Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

The uncertain future of data retention laws in the EU: Is a legislative reset possible?

*Marcin Rojszczak**

Faculty of Administration and Social Sciences, Warsaw University of Technology, Warsaw, Poland

ARTICLE INFO

Keywords:
General obligation to retain data
e-privacy regulation
Data protection
National security

ABSTRACT

The article discusses the CJEU's most important case law, including interpretations presented in recent cases relating to data retention for both national security purposes (Privacy International, La Quadrature du Net) and the fight against serious crime (H.K). The analysis is a starting point for discussing the draft e-Privacy Regulation, in particular a controversial proposal introduced by the EU Council that may limit the Court's jurisdiction in cases involving data retention rules that cover state security.

Negotiated over the past five years, the draft e-Privacy Regulation fleshes out EU data protection rules governing electronic communication services. As a result, the way in which obligations under the Regulation are defined is critical in setting a standard for retention rules consistent with CJEU case law for decades to come. At the same time, succumbing to pressure from Member States may have the opposite result – the emergence of new ambiguities concerning not only the admissibility of data retention but also the competence of EU institutions to regulate this area of the telecommunications sector.

1. Introduction

More than fifteen years after the adoption of Directive 2006/24 (the Data Retention Directive) ,[1] seven years after it was declared incompatible with EU law[2] and after a total of six precedent-setting judgments handed down by the CJEU to clarify the criteria for assessing domestic data retention provisions, the issue of the admissibility of a general data retention obligation and its compatibility with human rights standards continues to be the subject of much debate and controversy.[3]

The history of this dispute shows not only how the understanding of the need to protect individuals against modern forms of electronic surveillance has changed over the years, but also ideas about technical measures necessary to ensure public security. When the Court of Justice first examined the

E-mail address: marcin.rojszczak@pw.edu.pl
* ORCiD: 0000-0003-2037-4301.

[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 communication services or of public communication networks and amending Directive 2002/58/EC, OJ of 2006 L 105, pp. 54-63; act repealed.

[2] CJEU, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland (2014) EU:C:2014:238 ('DRI').

[3] It should be remembered, however, that doubts about the legality of this measure have not only been voiced in the EU. The problem has also been discussed in other democracies, such as the United States or Australia. *See e.g.* R Clarke, 'Data Retention as Mass Surveillance: The Need for an Evaluative Framework' (2015) 5 International Data Privacy Law 121; Catherine Crump, 'Data Retention: Privacy, Anonymity, and Accountability Online' (2003) 56 Stanford Law Review 191.

https://doi.org/10.1016/j.clsr.2021.105572

compatibility of the Data Retention Directive with EU law in 2010, it was less about the admissibility of a general obligation to retain data and more about whether the EU legislature, in adopting the Directive, had exceeded the scope of competences conferred on it by the Treaties.[4] It was only in subsequent decisions that the Court assessed the proportionality and admissibility of the measure, taking into account the requirements of respect for fundamental rights.[5]

With the entry into force of the Lisbon Treaty,[6] the interpretative context of data retention provisions has changed considerably. Apart from giving the Charter of Fundamental Rights force equal to primary law, a separate treaty provision was introduced covering personal data protection. The division into three pillars of European integration was abolished in favour of a single concept of the European Union – one having its own a legal personality and competencies, and which included the area of criminal cooperation. At the same time, Member States decided to extend the national identity clause by explicitly granting themselves exclusive competences in the area of national security. As a result, EU data retention rules, which were initially justified by the need to ensure coherence of the internal market, also had to be examined for their compatibility with fundamental rights. Furthermore, the entry into force of the Lisbon reform extended the Court of Justice' ability to scrutinise national retention laws, both in terms of the compatibility with EU law of procedures for the collection of data originating from electronic communication, and the subsequent accessing of such data by public authorities for general security purposes.

The Court of Justice has issued three important judgments in recent months, in each of which once again expressing its opinion on the admissibility of different forms of data retention in the national laws of Member States. In the *Privacy International*[7] and *La Quadrature du Net* (LQN)[8] judgments, the Court addressed the long-debated problem of the legality of establishing a general obligation to retain data for national security purposes. In turn, in the *H.K.*[9] case, it clarified the conditions for applying targeted retention and also explained the effects of a breach of fundamental rights from the perspective of criminal proceedings. Both issues are not only of fundamental importance for understanding the limits to national data retention rules, they also contribute significantly to the development of a European standard for the protection of individuals against modern forms of electronic surveillance.

Regardless of the Court's evolving case law in the area of data retention, work has continued for years to amend Directive 2002/58 (e-Privacy Directive, ePD)[10] – a legal act underpinning EU regulations protecting the privacy of electronic communication service users. The Directive has also introduced provisions limiting individuals rights – including telecommunications secrecy – on the basis of which national retention laws have been adopted. However, the ePD is almost 20 years old, has not taken into account changes resulting from the Lisbon reform, and has therefore not adapted to the current regulatory model of the telecommunications market. In recent years, the EU legislature has reformed both rules protecting personal data (GDPR[11]) and those established in the area of electronic communications (EECC[12]). Though the ePD links these regulations, the Directive itself has still not been modernised, despite being in force almost unchanged since 2002 – which, in practice, creates additional difficulty in analysing the EU legal framework for data retention.

Work on a new e-Privacy Regulation (EPR) to replace the ePD gained momentum in 2016, after the content of the GDPR was agreed.[13] However, it was not until February 2021 that a consensus was reached in the Council on the draft Regulation.[14] The ePR's agreed text contains several significant changes to the draft presented by the Commission in 2017,[15] including rules on data retention. In particular, they aim to exclude the collection and processing of electronic communication metadata from the scope of the Regulation if these activities relate even indirectly to national security. This amendment should exclude the CJEU from assessing the legality of data retention procedures and access to such data by Member States' secret services. The measure, promoted by France[16] amongst others, in fact seeks to render obsolete part of the CJEU's case law, including that presented in the *LQN* judgement, in which the Court of Justice critically assessed French retention laws. The Council's draft of the ePR is therefore an

[4] CJEU, C-301/06, Ireland v Parliament and Council (2010) EU:C:2009:68.

[5] For the first time, the Court addressed the proportionality of general data retention in the *Digital Rights Ireland* case (*see* n 2).

[6] Treaty of Lisbon, amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, OJ of 2007 C 306, pp. 1-271.

[7] CJEU, Case C-623/17, Privacy International (2020) EU:C:2020:790.

[8] CJEU, Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others (2020) EU:C:2020:791.

[9] CJEU, Case C-746/18, H.K. (2021) EU:C:2021:152.

[10] 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), OJ of 2002 L 201, pp. 37-47.

[11] 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), OJ of 2016 L 119, p 1.

[12] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, OJ of 2018 L 321, pp 36–214.

[13] *See* the EC draft of the EPR: '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)', European Commission 10 January 2017, COM(2017) 10 final.

[14] 'Confidentiality of electronic communications: Council agrees its position on ePrivacy rules', Council of the European Union Press Release (10 February 2021), <https://cli.re/kpaMaw> accessed 20 April 2021.

[15] *See* the Council's final draft of the ePR adopted by the Permanent Representative Committee on 10 February 2021, 6087/21, <https://cli.re/3oRd3b> accessed 20 April 2021.

[16] Theodore Christakis and Kenneth Propp, 'How Europe's Intelligence Services Aim to Avoid the EU's Highest Court—and What It Means for the United States' [2021] Lawfare <https://www.lawfareblog.com/how-europes-intelligence-services-aim-avoid-eus-highest-court-and-what-it-means-united-states> accessed 21 April 2021.

example of Member States attempting to invalidate a CJEU ruling unfavourable to them by changing the provisions that constitute its basis.

