rights: this is the case of the Bulgarian

[63] Luisa Marin, 'The fate of the Data Retention Directive: about mass surveillance and fundamental rights in the EU legal order', in Valsamis Mitsilegas, Maria Bergström, Theodore Konstadinides (eds), *Research handbook on EU criminal law*, Edward Elgar, 2016, p. 210 ff.

[64] Judgment of the Court (Grand Chamber) of 10 February 2009, *Ireland v European Parliament and Council of the European Union*, Case C-301/06, ECLI:EU:C:2009:68.

[65] Chris Jones and Ben Hayes, 'The EU Data Retention Directive: a case study in the legitimacy and

effectiveness of EU counter-terrorism policy',

https://www.statewatch.org/media/documents/news/2013/dec/secile-data-retention-directive-in-europe-a-case-study.pdf

[66] Judgment of the Court (Fourth Chamber) of 30 May 2013, *European Commission v. Sweden*, C-185/09 and C-270/11, ECLI:EU:C:2013:339.

[67] Judgment of the Federal Constitutional Court of Germany, 2 March 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08.

[68] C-329/12 Commission v. Germany, withdrawn after the case Digital Rights Ireland.

Supreme Administrative Court,[69] the Romanian Constitutional Court,[70] the Cypriot Supreme Court,[71] and the Czech Constitutional Court.[72]

The *Digital Rights Ireland* judgment, leading to the annulment of the Directive, marked the end of the existing EU data retention framework. However, it left the door open as to the impact of the judgment on domestic legal orders, thus leading to a first type of fragmentation. The Court failed to clarify whether the transposing national laws had to be declared invalid (or not), or whether they had to be set aside.[73] Thus, the judgment from the outset created uncertainty that paved the way for more preliminary references to come but also fed the 'politics of interpretation' by domestic actors (governments, parliaments and courts), leading to 'conflicts' between powers of the state.[74] This uncertainty translated into fragmentation in the readings of the judgment across Member States. Some governments, for example, interpreted the judgment in a lenient manner, assessing their national law in compliance with the judgment, allegedly thanks to stronger guarantees and safeguards than within the Directive. This was the case of the Danish government for example, which stated that it would probably propose a revision of the law.[75] The Dutch government, similarly, deemed that the case did not have a direct impact on the existing national legislation.[76] Interestingly, this position has been challenged by Privacy First and other associations before the Tribunal of The Hague, which struck down the law in 2015.[77] In other countries, the lenient reading of the judgment has been upheld by courts: it is the case of the Italian Supreme Court, which will be examined in more detail later. In contrast to this approach, minimizing the consequences of the judgment, in other

[69] Bulgarian Supreme Administrative Court, Decision No. 13627, 11 December 2008.

[70] The first Romanian data retention law (298/2008) was declared unconstitutional by Romanian Constitutional Court decision No. 1258/2009. Subsequently, a second law No. 82/2012 was held unconstitutional by decision no. 440 of 8 July 2014.

[71] Cyprus Supreme Court (Civil applications 65/2009, 78/2009, 82/2009 and 15/2010–22/2010).

[72] Pavel Molek, 'Czech Constitutional Court Unconstitutionality of the Czech Implementation of the Data

Retention Directive; Decision of 22 March 2011, Pl.U S 24/10', *European Constitutional Law Review*, 2012, pp. 348–49.

[73] See Luisa Marin, 'The fate of the Data Retention Directive, cit., p. 220.

[74] Niklas Vainio, Samuli Miettinen, Telecommunications data retention after *Digital Rights Ireland*: legislative and judicial reactions in the Member States, *International Journal of Law and Information Technology*, 2015, 290-309.

[75] 'Notat om betydningen af EU-Domstolens dom af 8 april 2014 i de forenede sager C-293/12 og C-594/

12 (om logningsdirektivet) for de danske logningsregler' 2 June 2014, referred in Niklas Vainio, Samuli Miettinen, Telecommunications data retention after Digital Rights Ireland, cit., p. 306.