The aim of this article is to discuss the current EU standard for assessing national retention laws, including interpretations presented in the *Privacy International, LQN* and *H.K.* judgments. Against this background, changes proposed to the draft e-Privacy Regulation and agreed by the Council will also be cited. Discussion of these amendments will focus on two areas – data retention applicable to criminal procedure, and in pursuing national security objectives. While it is clear that the draft ePR is not final and may be subject to further change, the aim of this analysis will be to consider whether the Council's proposal might indeed significantly affect the scope of application of EU law and the relevance of the Court's assessment of national retention laws.

2. Different dimensions of data retention

In principle, data retention relates to telecommunications law and concerns the obligation to retain so-called metadata, i.e. data covering the use of services other than the substantive content of transmissions. In the case of voice services, *metadata* consist of traffic data, such as information allowing identification of the communicating parties, the time of connection or its duration. In practice, *traffic data* is also a term used to refer to other electronic communication services, such as e-mail, VoIP or instant messaging. With these services, however, it can be much more difficult to separate metadata from message content because the same information, depending on the context, can either complement the message content (and therefore be included in the metadata) or actually be the message content itself.[17]

Data retention obligation is generally imposed on providers of electronic communication services – in most cases telecommunication operators. These providers are obliged, under relevant national legislation, to collect certain categories of metadata for a specific period (usually between 12 and 24 months[18]) and to make this data available on request to authorised public authorities (law enforcement or secret services).

Based on the scope of data collected, retention can be divided into bulk (generalised) or targeted. The first type – referred to as general data retention – involves collecting information on all users of electronic communication services, regardless of whether they are of any interest to public authorities. The indiscriminate nature of collecting such metadata, carried out without any real connection to public security, raises doubts as to whether such a measure can be reconciled with the principle of proportionality. The generalised nature of this type of retention is – in the opinion of its supporters – supposed to be a preventive measure, making it possible to analyse future threats and allow authorised authorities to counter the most serious crimes, including terrorism. Hence, it is often referred to as preventive retention. In this case, the procedures used to make the data available to authorities are of particular importance. Overly flexible rules, lacking rigorous oversight, including that exercised by courts, increase the risk of abuse of power and arbitrariness in the use of surveillance measures. Therefore, when evaluating regulations in the field of data retention, it is important to determine not only the scope of the data retention imposed on telecommunications operators, but also how the law regulates access to such data. An extreme example in this regard is legislation currently in force in Poland – where access to metadata is via dedicated IT systems made available by telecommunications operators to law enforcement agencies and security services, and which operate without any external control nor any real possibility of a court questioning the legality of actions taken.[19]

Data retention as a mechanism for collecting information on individuals is also used in the area of individual surveillance. In this case, only data on an individual or a group of individuals are collected. The way in which targeted retention is carried out varies between Member States and depends on the specific provisions of criminal procedure. Targeted retention is thus one surveillance measure used with people suspected of certain types of offences, usually classified as serious crime.

General and targeted retention differ not only in the scope and modalities of data provision but also in the different areas of state activity that use such measures. While targeted retention is usually associated with criminal law, general retention is seen as dedicated to state security purposes. In reality, of course, this division is a simplification, and in practice – in those countries where general data retention still applies – is used not only by security services but also by law enforcement agencies.[20] The importance of generalised retention for the early identification of serious threats to public security is strongly emphasised by the secret services.[21]

The attempt to separately define retention provisions in the area of combating crime and pursuing national security goals is made additionally difficult by the fact that these two areas of state activity largely overlap. While there is no doubt

[17] An example is information about a user's geolocation – information which can be attached to other data (metadata) or *per se* be the content of the communication.

[18] Article 6 of the Data Retention Directive states that the retention period should not be shorter than six months or longer than 24 months. National legislatures have adopted different retention periods; for example, in Poland and France, it is 12 months, but in Italy – 30 months. *See* Article 180(a) of the Polish Telecommunications Law of 16 April 2004 (the 'Telecommunications Act'); Article R10-13(I) of the French Postal and Electronic Communications Code (the 'Code des postes et des communications électroniques'); Article 132 of the Italian Data Protection Code (Decreto Legislativo 30 giugno 2003, n. 196).

[19] Marcin Rojszczak, 'Surveillance, Legal Restraints and Dismantling Democracy: Lessons from Poland' (2021) 17 Democracy and Security 1.

[20] For example, Europol argues that targeted data retention is in fact impossible to implement, as the potential significance of the captured metadata cannot be predicted in advance. As a result, the Agency's proposal is to base the future retention framework on bulk collection supplemented with a limited data retention regime. *See* 'Proportionate data retention for law enforcement purposes,' Europol (21 September 2017), WK 9957/2017 INIT, p. 14-15.

[21] *See e.g.* the position presented by Michael V. Hayden, former director of the NSA, regarding the usefulness of communications gathered through mass surveillance programs operated by the Agency in: Michael Vincent Hayden, *Playing to the Edge: American Intelligence in the Age of Terror* (Penguin Press 2016) 83.

that, for example, the foreign intelligence or gathering information relevant to the economic interests of the state are not linked to those concerning criminal law, the fight against terrorism is a task carried out by both law enforcement authorities (criminal procedure) and security services (national security). Furthermore, the legislation of some Member States also gives national intelligence services powers to conduct criminal proceedings.[22] As a result, the same body has competence in the area of state security objectives, as well as in the fight against crime. In this case, an attempt to introduce a general obligation to retain data only in the area of national security, without reforming the structure of secret services at the same time (that is, removing their competence to conduct criminal investigations), would be fraught with a significant risk of abuse of power.

In the past decade, the problem of the admissibility of data retention and its compatibility with EU law has been analysed in relation to both general and targeted retention, used to fight t serious crime and for national security purposes. Therefore, with the EU legal model, retention of electronic metadata should not be seen as a single measure but rather as a set of measures with different specific rules on data collection and sharing – and, as a result, differently integrated into the right to privacy of electronic communication users.

3. General data retention after the privacy international and LQN rulings

The issue of the compatibility of a general data retention obligation with EU law was first addressed by the Court of Justice back in 2010, following an action brought by Ireland, which sought to annul the Data Retention Directive on the grounds that it had been adopted on the basis of an incorrect rule of competence.[23] Ireland, supported by Slovenia, argued that data retention was not, in fact, a measure relating to the harmonisation of the internal market but rather a measure concerning cooperation in criminal matters, and that, as a consequence, incorrect legal procedures had been used in adopting the Directive, thus rendering it invalid. However, the Court did not accept this argumentation. Significantly, it pointed out that the mere collection of data – without reference to the way in which they are used — is "closely linked to the exercise of the commercial activity of the service providers" and therefore has no connection with tasks carried out by Member States.[24] This is an important conclusion, as it demonstrates that, in the Court's opinion, retention legislation should be assessed in two areas: rules for collecting and storing data, and the way they are made available and subsequently used by authorised entities.[25]

Directive 2006/24 provided for a general obligation for data retention, i.e. the retention of all traffic and location data of all users of all electronic communication services provided within the EU. The information collected was to be used in the fight against crime. In this regard, the Data Retention Directive referred to the criterion of "*serious crime*", a term not defined in EU law at that time.[26] This is important because Article 15(1) of the ePD (that still forms the basis of national retention laws) does not limit the establishment of data retention measures exclusively to cases of combatting serious crime, but to all criminal offences.

The wide scope of the data retention obligation under the Data Retention Directive raised serious concerns about its compliance with the principle of proportionality. These doubts led the Court of Justice to issue a judgement in the *Digital Rights Ireland* (DRI) case, in which the Court ruled for the first time on the incompatibility of a general data retention obligation with EU law. The Court stressed that respect for fundamental rights – in particular the right to privacy and the right to protection of personal data – requires that derogations must be limited to what is strictly necessary.[27] This requirement cannot be met by a measure which permanently and generally restricts the right to privacy of all electronic communication users, and which lacks any real connection to public security objectives.[28] In conclusion, the Court held that the Data Retention Directive, because it breached the principle of proportionality, could not be reconciled with the overriding norms of EU law and was therefore invalid.[29]

Though the Court's decision effectively abrogated the contested Directive, it was beyond the Court's jurisdiction to annul any national legislation based on it. In effect, the *Digital Rights Ireland* judgement did not result in a repealing of the general obligation to retain data introduced by Member States. Moreover, it was not clear whether, in its argumenta-

[22] For example, the powers of the Polish Internal Security Agency (*Agencja Bezpieczeństwa Wewnętrznego*) combine competences in the areas of crime prevention and state security. In the case of Austria, similar powers have been granted to the Office for the Protection of the Constitution and Counterterrorism (*Bundesamt für Verfassungsschutz und Terrorismusbekämpfung*).

[23] *See* n 4.

[24] *See* n 4, para. 82.

[25] *See also* the reasoning presented by the Court in Opinion 1/15 (EU:C:2017:592, para 124): „the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental right enshrined in Article 7 of the Charter, whatever the subsequent use of the information communicated. The same is true of the retention of personal data and access to that data with a view to its use by public authorities"

[26] Art. 83(1) of the TFEU introduces the term "particularly serious crime" and defines the areas in which the Union has competence to approximate substantive criminal law. This provision, however, does not contain a definition or a closed list of acts that can be classified as "serious crime". Valsamis Mitsilegas, *EU Criminal Law after Lisbon: Rights, Trust and the Transformation of Justice in Europe* (Hart Publishing 2018).

[27] *Digital Rights Ireland* case, n 2, para. 52.

[28] *Digital Rights Ireland* case, n 2, paras. 57-59.

[29] In particular, the Court pointed out that the general data retention obligation led to disproportionate interference with the right to privacy and the protection of personal data - and thus did not comply with the principle of proportionality (Art. 52(1) of the Charter). However, the Court also found that the Data Retention Directive did not affect the essence of the right to privacy and personal data, as the processing of metadata did not allow access to the content of electronic communications. For a more extensive discussion of the judgment see: Niklas Vainio and Samuli Miettinen, Telecommunications Data Retention after *Digital Rights Ireland* : Legislative and Judicial Reactions in the Member States' (2015) 23 International Journal of Law and Information Technology 290.

tion, the Court had in fact ruled on the incompatibility of all forms of generalised data retention with EU law. It was possible to take the view that the *DRI* judgement concerned only the obligation to retain data as provided for in the Data Retention Directive.

These doubts led to further preliminary questions and the judgement in the *Tele2 Sverige* case, in which the CJEU found that national provisions introducing a generalised data retention obligation in relation to all users and all means of electronic communication could not be reconciled with EU law.[30] In doing so, it settled the dispute as to whether a measure such as a generalised data retention obligation could be reconciled with the obligation to respect the rights guaranteed by the Charter of Fundamental Rights.[31]

In both the *DRI* and *Tele2 Sverige* cases, the Court examined legislation enacted for the purpose of combatting serious crime. Against this background, it held that the lack of a link between the extent of the data retained and the need arising from ongoing criminal proceedings meant that generalised data retention "exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society."[32] However, this interpretation did not explicitly refer to retention rules applicable in the area of state security.

In principle, the area of national security is excluded from the scope of EU law. This exclusion stems directly from Art. 4(2) of the TEU, and is further reiterated in Art. 1(3) of Directive 2002/58. Moreover, the competence of the CJEU in matters concerning not only national security but also public order and internal security has been considerably limited by treaties, and does not include, inter alia, control of the validity or proportionality of actions taken by law enforcement authorities.[33]

At the same time, however, in Art. 15(1) of the ePD, the EU legislature introduced limitations on the establishment of domestic data retention programmes introduced to combat crime and for national security purposes. Doubts therefore arose about the possibility of a concurrent application of Article 15(1) of the ePD, with regard to data retention rules concerning national security, when Article 1(3) of the ePD explicitly excluded this area from the scope of the Directive. The problem boiled down to presenting an interpretation of EU law which, while preserving the limitations arising from the national security clause, would not completely deprive Article 15(1) of the ePR of its effectiveness. These doubts were the reason why the Belgian,[34] French[35] and British[36] courts decided to request a preliminary ruling from the CJEU.

In its judgments of 6 October 2020 in the *Privacy International* and *LQN*[37] cases, the Court clarified that, in principle, the activities of Member States' public authorities in the area of national security were excluded from the scope of EU law, and thus the provisions of Directive 2002/58, concerning the legality of national retention legislation, did not apply either.[38] At the same time, however, the Court pointed out that "the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law."[39] In doing so, the Court emphasised that the criteria for the lawfulness of actions taken by secret services pursuing national security objectives, including those concerning the interception of electronic communications – as excluded from EU law – are to be assessed solely on the basis of their compatibility with the national law of a given Member State. However, when national law imposes an obligation to retain data on private entities (such as telecommunications providers) – the admissibility of such a measure must be assessed also in the context of the overriding norms of EU law.[40] In this case, the binding interpretation of the Charter of Fundamental Rights resulting from the case law of the CJEU should also be applied.

The Court thus shared the opinion expressed by the Advocate General[41] that, as a matter of principle, the national security clause determines the exclusive competences of states and may be used as a basis for excluding EU law as long as it concerns activities undertaken directly by public authorities.[42] The Court recalled that, in its judgement in the *Tele2 Sverige* case, it had already found that a different interpretation, leading to the conclusion that the national security clause covered all activities, including those indirectly motivated by state security objectives, would render Article 15(1) of the ePD superfluous, which clearly could not be reconciled with the principle of effectiveness of EU law (*effet utile*).[43]

Data retention conducted by private entities is not a national security activity, and thus provisions establishing a general data retention obligation cannot be regarded as excluded from the scope of application of EU law. In turn, finding that data retention laws – including those used for national security purposes – are not excluded from the scope of EU law, led

[30] CJEU, Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB (2016) EU:C:2016:970, para. 103.

[31] For a broader discussion of the implications of the *Tele2 Sverige* judgment, see: Anja Møller Pedersen, Henrik Udsen and Søren Sandfeld Jakobsen, 'Data Retention in Europe-the Tele 2 Case and Beyond' (2018) 8 International Data Privacy Law 160, 2.

[32] *Tele2 Sverige* case, n 30, para 107.

[33] *See* Art. 276 of the TFEU. More about the jurisdiction of the Court of Justice after the Lisbon Treaty in: Koen Lenaerts, 'Challenges Facing the European Court of Justice after the Treaty of Lisbon' (2010) 2 Analele Universitatii din Bucuresti: Seria Drept 1.

[34] *See* the request for a preliminary ruling of 2 August 2018 referred by the Cour constitutionnelle (Belgium), C-520/18, <https://cli.re/B333Dq> accessed 20 April 2021.