[76] 'Reactie van het kabinet naar aanleiding van de ongeldigverklaring van de richtlijn dataretentie'

17 November 2014; available at https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vjp2eocx4zwl?ctx=vhqn8x5wcqzv&s0e=vhdubxdwqrzw; for a comment, see https://www.bitsoffreedom.nl/2014/12/16/dutch-government-lets-keep-data-retention-mostly-unchanged/

[77] Judgment of the Tribunal of the Hague of the 11 of March 2015, available https://tweakers.net/files/upload/uitspraak-WBT.pdf and also https://edri.org/our-work/dutch-data-retention-law-struck-down-for-now/

Member States higher courts annulled their transposing law. This path has been followed notably in Austria by a ruling from the Constitutional Court that essentially stated that massive surveillance cannot pertain to a democratic society.[78] Similarly, Slovakia and Slovenia annulled their laws, on the grounds of an infringement with the ECHR,[79] and on the infringement of the principle of proportionality.[80] Pursuant to this, many other Member States opted for annulment (for example Romania, Poland, Bulgaria, Portugal and Belgium).

Thus, the data retention directive and its subsequent annulment in the *Digital Rights Ireland* case caused fragmentation with regards the diverse reactions it brought. While some Member States and national courts were eager to follow the path taken by the Court of Justice with the annulment, others deemed their laws in compliance with the requirements of the Court. Furthermore, others preferred to further engage in dialogue with the Court of Justice, raising new preliminary references which have prompted the abundant case law on the topic.

3.2. Strategic personalization as second-level fragmentation: the reactions to *La Quadrature du Net*

The fragmentation went a step further and appeared in the subsequent case law adopted by the Court after *Digital Rights Ireland*. Thus, while fragmentation already existed, it further exacerbated with the divergent interpretations of the different preliminary references brought to the Court.

To illustrate this idea of fragmentation in the implementation of a judgment, *La Quadrature du Net* provides the best example.[81] The final decision of the Court of Justice was interpreted differently by the referring courts in Belgium and in France, two countries that essentially share the same legal culture. On the one hand, the Belgian Constitutional Court quasi-automatically overturned the national data retention law in question and followed the reasoning of the Court of Luxembourg in stating that generalized data retention should be an exception and not a norm in a state's activities.[82] On the other hand, the French *Conseil d'Etat* (Higher administrative court) took another route. It not only refrained from annulling the national law, but even personalized the Court of Justice's decision.[83] In other words, the higher French administrative court engaged in a process of strategic personalization. Indeed, the *Conseil d'État* required the lawmakers to add a procedural safeguard in the law, namely the introduction within six months of regular monitoring by the Government to control the persistent existence of a national security threat. This should reconcile the national legislation with EU law. In addition, it stated that France is still facing constant and genuine terrorist threats, since

[78] Austrian Constitutional Court, Decision G 47/2012-49, *Seitlinger and others*, 27 June 2014.

[79] Constitutional Court of Slovakia (Grand Chamber), judgment of April 2015, (PL. S 10/2014) 94.

[80] Constitutional Court of the Republic of Slovenia, judgement U-I-65/13-19 of 3 July 2014.

[81] Judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others,* C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791.

[82] Cour Constitutionnelle de Belgique, Communiqué de presse Arrêt 57/2021 (22 April 2021).

[83] For example, the Conseil reinterpreted national security to include economic espionage, drug trafficking or the organization of undeclared demonstrations. Marcin Rojszczak, 'National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts' [2021] *European Constitutional Law Review* 17.

the adoption of the law after the Charlie Hebdo attack.[84] This is highly problematic since the state of emergency should supposedly not last for several years. France thus threatens to establish a permanent restriction of fundamental rights, and a more lenient approach to data retention under the pretext of combatting a persistent terrorist threat.[85] The French approach highlights the issue of feasibility and practical implications of Luxembourg's decisions. The *Conseil d'État*, like other courts and law enforcement authorities, pointed out that targeted retention is in practice ineffective for identifying new threats, since it is impossible to determine *a priori* whether an offense will be committed, where and by whom.[86] Through the personalization of the Court of Justice's case law, the French administrative High Court claims to provide a concrete solution to the difficult balance between national security and fundamental rights.[87]