[35] *See* the request for a preliminary ruling of 3 August 2018 referred by the Conseil d'État (France), C-511/18, <https://cli.re/rw383k> accessed 20 April 2021.

[36] *See* the request for a preliminary ruling of 31 October 2017 referred by the Investigatory Powers Tribunal (United Kingdom), C-623/17, <https://cli.re/KaaV9R> accessed 20 April 2021.

[37] *See* n 7 and 8.

[38] *LQN* case, n 8, para 103.

[39] *LQN* case, n 8, para 99.

[40] *Privacy International* case, n 7, para 49.

[41] Opinion of Advocate General delivered on 15 January 2020, Joined Cases C–511/18 and C–512/18, EU:C:2020:6, para. 79.

[42] *LQN* case, n 8, para 103.

[43] *Tele2 Sverige* case, n 30, para 73.

to an assessment of their proportionality according to the criteria defined by the Court in previous cases, including *DRI* and *Tele2 Sverige*.

In carrying out this assessment, the Court first noted that "the transmission of traffic data and location data to a third party constitutes interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, regardless of how that data is subsequently used."[44] At the same time, it confirmed that the pursuit of national security objectives may justify the adoption of measures leading to a more far-reaching interference with fundamental rights than measures relating to the fight against crime.[45] That interference cannot, however, be without any real connection to the objective pursued by its introduction.[46] In particular, it cannot be considered necessary to introduce a generalised and indiscriminate measure that consists of making traffic and location data relating to all persons using electronic communication services available to security services where there is no relation, even an indirect one, to the attainment of national security objectives. Such a measure cannot be considered proportionate, which inevitably leads to the conclusion that it "exceeds the limits of what is strictly necessary."[47] As a result, in the *Privacy International* and *LQN* judgments, the Court ruled that the application of a bulk data retention obligation was inadmissible — even if the information thus collected is intended, but not required, by the security services to pursue national security objectives.[48]

4. Access to retained data after the H.K. ruling

Although the issue of retaining telecommunications data is usually discussed in the context of indiscriminate data retention, one should not forget the Court's position regarding the conditions for targeted retention. In this case, the purpose is not to preventively analyse all available data but to obtain information concerning specific persons or groups of persons of interest to the authorities.

Already in the *Tele2 Sverige* case, the Court had ruled that, in principle, it was permissible for states to use targeted retention, provided that it did not exceed what was strictly necessary in a democratic state.[49] Compliance with this condition requires adapting current categories of data recorded, the methods of their collection, the duration of storage and the rules of access to the actual needs of the criminal proceedings or the objectives of general prevention. Here the Court referred to the rich ECtHR jurisprudence, which contains a set of minimum legal safeguards to be applied to electronic surveillance by public authorities. The CJEU also stressed the necessity of using retained data only for combatting serious crime and only after a prior judicial review.[50]

The restriction on using retention only when combatting *serious* crime does not explicitly follow on from the provisions of Directive 2002/58 or from the Charter of Fundamental Rights. In fact, the condition was introduced by the Data Retention Directive, but, at the time of the *Tele2 Sverige* judgement, the instrument was no longer part of the EU legal order. The need to limit the obligation to retain data only to cases of combatting serious crime follows from an interpretation of the principle of proportionality. In the Court's view, in light of the scale of interference with fundamental rights inherent in national legislation providing for the mandatory retention of traffic and location data, such a measure satisfies the condition of proportionality only if it is used to combat crimes regarded as *serious*.[51]

In addition, the requirement that access to retained data must receive prior (*ex-ante*) authorisation by a court or an independent administrative authority does not derive directly from statutory law. Both Article 16(1) of the TFEU and Article 8(3) of the Charter show that an inherent component of the right to data protection is the establishment of an independent supervisory authority. However, these standards do not demand that any interference with the right to data protection is preceded by a prior judicial review. Nor does ECtHR case law – which sets a minimum standard for the interpretation of the EU right to privacy – contain such a requirement.[52] Indeed, in its case law the Strasbourg Court permits the application of *ex-post* oversight, provided that it is of a random nature.[53]

However, the conditions governing targeted retention set out in the *Tele2 Sverige* case did raise questions of interpretation. In particular, it was not clear whether the required link with serious crime excluded the possibility of using metadata in cases relating to minor offences. These interpretations were clarified in the *Ministerio Fiscal* judgement, in which the Court inferred that respect for the principle of proportionality required that the criterion of serious crime be mandatory in all cases where access to retained data makes it possible to reach precise conclusions concerning the private lives of the data subjects.[54] Conversely, any processing of information which does not reveal details of a subject's private life – such as data enabling the subscriber of a particular telecommunication service to be identified – does not lead to a serious interference with the right to privacy, and it is therefore not necessary in such a case to limit the application of the measure solely to cases involving the fight against serious crime.[55]

[44] *Privacy International* case, n 7, para 70.
[45] *Privacy International* case, n 7, para 75.
[46] *LQN* case, n 8, paras 131-132.
[47] *Privacy International* case, n 7, para 81.
[48] A broader discussion of the *Privacy International* and *LQN* judgments can be found in: Xavier Tracol, 'The Two Judgments of the European Court of Justice in the Four Cases of Privacy International, La Quadrature Du Net and Others, French Data Network and Others and Ordre Des Barreaux Francophones et Germanophone and Others: The Grand Chamber Is Trying Hard to Square the Circle of Data Retention' (2021) 41 Computer Law & Security Review 105540.
[49] *Tele2 Sverige* case, n 30, para 108.
[50] *Tele2 Sverige* case, n 30, para 125.
[51] *Tele2 Sverige* case, n 30, para 114; also CJEU, Case C-207/16, Ministerio Fiscal (2018) EU:C:2018:788, para. 56.
[52] Art. 52(3) of the Charter.
[53] ECtHR, Appl. 37138/14, Szabó and Vissy v. Hungary (2016), para. 77.
[54] CJEU, Case C-207/16, Ministerio Fiscal (2018) EU:C:2018:788, paras. 58-60.
[55] Analysis of the *Ministerio Fiscal* case in: Christopher Docksey, '*Ministerio Fiscal* : Holding the Line on EPrivacy: Case C-207/16 *Ministerio Fiscal*, EU:C:2018:788.' (2019) 26 Maastricht Journal of European and Comparative Law 585.

In principle, the reasoning presented above is also valid when pursuing state security objectives. While the Court stressed that the specific nature of threats to national security may justify the adoption of measures leading to a more far-reaching interference with fundamental rights than measures related to the fight against crime, this cannot justify any infringement of the principle of proportionality. Therefore, also with regard to the pursuit of state security objectives, "the national legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to (…) to contribute (…) to preventing a serious risk to public security."[56]

By contrast, in the *H.K.* judgement, issued in March 2021, the Court ruled on the consequences of providing access to retained data in a way that violated fundamental rights guaranteed under EU law. The background to the case was Estonian legislation that made it possible for a prosecutor to access metadata.[57] In the legal model being examined, the prosecutor's office has investigative powers and is thus an active participant in criminal proceedings, rather than an independent arbiter who would uphold individual rights by resolving doubts as to the need for surveillance measures. As a result, the Court held that the prosecutor's control over the use of surveillance measures did not meet the criterion of independence and could not therefore replace the supervision exercised by the court. Moreover, the Court stated that this lack of independent control could not be remedied 'after the fact' by later oversight, conducted during judicial proceedings. In the Court's view, "such subsequent review would not enable the objective of a prior review, consisting in preventing the authorisation of access to the data in question that exceeds what is strictly necessary, to be met."[58]

The *H.K.* judgement also set a precedent for another reason. The Court addressed the possible consequences of using faulty evidence in criminal proceedings, including evidence obtained in a way that violates procedural requirements. Since EU law does not include provisions that harmonise rules for dealing with evidence obtained through generalised and indiscriminate data retention, it is up to national law to determine the conditions for its admissibility before the courts. In laying down these rules, the national legislature must seek "to prevent information and evidence obtained unlawfully from unduly prejudicing a person who is suspected of having committed criminal offences."[59] In the Court's view, a way to achieve this goal may be not only to impose wrongfully collected evidence as inadmissible but also to assess the weight of such defective evidence in ongoing proceedings, and during sentencing. Significantly, however, according to the Court, the principle of effectiveness of EU law "requires national criminal courts to disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law or by means of access of the competent authority thereto in breach of EU law" if suspects are not given the opportunity to challenge the evidence thus gathered.[60]

The fact remains that the general obligation to retain data is still applied by some Member States to collect information for the purpose of criminal proceedings.[61] The interpretation set out in the *H.K.* case demonstrates that the continued failure of domestic legislatures to adopt retention laws not only breaches the overarching standards of EU law, but also has implications for criminal proceedings, as evidence gathered from generalised data retention, being unlawfully collected, should be assessed at the stage of judicial proceedings.

5. Member states' pressure and the draft e-Privacy regulation

In parallel to the development of the Court of Justice standard in data retention, the EU legislature worked on agreeing the content of a new e-Privacy Regulation (EPR). The new Regulation was to replace Directive 2002/58 and adjust the model of privacy protection in telecommunication services to amended regulations on personal data protection and the new regulatory model for electronic communication services. The first draft of the Regulation was presented by the Commission back in 2017 with the expectation that its content could be quickly agreed and approved so that the ePR would come into force at the same time as the GDPR, i.e. in May 2018. However, it turned out that this was too ambitious a goal and that such a fast pace was impossible, given the numerous objections to individual elements of the proposed Regulation subsequently raised by Member States.

One element of the proposed e-Privacy Regulation are the boundary conditions for introducing national retention laws. Data retention, being a measure that interferes with the right to privacy, is a derogation from telecommunications secrecy. In the Commission's 2017 draft, this aspect of the Regulation was not made more specific in relation to the current text of Directive 2002/58. The Commission, in the draft's explanatory memorandum, stressed that the proposed form of Article 11 of the ePR was based on Article 15 of the ePD and, as such, created a general legal framework for the adoption of national retention rules. Thus, the Commission's draft reproduced the regulatory model adopted in the Directive and provided that national data retention rules could be adopted on the condition that they complied with EU law, and after taking into account the jurisprudence of the CJEU. It is worth noting that already at this (initial) stage of legislative work, the Commission's draft was referring to Art. 23(1) of the GDPR in terms of defining general security objectives justifying the introduction of limitations to rights and the obligations of electronic communication services. In principle, these restrictions could be imposed in the area of fighting crime (Art. 23(1)(d) of the GDPR), pursuing national security objectives (Art. 23(1)(a) of the GDPR) and defence (Art. 23(1)(b) of the GDPR). The legal

[56] *Tele2 Sverige* case, n 30, para. 111; also n 7, para 147.
[57] Factual background of the case in: Ioannis Revolidis, 'H.K. v Prokuratuur: On Balancing Crime Investigation and Data Protection (C-746/18 H.K. v Prokuratuur, Opinion of AG Pirtuzzella)' (2020) 6 European Data Protection Law Review 319.
[58] *H.K.* case, n 9, para. 58.
[59] *H.K.* case, n 9, para. 43.
[60] *H.K.* case, n 9, para. 44.
[61] 'National Data Retention Laws since the CJEU's Tele-2/Watson Judgment', Privacy International (September 2017), < https://cli.re/qDAEDp> accessed on 20 April 2021.

framework for retention contained in the Commission's draft of the new Regulation was therefore almost identical to the one in force under Directive 2002/58.

During initial discussion in the Council, some Member States raised concerns about the overly restrictive nature of the proposed retention rules.[62] It was stated that the new draft Regulation reproduced ambiguities in the then current Directive – in particular, those concerning interpretation of the derogation clause proposed in Article 11 of the ePR, which allowed the establishment of data retention rules for national security purposes at the same time as, under Article 2 of the ePR, national security tasks were excluded from the scope of the Regulation altogether. Moreover, it was pointed out that the Regulation – as *lex specialis* in relation to GDPR – should wholly regulate the processing of personal data in the field of electronic communication services. Therefore, in the opinion of the Member States, it was necessary to supplement the draft with a formal basis for processing retained data, which would be equivalent to the legal grounds for processing personal data enshrined in Article 6 of GDPR. It was also argued that the general nature of retention regulations proposed by the Commission could lead to more restrictive rules for data retention than those resulting from the current regulations – whereas the expectation of most Member States was that greater flexibility would be granted in regulating this matter in domestic law.

This discussion led to the first set of amendments to the draft Regulation – clarifying that service providers may process any metadata necessary to ensure compliance with national retention regulations (Article 6(1)(d)) and explaining that Union or Member State law may provide for a longer period of metadata retention than that resulting from the general rules (Article 7(4)). The Council also decided to modify the derogation clause in Article 11 by deleting the reference to the pursuit of national security and defence purposes from the catalogue of grounds justifying the introduction of data retention measures. The intention was to ensure that the legality criteria set out in Article 11 would not provide a standard of review for the evaluation of national retention provisions established in the field of state security. Although the Council was aware that some of the changes introduced might be questioned in terms of their compatibility with CJEU case law at the time, it was expected that the Court would clarify the conditions for targeted retention in subsequent judgments – so that the provisions adopted in the Regulation could provide a basis for more extensive retention provisions than was possible at the time of their adoption (the "*leaving the door open*" strategy).[63]

At the same time, more detailed rules for data retention were discussed. The limiting of categories of collected data, specifying principles of access to them and the introduction of a new legal instrument – Renewable Retention Warrants – were all analysed.[64] However, this work did not result in the formation of a common position in the Council.

By contrast, the CJEU's judgments in the *Privacy International* and *LQN* cases had the effect of reducing, rather than loosening, national data retention rules. As a result, it became obvious that trying to establish a general framework for data retention in the form proposed by the Council could lead to a challenge of the new Regulation's compliance with requirements arising from the Charter of Fundamental Rights. For this reason, the German Presidency decided to refer the text of the Regulation for further consultation, deleting changes that had been previously introduced (in particular Articles 6(1)(d) and 7(4)) and adhering to the general content of Article 11 – as originally proposed by the Commission.[65]

Such a proposal was not, however, satisfactory to all Member States. In particular, according to media reports, France threatened not to adopt the draft Regulation if the amendments to completely exclude its application in the area of pursuing national security objectives were not taken into account. Subsequent discussions in the Council saw a common position agreed on and a mandate given for negotiations on the draft act with the European Parliament.