Even if subsequent preliminary references have been raised by domestic interpreters, to further clarify the requirements of the Court, a second level of fragmentation has appeared, resulting from their reception (and interpretations) of the same rulings. On the one hand, we observe a case of devoted compliance, in the Belgian case. On the other hand, there is a case of strategic personalization with France. This seems to question the effectiveness of the choice of the Court of Justice, which engaged in a process of active specification and definition of the requirements of a data retention legal framework compliant with data protection and privacy. All these 'requirements' must be respected and implemented by domestic actors, which might however be embedded in political, legal and operational contexts having strong preferences for other options, different from the ones expressed by the Court. This activism of the Court of Justice can be represented as a device that, once set in motion, continues in perpetual motion. This leads us to the third level of fragmentation, to which the next section is devoted.

3.3. Silent stillness as an escape from EU law: the example of Italy

If the Court of Justice is on a path of perpetual motion, in contrast, some states are in a situation of stillness. Italy failed to amend domestic laws to comply with the criteria set down by the Court of Justice in its case law. If we add that neither the Commission made a move toward sanctioning this inaction, the picture is particularly worrisome. This represents a tolerated escape from correct enforcement of EU law.

The example of Italy perfectly illustrates this point. In Italy, the national data retention law is the Privacy Code,[88] which was reformed in 2017 by Law 167. The latter extended the retention of metadata to a maximum time limit of 72 months (6 years), which goes way beyond the maximum retention time of 2 years permitted by the annulled Directive. This law clearly conflicts with the *Digital Rights Ireland* ruling, which prohibits generalized data retention: the Italian law indicates a long list of crimes allowing retention of traffic data, in contrast to the case law of the Court. The Italian Supreme Court (*Corte di cassazione*), however, on several

[84] On 7 January 2015 the premises of the French satirical newspaper *Charlie Hebdo* in Paris have been under attack by two brothers linked to al-Qaeda.

[85] Marcin Rojszczak, 'The uncertain future of data retention laws in the EU: Is a legislative reset possible?' [2021] Computer Law & Security Review 41.

[86] Conseil d'État 21 April 2021, Case 393099, ECLI:FR:CEASS:2021:393099.20210421, para. 54.

[87] Arianna Vedaschi, '"Customizing" *La Quadrature du Net*: The French Council of State, National Security and Data Retention' (2021) Bridgenetwork < https://bridgenetwork.eu/2021/05/05/customizing-la-quadrature-du-net-the-french-council-of-state-national-security-and-data-retention/ >, accessed 10 December 2021.

[88] Decreto Legislativo 30 giugno 2003, n. 196, Art. 132.

occasions declared that the Italian legislation was proportionate and in compliance with the principles stated by the Court of Justice in its case law.[89] According to the Italian court, the law temporarily limits the length of retention and ensures a check on its necessity by a judicial authority, the public prosecutor. After the judgment in the *H.K. Prokuratuur* case, the check by the public prosecutor represented another point of friction with the EU law. This case clarifies that access to and utilization of traffic data in criminal proceedings must be limited to serious crimes or serious threats to public security, and, additionally, must be scrutinized by a judicial authority which is independent from the authority requesting the access and that this decision must be given after a request by the requesting authority. Thus, the Italian law was not in compliance with the Court of Justice's case law due to the 72-months retention limit, the scope of retention, and the supervising authority.