The text of the Regulation agreed upon by the Council not only reinstated detailed provisions on data retention rules (Art. 6(1)(d) and Art. 7(4), discussed earlier) but also introduced another significant change. In Article 2(2) of the draft – which defines the substantive scope of the Regulation – the scope of exemption of activities not covered by EU law was extended. The new wording of the provision states that the Regulation does not apply to any measures, processing activities and operations concerning national security and defence, regardless of who undertakes them – in particular, whether or not it is a public entity or a private entity acting on behalf of the public entity. The amended text of Article 2(2) is clearly intended to exclude retention rules established in the area of national security from the scope of the Regulation. It is quite obvious that it would thus render the interpretation of the Court presented in the *Privacy International* and *LQN* cases irrelevant. This, according to media reports, is the actual goal of France, dissatisfied with the direction the Court's evolving case law is taking, which – in its view – is encroaching on an area of competence reserved for Member States.[66]

As a result, the five-year-long discussion on the shape of the future e-Privacy legislation gained new momentum just at the end of the Council's work on it. The proposed scope of the Regulation gave rise to discussion not only about the need for a general obligation of data retention in the legal orders of the Member States but, above all, about the possibility and legitimacy of the European legislature influencing the effec-

[62] 'Contributions by delegations on processing and storage of data in the context of the draft of ePrivacy Regulation', Council of the European Union (15 September 2017), WK 9374/2017 rev 1.

[63] *See* 'The issue of data retention in the proposal for ePrivacy Regulation - discussion paper', Council of the European Union (14 February 2019), 6358/19, p. 2. The lack of success in formulating a position acceptable to all Council members is best summarised by the following conclusion: *'After two years of work in the DAPIX Working Party, no solution has yet been found on how to implement a targeted/restricted retention' (ibid.*, p. 3).

[64] 'Data retention - State of play', Council of the European Union (23 November 2018), 14319/18.

[65] Draft of the ePR issued by the German Presidency on 4 November 2020, 9931/20, <https://cli.re/xmPxkN> accessed on 20 April 2021, p. 3.

[66] *See* n 16.

tiveness of the Court's case law by changing secondary legislation. These issues are particularly important, bearing in mind the fact that the Court's landmark judgements on data retention are based mainly on an assessment of the compatibility of the regulations under examination with the Charter of Fundamental Rights – which, since the Lisbon reform, has become part of EU primary law.

6. Implications of the adoption of the council draft for national retention legislation

To assess whether adopting the Regulation proposed by the Council will limit the Court of Justice's jurisdiction and thus effectively deprive data retention case law of its effectiveness, one must first recall the position of e-privacy regulations in the EU legal model.

The ePR – as explicitly stated in the GDPR[67] and also pointed out during the Council's work[68] – is *lex specialis* in the area of the privacy of electronic communication service users. With the entry into force of the ePR, this Regulation will become the exclusive basis for the processing of personal data in relation to telecommunication services. According to the principles of legal interpretation, a specific norm constitutes an exclusive regulation to the extent that its provisions cannot be reconciled with general provisions (in this case – with the GDPR). To the extent that the detailed norm does not contain regulations introduced in the general norm, the general norm should be applied. The principle of *lex specialis derogat legi generali* should be applied as long as the detailed provisions contain other – different – regulations from the provisions of the general act. Transferring these considerations to the proposed e-Privacy Regulation – which introduces an exemption covering all activities undertaken in the area of national security, including those performed by private entities – one can conclude that it will not have the effect intended by its authors. The result will not be the exclusion of such activities from the scope of EU law, but only their exclusion from the scope of the e-Privacy Regulation. It will still be possible to evaluate these activities according to the provisions defined in the *lex generali* – which, in this case, is the GDPR.[69] This is because the retention of telecommunications data constitutes a data processing activity,[70] and entities carrying out this processing (telecommunications operators) are covered by the scope of application of the GDPR. In practice, therefore, if the ePR as proposed by the Council is adopted, the Court will be ruling on the compatibility of retention provisions with Article 23 of the GDPR rather than with Article 11 of the ePR.[71] Given the almost identical wording of these clauses, the amendment to the draft ePR should therefore not limit the Court's competence in the area of testing the compatibility of national data retention measures with EU law.[72]

Regardless of the above, the very construction of the exemption proposed in Art. 2(2) raises doubts about its internal consistency. The Council draft states that the scope of the exemption should cover all "measures, processing activities and operations concerning national security and defence, regardless of who is carrying out those activities". In accordance with not only the literal wording of Art. 4(2) of the TEU but also the CJEU's interpretation in, amongst others, the *Privacy International* case, activities concerning national security fall within the exclusive competence of Member States. At the same time, however, the Court noted that activities undertaken by private entities (in this case – telecommunication operators) in performance of data retention obligations do not fulfil national security tasks. Of course, it is possible to argue that the phrase "processing activities and operations concerning national security" should be interpreted differently from how it is in the *Privacy International* judgement and to conclude that the retention of data by telecommunications providers is part of a state's national security activities that are excluded from the EU law. It should be borne in mind, however, that the Court has held on several occasions that invoking the public security clause does not exclude judicial review of such an exclusion's validity and that, "although it is for Member States to take the appropriate measures to ensure their internal and external security, the mere fact that a decision concerns state security cannot result in European Union law being inapplicable."[73] Irrespective of the literal wording of the EPR, it will ultimately be up to the CJEU to decide whether the provision introduced by the Council actually has the effect of precluding any assessment of the compatibility of national provisions laying down a generalised data retention obligation with overriding norms under EU law. It is difficult to conclude that, in the event of such an assessment, the CJEU will not apply its interpretation of EU law as set out in previous judgments.

Member States interested in excluding (or limiting) EU competences in the area of data retention should thus make an effort to amend the EU's primary laws. It is the Treaties that define EU competences, which, according to the principle of conferral, set the limits for the Union's action. This way

[67] *See* recital 173 of the GDPR (n 11).

[68] *See* n 63, p. 3: "By virtue of to the *lex generalis - lex specialis* relationship between the GDPR and the ePrivacy Regulation, it means that, for matters specifically governed by the ePrivacy Regulation, it should apply instead of the GDPR provisions."

[69] This conclusion is also supported by Article 95 of the GDPR, according to which the Data Protection Regulation does not impose additional obligations on providers of electronic communications services to the extent that such providers are subject to specific obligations under the e-privacy legislation.

[70] *Digital Rights Ireland* case, n 2, para 29: "retention of data also falls under Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, therefore, necessarily has to satisfy the data protection requirements arising from that article".

[71] Art. 23(1) of the GDPR – like Art. 11(1) of the ePR – also requires that national measures interfering with fundamental rights not only be proportionate but also respect the essence of these rights. Therefore, the GDPR enshrines in this regard the requirement arising also from Art.52(1) of the Charter. 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' (2019) 20 German Law Journal 864.

[72] The European Data Protection Board presents a similar conclusion in its position paper: 'Statement 03/2021 on the ePrivacy Regulation', European Data Protection Board (9 March 2021), <https://cli.re/qD3YxV> accessed 21 April 2021.

[73] CJEU, Case C-300/11, ZZ (2013) EU:C:2013:363, para. 38.

of amending EU competences also follows directly from the Declaration annexed to the Lisbon Treaty.[74]

The adoption of regulations specific to the telecommunications sector – being an essential part of the internal market – is a competence shared between the EU and Member States. There is no doubt that the introduction of data retention measures constitutes an interference with the general principles of providing services in the telecommunications market. As early as 2010, the Court ruled that the Data Retention Directive served to harmonise the internal market and, consequently, its adoption on the basis of rules on economic cooperation had not infringed the Treaties. This interpretation remains valid, and although today's draft ePR also pursues objectives relating to the protection of personal data, without doubt the Lisbon reform has not had the effect of limiting the EU's competence to regulate the rules of the telecoms market.

In accordance with the principle of loyal cooperation, Member States should refrain from taking any action – including legislative – that could jeopardize the attainment of the Union's objectives.[75] The entry into force of the ePR as proposed by the Council could be considered a discontinuation of the exercise of EU competences – and therefore, under Article 2(2) of the TFEU, lead to the exclusive power of Member States to regulate data retention rules applicable in the area of national security.[76] However, even if that argumentation is be found to be correct, the power to adopt regulations at a national level is not tantamount to the freedom to shape them. It follows from the Court's established case law that, in the absence of EU legislation, it is for the domestic legal order of each Member State to lay down rules ensuring the protection of rights derived from EU legislation – but in such a way that they do not render the exercise of these rights impossible or excessively difficult in practice.[77]

Furthermore, it must be borne in mind that the Court has mainly used the provisions of the Charter of Fundamental Rights as a standard of review in cases involving data retention legislation. The Charter has the same force as the Treaties in the EU legal model.[78] Additionally, both the fundamental rights that are subject to limitation as a result of the introduction of the obligation to retain data (the right to privacy and the right to protection of personal data) and the conditions of permissible interference with these rights (the principles of proportionality and necessity) derive directly from the Charter. To that extent, Article 15(1) of the ePD, which is of concern to Member States, simply reiterates principles already arising from primary law rather than creating them.[79] This means that even the deletion of Article 11 of the ePR (which is the counterpart of Article 15(1) of the ePD) or excluding the application of the entire new e-Privacy Regulation in general will not in any way affect the interpretation of the principle of proportionality or the limits of protection of individual rights that the Court has established based on the interpretation of the Charter. This opinion is also shared by the Commission, according to which the introduction of changes to the draft ePR may – contrary to the expectations of the authors of the proposed amendments – lead to the strengthening of the position of the CJEU based on the Charter.[80] The Court has repeatedly pointed out that the powers of public authorities face an insurmountable barrier, namely the fundamental rights of individuals.[81] In this respect, it is also worth recalling the apt observation by Koen Lenaerts, who pointed out that, in light of the provisions of the Charter, "a measure that compromises the essence of a fundamental right is automatically disproportionate."[82]

It seems that the Council, by adopting the draft Regulation, also lost sight of the positions expressed by other courts that have had an impact on the legal order of Member States. Although, in recent years, the case law of the ECtHR seems to have had less influence on the application of domestic electronic surveillance measures, it would be a mistake to assume that in the Strasbourg Court's opinion, states have unfettered freedom to adopt surveillance laws for national security purposes. As a matter of law, the ECtHR allows states a wider margin of appreciation in matters of national security,[83] but this does not mean that in such cases it is permissible to depart from the principle of proportionality or strict necessity.[84]

The issue of admissibility of data retention has also been examined by the constitutional courts of Member States. In many cases, the assessment of the constitutionality of the contested provisions resulted in their withdrawal from the national legal order.[85] In the case of some Member States, such judgments were delivered even before the ruling in *Digital Rights Ireland*. In those instances, the CJEU's interpretation of EU law was therefore not decisive in recognising the incom-

[74] *See* the text of Declaration No. 18 in relation to the delimitation of competences annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, OJ of 2008 C 115, pp. 1–388.

[75] Art. 4(3) of the TEU; more on the principle of loyalty in: Marcus Klamert, *The Principle of Loyalty in EU Law* (First edition, Oxford University Press 2014). It should be noted, however, that the principle of loyal cooperation is also binding in the area of police and judicial cooperation in criminal matters (C-105/03, EU:C:2005:386, para. 42).

[76] *See also* Declaration No. 18 in relation to the delimitation of competences (n 74): „[This] situation arises when the relevant EU institutions decide to repeal a legislative act, in particular better to ensure constant respect for the principles of subsidiarity and proportionality".

[77] *See e.g.* CJEU, Case C-69/14, Târșia (2015) EU:C:2015:662, para. 26; CJEU, Case C-752/18, Deutsche Umwelthilfe eV (2019) EU:C:2019:1114, para. 33.

[78] *Digital Rights Ireland* case, n 2, para. 31.

[79] *See e.g.* CJEU, Case C-58/08, Vodafone (2010) EU:C:2010:321, para. 51, in which the Court recalled that the principle of proportionality is one of the fundamental principles of EU law. The Court applied the principle of proportionality also to measures used in the area of national security – *see* CJEU, Case C–601/15 PPU, J.N. (2016) EU:C:2016:84, paras. 53-55.

[80] 'Informal Outcome of Proceedings of the informal VTC of the members of CATS on 8 February 2021', Council of the European Union (26 February 2021), WK 2732/2021 INIT, p. 4.

[81] *See* n 41, para. 132.

[82] Koen Lenaerts, 'Limits on Limitations: The Essence of Fundamental Rights in the EU' (2019) 20 German Law Journal 779.

[83] ECtHR, Appl. 54934/00, Weber and Saravia v. Germany (2006), para. 106.

[84] ECtHR, Appl. 47143/06, Roman Zakharov v. Russia (2015), para. 232.

[85] Marek Zubik, Jan Podkowik and Robert Rybski (eds), *European Constitutional Courts towards Data Retention Laws* (Springer, Cham 2021).

patibility of a general data retention obligation with the European standard of protection of human rights.[86]

The CJEU's interpretation of the permissible scope of interference in the area of fundamental rights guaranteed by the Charter is part of the European acquis, and it is hard to imagine that it will be disregarded in future rulings on the admissibility of data retention issued by both national constitutional courts and the ECtHR. Therefore, whatever the evolution of EU law, the incompatibility of a general obligation to retain data with the principles of necessity and proportionality has already been made sufficiently clear in the case law of the Court of Justice. For this reason alone, amending the scope of the Regulation, as proposed by the Council, so as to limit the Court's jurisdiction in cases involving national retention rules, is not only ineffective but also devoid of substance. The case law of the CJEU cannot be overturned by an amendment of secondary legislation, nor can its impact on the future shape of the European data protection model be diminished.

7. Summary and conclusions

Despite the clear position of the Court, it should not be thought that the problem of the admissibility of retention regulations has been finally clarified. One reason for the unflagging interest in the adoption of retention regulations is the conviction – expressed not only by a significant number of experts but also by the public – that such a measure is needed and is of vital importance for the implementation of basic tasks in the area of public security. There is no doubt that data retention is a useful tool which can provide valuable information to public authorities. However, the usefulness of a measure should in no way predetermine the necessity of its use.[87]

It is worth recalling in this context a report published by the Privacy and Civil Liberties Oversight Board, an independent body set up by the US Congress to oversee the use of powers by the secret services and to ensure that their actions do not violate fundamental rights. In its report, addressing the effectiveness of the general data retention obligation[88] being used by federal law enforcement agencies, the Board noted: "we have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack."[89]

One can, of course, trivialise these findings by saying that European secret services process metadata more efficiently than US agencies. However, if this is the case, any further discussion on the need for data retention should be preceded by adducing evidence that this measure is in fact effective – and thus necessary – in identifying previously unknown serious threats to public security. Understanding the reasons (based on verifiable data) why some governments are convinced of the need for indiscriminate data retention would certainly help to define its modalities in a way that takes into account the criteria presented in CJEU case law. Currently, the ongoing discussion has sharply polarised: on the one hand arguments are being advanced in favour of prohibiting any form of generalised data retention, and on the other, reasons presented for leaving the public authorities completely free to introduce retention laws. It is worth remembering that the Court of Justice has also indicated that it is possible to look for a compromise – introducing generalised forms of retention, but not going beyond what can be considered necessary in a democracy.[90]