The European Parliament was informed about the loophole represented by the Italian case and raised the issue with the Commission.[90] However, as expressly stated by Commissioner Avramopoulos in March 2018, the Commission has opted for a wait-and-see approach, not taking up its role of guardian of the treaties.[91] Instead, the Commission recalled that it is up to the domestic Data Protection Authorities (DPAs) and courts to ensure the correct application of data protection rules, including the case law of the Court. On the national side, the Italian DPA (*Garante per la Protezione dei dati personali*) raised these points in several opinions, inviting the legislator to pass the necessary domestic reforms.[92] However, the Italian legislator took a selective approach and chose strategically what to reform. For example, the maximum conservation period has not been amended, nor the scope of the conservation, which is possible for a broad list of crimes.[93] In contrast, it decided to amend the supervision procedure, with the Law Decree of 30 September 2021, No. 132, converted into Law by Parliament.[94]

Overall, it is possible to conclude that, on the one side, the case law of the Court of Justice has designed a complex and detailed system of requirements and guarantees to ensure harmonious coexistence between privacy and surveillance; on the other side, its reception at domestic level reveals a fragmented picture of different positions, where the judgments of the Court are translated – and adapted – to the peculiarities of domestic realities. Our analysis has shown that fragmentation takes shape in different forms and levels. This shows a real gap in

[89] Italian Supreme Court (*Cassazione*), Sez. V, 24 aprile 2018, No. 273892 & Sez. III, 23 August 2019, No. 36380. The judgment *Cassazione*, Sez. II, 10.12.2020, No. 5741, reiterates this position referring to the CJEU's cases in Digital Rights Ireland and Tele 2/Watson.

[90] 'In 't Veld worried about new Italian telecommunications data retention period of 6 years' https://www.sophieintveld.eu/nl/in-t-veld-worried-about-new-italian-telecommunications-data-retention-period-of-6-years#_ftn2

[91] European Parliament, Answer given by Mr Avramopoulos on behalf of the Commission. Question reference: E-006966/2017, 16 March 2018.

[92] Garante per la protezione dei dati personali, Opinions No. 99/2018 and 312/2018, in: Newsletter No. 480 of 2.8.2021, titled: 'Segnalazione sulla disciplina della conservazione, a fine di giustizia, dei dati di traffico telefonico e telematico', at https://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9687860

[93] It should be recalled that for a category of crimes the maximum conservation period is 72 months. This list is also quite broad, as it comprises a defined list of crimes of serious social alarm, going from terrorism to organized crimes, to crimes against the public administration.

[94] Leonardo Filippi, 'La nuova disciplina dei tabulati: il commento "a caldo" del Prof. Filippi', *Penale: Diritto e Procedura*, 1.10.2021, at https://www.penaledp.it/la-nuova-disciplina-dei-tabulati-il-commento-a-caldo-del-prof-filippi/ .

the uniform and coherent enforcement of EU law, especially worrisome because of the inactive role taken by the Commission.

This fragmentation of national data retention laws and national interpretations of the Court of Justice's requirements creates a problematic situation within the EU. While data retention undoubtedly impacts fundamental rights and freedoms of individuals, particularly privacy, fragmentation brings an additional layer of issues. It brings legal uncertainty and differentiated treatments of data, belonging to individuals, which is problematic due to the cross-border nature of crimes. This shows that despite the existence and emergence of abundant case law and interpretations by the Court of Justice, its implementation at domestic level creates several difficulties, which domestic actors autonomously sort out using the toolkit they have. No consensus has been reached on standards for application of national retention rules.[95] While several criteria were developed by the Court of Justice, some Member States still fail as of today to adopt compatible data retention legislation. Interestingly, this has been the case of Belgium, which has continuously tried to develop a national data retention law in line with the European case law but has already failed to do so twice.[96] Alongside some questions about the legitimacy of the activism of the Court of Justice, it is essential for the EU to act at the political level to prevent further aggravation of this fragmentation. The next section will explore the legacy of this saga from a political perspective.

4. The impact of the data retention saga on the political debate

The data retention saga, developed in this chapter, played an essential role in the discussions and debate on the new recast of the e-Privacy directive and on a new data retention instrument. Before diving into the development of the new Regulation, it is worth noting that another political debate on Europol showed the clear eagerness of Member States to have data retention legislation.

4.1. A clear preference for data retention: the Europol big data saga

The Member States' shared preference for keeping data retention rules in place for the fight against crime was already visible at an early stage. In fact, while the Court of Justice repeatedly stated that general and indiscriminate retention of all traffic and location data is essentially precluded by EU law, some Member States seem to fully ignore this statement and continually attempt to find a way around it. France, for example, reintroduced mass data retention justifying it with a major terrorist threat.[97] Denmark also proposed a bill maintaining general and indiscriminate data retention.[98] Italy keeps a maximum retention period of 6 years. Finally, as the European Digital Rights network pointed out, even when national governments introduce

[95] Marcin Rojszczak, 'The uncertain future of data retention laws in the EU: Is a legislative reset possible?' [2021] Computer Law & Security Review 41.

[96] Chloé Berthélémy, 'New Belgian data retention law: a European blueprint?' (2021) EDRI < https://edri.org/our-work/new-belgian-data-retention-law-a-european-blueprint/ >, accessed 10 December 2021

[97] Loi n° 2021-998 du 39 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement.

[98] Chloé Berthélémy, 'Data Retention? Advocate General says "Asked and answered!"' (2021) EDRI < https://edri.org/our-work/data-retention-advocate-general-says-asked-and-answered/ > accessed 10 December 2021.

targeted retention schemes, they add an extensive list of criteria reducing the meaning of 'targeted retention'.[99]

This preference common to Member States to keep data retention for the fight against crime can be observed in the debate on the amendments to the Europol Regulation.[100] Europol has been the subject of a large and complex data sets saga, also called 'the Big Data challenge', since 2019.[101] The issue was that it came to light that Europol received and processed large data sets from several Member States that included data of individuals having no clear link to any criminal activity.[102] This was not allowed under the current Europol Regulation. After multiple exchanges between the European Data Protection Supervisor (EDPS) and Europol, some changes were made for the Agency to ensure compliance with data protection.[103] However, one issue remained unsolved and debated, namely the data retention period. Consequently, the EDPS adopted an order for Europol to ensure data subject categorization within six months for new datasets, and twelve months for existing datasets.[104] Without categorization, datasets must be deleted. The Member States, however, noted their support for data retention by adopting the provisional agreement on Europol's Regulation.[105] Despite this, the EDPS still adopted its decision and used its corrective powers, Member States and the Commission ignored it and agreed to grant an extended data retention period to Europol. Thus, Europol can take up to three years to categorize and process large and complex data sets sent by Member States. This is a way for Member States to be able to send data that they cannot legally retain in their Member States, due to the conditions imposed above all by the Court of Justice. They can circumvent the rules and Europol can still analyse and retain these datasets. This shows an eagerness of Member States to retain datasets, and a will for the European Commission to keep data retention on the agenda. In a different perspective, this stand is in line with the Commission's failure to initiate infringement procedures for non-compliance with data retention requirements laid down by the Court of Justice.

---

[99] Chloé Berthélémy, 'Data Retention? Advocate General says "Asked and answered!"' (2021) EDRI < https://edri.org/our-work/data-retention-advocate-general-says-asked-and-answered/ > accessed 10 December 2021.

[100] Conseil de l'UE, Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2016/794 en ce qui concerne la coopération d'Europol avec les parties privées, le traitement de données à caractère personnel par Europol à l'appui d'enquêtes pénales et le rôle d'Europol en matière de recherche et d'innovation (Confirmation du texte de compromis final en vue d'un accord) 5920/22 (9 février 2022) < https://data.consilium.europa.eu/doc/document/ST-5920-2022-INIT/x/pdf > (accessed 24 March 2022).

[101] Sarah Tas, 'Europol's 'Big Data Challenge': A Neutralisation of the European Watchdog', in *Digicon* < https://digi-con.org/europols-big-data-challenge-a-neutralisation-of-the-european-watchdog/ > (accessed 21 February 2022).

[102] Luca Bertuzzi, 'EU watchdog orders Europol to delete personal data unrelated to crimes', in *Euractiv* < https://www.euractiv.com/section/data-protection/news/eu-watchdog-orders-europol-to-delete-personal-data-unrelated-to-crimes/ > (accessed 24 March 2022).