Discussion on adopting EU data retention laws have resumed in recent months.[91] Such a need, debated in Council meetings, is another attempt to develop a common EU position on the application of data retention measures. Given the progressive globalisation of telecommunications services, thinking about mechanisms of obligatory data retention only in terms of national provisions seems to be unrealistic. At this very moment, millions of users Europe-wide are benefitting from modern telecommunication services, such as VoIP and

[86] In particular, the ruling of the German Federal Constitutional Court, pointing out the incompatibility of national retention laws with the Basic Law, was widely commented upon. However, similar conclusions were also reached by other constitutional courts, including those in Bulgaria and the Czech Republic, before the date of the ruling in *Digital Rights Ireland*. Discussion of the cited case law: Anna-Bettina Kaiser, 'German Federal Constitutional Court: German Data Retention Provisions Unconstitutional In Their Present Form; Decision of 2 March 2010, NJW 2010, p. 833.' (2010) 6 European Constitutional Law Review 503; Pavel Molek, 'Czech Constitutional Court. Unconstitutionality of the Czech Implementation of the Data Retention Directive; Decision of 22 March 2011, Pl. ÚS 24/10' (2012) 8 European Constitutional Law Review 338; Adrian Bannon, 'Romania Retrenches on Data Retention' (2010) 24 International Review of Law, Computers & Technology 145.

[87] The following observations formulated by Patrick Breyer lose nothing in this respect: "data retention can be expected to support the protection of individual rights only in a few, and generally less important, cases. A permanent, negative effect on crime levels, even in the field of cyber-crime, is not to be expected. The potential use of data retention in fighting organised crime and in preventing terrorist attacks is marginal or non-existent." Patrick Breyer, 'Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR' (2005) 11 European Law Journal 365.

[88] It should be remembered that, as a general rule, the concept of "*data retention*" in the sense given to the term in the EU is not used in federal law. The powers relating to the conduct of generalised metadata retention programmes were exercised on the basis of Section 215 of the USA PATRIOT Act of 2001, but the scope of data to be retained, the duration of data retention and the manner of processing were different (broader) than in Europe. *See more* Laura Donohue, 'Bulk Metadata Collection: Statutory and Constitutional Considerations' (2014) 37 Harvard Journal of Law and Public Policy 757.

[89] 'Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court', Privacy And Civil Liberties Oversight Board (23 January 2014), <https://cli.re/omAxva> accessed on 21 April 2021, 11. *Cf* testimonial of General Michael Hayden in n 21.

[90] *See* n 8, para 75: "Subject to meeting the other requirements laid down in Article 52(1) of the Charter, the objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives".

[91] *See* n 80, p. 3-4.

various online messengers, the provision of which is not restricted by national borders.

This makes all the more surprising the position of the French government, which, in parallel to the changes pushed for in the draft EPR, has taken steps to block the effectiveness of the *LQN* ruling in the national legal system. The *LQN* judgement was delivered in response to preliminary questions referred by the Conseil d'État, the highest French administrative court. Any interpretation of EU law provided by the Court of Justice must first enable the referring court to decide the national case in which the questions referred for a preliminary ruling were formulated. The French Government, envisaging the possibility of the Conseil d'État challenging the national retention rules as a result of the interpretation provided in the *LQN* case, objected that the Court of Justice was acting outside the scope of its powers under EU law.[92] The matter of *ultra vires* control has been widely commented on in recent years, mainly in connection with the judgement of the German Constitutional Court in the EU's Public Sector Purchase Programme case.[93]

However, in its April 2021 ruling, the Conseil d'État recognised that the EU Treaties do not confer on it the competence to challenge CJEU rulings, including whether the judgments of the Court of Justice contain a correct interpretation of EU law.[94] More significantly, however, the Conseil d'État made a very controversial interpretation of the *LQN* judgement, which led it to conclude that French data retention laws could be reconciled with EU law. The Council found that the conditions defined by the Court of Justice for introducing a general data retention obligation – relating to a "genuine and present or foreseeable"[95] threat to national security – had been met in France's case.[96] In the opinion of the Conseil d'État, such a threat existed and related to a terrorist threat that had already been in existence for years. The French Court also decided that, as other less invasive measures (e.g. targeted retention) did not allow the identification of unknown terrorist threats, using general data retention in pursuing national security objectives was a measure compatible with the principle of proportionality and necessity.

In its argumentation, the Conseil d'État therefore decided that the exception – that is, the application of any interference with fundamental rights - could become the norm. However, not only is such a concept not in line with the CJEU's position – as already expressed in the 2016 *Tele2 Sverige* case[97] – it is also threatening to establish a permanent restriction of fundamental rights under the pretext of combatting a persistent terrorist threat. It therefore raises concerns not only about proportionality, but also about respect for the very essence of the fundamental right to privacy.[98] Significantly, the day after the Conseil d'État delivered its judgement, the Belgian Constitutional Court – to which questions referred in the *LQN* judgement were also addressed – presented its position. It interpreted the position of the Court of Justice in a completely different way than the Conseil d'État. Indeed, in its assessment, the Cour constitutionnelle confirmed that data retention must be seen as an exception applicable only in strictly defined cases.[99] As a result, the Court invalidated the Belgian retention regime.

This means that, just two days apart, the highest national courts of two Member States came to fundamentally different conclusions interpreting the same judgement of the CJEU. This situation is the best illustration that, despite the existence of a clear interpretation of the Court of Justice, it is still not possible to say that a universally accepted standard for the application of national retention regulations has yet been established. For this reason alone, it seems necessary that the ongoing work on the ePrivacy Regulation strengthen the position expressed by the Court, the sources of which can be found in the Charter of Fundamental Rights and the constitutions of all Member States.

The development of the Digital Single Market must take into account the need to uphold public security objectives and support the national security efforts of Member States. However, this must not be to the detriment of the protection of fundamental rights. The right to privacy and secrecy of communication are foundations on which the European legal model has been built. Therefore, any attempt to circumvent or depart from these principles, including by seeking to lower the standard of protection arising from the Court of Justice case law, must arouse legitimate opposition.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

[92] 'France seeks to bypass EU top court on data retention', Politico (3 March 2021), <https://cli.re/RwEqKe> accessed on 21 April 2021.

[93] More on the *ultra vires* doctrine in context of the PSPP case in: Franz C Mayer, 'The Ultra Vires Ruling: Deconstructing the German Federal Constitutional Court's PSPP Decision of 5 May 2020' (2020) 16 European Constitutional Law Review 733; Mattias Wendel, 'Paradoxes of Ultra-Vires Review: A Critical Review of the PSPP Decision and Its Initial Reception' (2020) 21 German Law Journal 979.

[94] Conseil d'État 21 April 2021, Case 393099, ECLI:FR:CEASS:2021:393099.20210421, para. 6. *See also* J. Ziller, 'The Conseil d'Etat refuses to follow the Pied Piper of Karlsruhe', Verfassungsblog (26 Apr 2021), <https://cli.re/A41Nq3> accessed on 26 May 2021.

[95] *LQN* case, n 8, para. 177.

[96] Conseil d'État 21 April 2021, n 94, para. 30.

[97] *Tele2 Sverige* case, n 30, para. 104.

[98] *See* n 82; *cf Privacy International* case, n 7, para 70.

[99] Cour constitutionnelle 22 April 2021, Case 57/2021, para. B.18.