[103] Notably after the admonishment of the EDPS, 'EDPS Decision on the own-initiative inquiry on Europol's big data challenge' (18 September 2020), < https://edps.europa.eu/sites/edp/files/publication/20-09-18_edps_decision_on_the_own_initiative_inquiry_on_europols_big_data_challenge_en.pdf > (accessed 24 March 2022).

[104] EDPS, EDPS Decision on retention by Europol of datasets lacking Data Subject Categorization (Cases 2019-0370 & 2021-0669), in < https://edps.europa.eu/system/files/2022-01/22-01-10-edps-decision-europol_en.pdf > (accessed 24 March 2022)

[105] Council of the EU, 'Europol: provisional agreement between the Council presidency and the European Parliament on the agency's new mandate' (2022) Press Release.

These long-standing discussions on data retention show that it is a very complex topic, and careful consideration is needed for all the interests of the actors concerned. As Eurojust pointed out, data retention schemes are a necessary tool to fight serious crime, but they need to be balanced with sufficient safeguards, such as the ones developed by the Court of Justice.[106] It is therefore essential to pursue work on legislative instruments to develop and agree upon common standards for retention provisions.

4.2. The complex road to development of new data retention instruments

Having learned from the Europol datasets case that data retention is an instrument valued by Member States, it remains to be seen if and how the legislator is considering the pursuit of legislative reforms, after the annulment of the Directive. In this connection, two developments can be observed: first, the recast of the e-Privacy Directive, and second, the discussion on new data retention legislation.

Nowadays, the e-Privacy Directive is going through a process of recast. The Directive is twenty years old and is not up to date with the changes introduced by the Treaty of Lisbon and the current regulatory models of the telecommunications market.[107] Work on the Regulation gained importance in 2016, with the development of the Data Protection Package,[108] and a first draft was presented in 2017. The proposal faced numerous objections by Member States, and amendments were added, such as the possibility for Member States to provide for a longer period of metadata retention than that resulting from the general rules. The proposal was blocked in the Council for four years.[109] The Council finally agreed on a negotiating mandate in February 2021, after eight Council presidencies, and the trilogue negotiation started in May 2021.[110] The agreed text contained changes from the initial Commission's proposal of 2017, and notably included rules on data retention.[111] The compromise draft from the Council excludes the collection and processing of metadata from the scope of the Regulation when the activities even indirectly relate to national security, and provides for possibilities to retain traffic and location data as a preventive measure.[112]

---

[106] FRA, Data retention across the EU (2017), < https://fra.europa.eu/en/publication/2017/data-retention-across-eu > (accessed 24 March 2022).

[107] Marcin Rojszczak, 'The uncertain future of data retention laws in the EU: Is a legislative reset possible?' [2021] Computer Law & Security Review 41

[108] Notably the General Data Protection Regulation and the Law enforcement Directive

[109] Thomas Wahl, 'Council Agrees on Negotiating Mandate for e-Privacy Regulation – Data Retention Included', *EUcrim* (2021) < https://eucrim.eu/news/council-agrees-on-negotiating-mandate-for-e-privacy-regulation-data-retention-included/ > (accessed 4 March 2022).

[110] Benedikt Gollatz, 'Data retention, location data, cookie banners : the ePrivacy Regulation is coming' (2021) *EDRI* < https://edri.org/our-work/data-retention-location-data-cookie-banners-the-eprivacy-regulation-is-coming/ > (accessed 4 march 2021).

[111] Council of the European Union, document No. 6087/21 of 10 February 2021, concerning Proposal for a Regulation of the European Parliament and of the Council concerning respect for private life and protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Mandate for negotiations with EP.

[112] Art. 7(4) of the Council Proposal for a Regulation of the European Parliament and of the Council concerning respect for private life and protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation of Privacy and Electronic Communications) – Mandate for negotiations with EP 6087/21.

This aspect was deleted by the Portuguese Council Presidency and has been seen as highly problematic by the European Data Protection Board.[113] In fact, the Regulation should not deviate from the Court of Justice's case law and should be compatible with the EU Charter of Fundamental Rights. This compromise and the two changes brought to it go against the previously discussed Court of Justice rulings, which precludes legislative measures that provide for general and indiscriminate retention of traffic and location data as a preventive measure. The adoption is still under discussions and will not be an easy process. While the trilogue began in May 2021, and some progress was made under the French and Czech Council Presidency, notably on the technical level, the Regulation sits on stand-by. This is not expected to change under the current Spanish Council Presidency, as they do not consider it a priority file.[114] The focus has now essentially shifted to the Artificial Intelligence Act, the Digital Service Act and the Digital Market Act. What is clear is that the new regulation needs to tackle the open questions and practical impediments regarding implementation of the current conditions, which does not seem to be currently happening. Furthermore, the case law of the Court seems to have left an important heritage that Member States might want to discuss again. It is interesting to note that in adopting this compromise draft agreement, Member States tried to influence the outcome of the new legal instrument. In this regard, France strongly pushed for an amendment aiming to exclude collection and processing of metadata from the scope of the Regulation, when the activities relate even indirectly to national security and defence. In *La Quadrature du Net* the Court has recalled that activities undertaken by telecommunications companies in data retention do not fulfil national security tasks. In light of this decision, the French preference is not surprising. The Court of Luxembourg critically evaluated the French data retention law, and the *Conseil d'Etat* did not fully welcome that decision. France, through this amendment, tried to render the Court of Justice's judgment invalid.[115] At the same time, as already shown by the case law of the Court, the Court might find it easy to set boundaries to the national security exception, and regain some control over the topic, as it has already done so before.

In 2021 other options were discussed by the European Commission on the way forwards on the data retention debate. A 'non-paper on the way forward on data retention' prepared by the Commission's staff but not officially approved as the Commission's position showed three possible policy routes:[116] 1) no EU initiative; 2) guidance at EU level (non-binding guidelines from the Commission) and 3) legislation at EU level (new proposal on data retention). Interestingly, the first option is a release of a competence field back to the Member States, which would also keep the control on implementation of the Court of Justice' judgments at national level. This would be a continuation of the *status quo*, and the Commission would play a supporting role and function as a facilitator. This seems to be the way the Commission interprets its role also with regard to the implementation of the case law of the Court. In its second approach the Commission would adopt a non-binding recommendation, which would

[113] EDPB Statement 03/2021 on the e-Privacy Regulation of 9 March 2021

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

[115] Marcin Rojszczak, 'The uncertain future of data retention laws in the EU: Is a legislative reset possible?' [2021] Computer Law & Security Review 41.

[116] European Commission, 'Non-paper on the way forward on data retention – Presentation by the Commission and exchange of views', WK 7294/2021 INIT, Brussels, 10 June 2021.

have the advantage of the flexibility desired by Member States, and the disadvantage of poor harmonization. The third approach would consist in integrating the case law of the Court of Justice into a binding legislative instrument, and here the matter is indeed how much of this rich saga can be accepted by the legislator and translated into a legal instrument, which can be comprehensive to different extents, depending on the political agreement of the states. Interestingly, in this proposal the Commission includes over-the-top communication providers, such as WhatsApp, Telegram and Skype, which increases the scope of the new instrument, since these companies collect more data for business than traditional operators.[117] What emerges from this non-paper is that the policy options on the table are many, and that if a legislative instrument is proposed, it will have to consider the matrix of cases and typologies of data created by the Court with several layers of cases, next to the web of requirements and guarantees specified by the Court. This amounts to a rich legacy that is going to constrain the political debate and to some extent, might also hinder it.

5. Conclusions: the data retention saga as a validation of the axiom 'less is more'?

The chapter has provided a panoramic overview of the core episodes of the data retention saga, covering a period of eight years after the judgment that annulled the DRD. Since then, the legislator has not adopted a new instrument, nor has the Commission made a proposal. Instead, the Court of Justice has been urged to provide clarifications by national courts, activated by companies, private and associated privacy activists. Curiously enough, the richness of the case law did not answer all the questions, and as we are publishing this research, new cases are arising. This means that the Court does not clarify all the issues, because many questions and answers are intertwined with domestic legislations and competences, such as the concept of serious crime.

If one of the merits of the case law of the Court is a European doctrine on the balance between privacy and surveillance, and the fortification of fundamental rights against misuse by private and public powers in the digital era, the ramifications of this case law touch upon criminal justice systems and national security, which are sensitive for its domestic implications, and to some extent remain outside the scope of EU law. Furthermore, at the global stage, the *Digital Rights Ireland* case has paved the way for the extraterritorial effect of the European data protection legislation,[118] which has materialized, among other developments, with the *Schrems* cases and Opinion 1/15 on the EU-Canada PNR.[119] All in all, the Court of Justice has

[117] This non-paper puts forward five categories of retention, from generalized traffic retention data for national security purposes, the exception carved out in *La Quadrature du Net*, to targeted data retention of traffic and location data for serious crimes and serious threats to public security, expression of *Tele 2*, to be declined as geographical targeting and targeting of specific categories of persons, thus ranging as far as the less intrusive option of the generalized retention options, of IP addresses and civil identity data.

[118] Marise Cremona, Joanne Scott, 'Introduction', in Marise Cremona and Joanne Scott (eds), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (OUP, 2019). On the influence of *Digital Rights Ireland* on *Schrems I*, see Luisa Marin, 'The fate of the Data Retention Directive', cit.

[119] Judgment of the Court (Grand Chamber) of 6 October 2015, Maximillian Schrems v Data Protection Commissioner (Schrems I), Case C-362/14, ECLI:EU:C:2015:650; Opinion of the Court (Grand Chamber) of 26 July 2017, Case Opinion 1/15, ECLI:EU:C:2016:656; Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (Schrems III), Case C-311/18, ECLI:EU:C:2020:559.

contributed to setting the EU as an actor at the global stage,[120] also thanks to its case law on data retention.

The chapter has shown that this case law has been incorporated into the legislations of the Member States in different manners, thus feeding a process of politics of interpretation. Uncertainty and fragmentation have been observed, at many levels. The most worrisome implication is a process of selective reception enacted by domestic courts, or strategic personalization of the judgments of the Court, depending on domestic situations and preferences. All in all, one can reasonably ask whether the axiom of architectural minimalism 'less is more' might be transposable to this situation. In a more constitutional perspective, it looks as if the Court has stepped into the shoes of the legislator, since the construction of the typologies of data and situations for retention, the reason for the richness of this case law, is typical of a process of creation of law, rather than interpretation.[121] This doctrine certainly represents a legacy for the European legislator but might be of hindrance to the process of research of a new agreement, matching commonly shared domestic preferences on data retention. Interestingly, it has been shown that one of the options put on the table by the Commission, in an internal document, is to refrain from proposing a new European legislative instrument, thus releasing back to the Member States a field of competence, or instead leaving it to be regulated through the e-Privacy Directive, which has been under reform for about five years. In a more constructive perspective, the significance of the data retention saga might provide the boundaries of future exploitations of AI and machine learning techniques for policing, currently debated.[122]

[120] The literature is vaste. For some references, see Anu Bradford, Brussels Effect: How the European Union Rules the World, OUP, 2020; Marise Cremona and Joanne Scott (eds), EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law (OUP, 2019); Elaine Fahey, The Global Reach of EU law (Routledge, 2016).

[121] For a similar but more nuanced criticism, see Giulia Formici, La data retention saga al capolinea? Le ultime pronunce della CGUE in materia di conservazione dei metadati per scopi securitari, tra conferme e nuove aperture. *DPCE Online*, [S.l.], v. 46, n. 1, apr. 2021, p. 1363.

[122] Gloria GONZÁLEZ FUSTER, 'Artificial Intelligence and Law Enforcement: Impact on Fundamental Rights', Study requested by LIBE Committee, European Parliament, 2020.