National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts

Marcin Rojszczak*

The Court of Justice is once again clarifying the limits of the application of data retention laws – General obligation to retain data exceeds the limits of what is strictly necessary within a democratic society – The national security exception does not preclude a judicial assessment of the legitimacy of its application – The existence of a genuine and specific threat as a premise for the use of untargeted data retention measures – The possibility of searching for the gold standard of data retention based on algorithmic processing – Different perceptions of the Court of Justice position by the referring courts – The Conseil d'État's position distorts the idea of the protection of fundamental rights that is enshrined in the EU legal order

Introduction

There are concepts in modern European law which, despite the passage of many years and a plethora of case law, are still the subject of dispute and debate. There is no doubt that this category includes a general data retention obligation that, according to some, is a measure that is a necessary to fight against serious crime and, according to others, poses a threat to civil liberties and freedoms.[1]

*Assistant professor at Warsaw University of Technology, Faculty of Administration and Social Sciences, Poland. Email: marcin.rojszczak@pw.edu.pl.

[1] *See*, e.g. P. Breyer, 'Telecommunications Data Retention and Human Rights: the Compatibility of Blanket Traffic Data Retention with the ECHR', 11 *European Law Journal* (2005) p. 365; R. Clarke, 'Data retention as mass surveillance: the need for an evaluative framework', 5 *International Data Privacy Law* (2015) p. 121; V. Lubello and A. Vedaschi, 'Data Retention and its Implications for the Fundamental Right to Privacy: A European Perspective', 20 *Tilburg Law Review* (2015) p. 14-34.

European Constitutional Law Review, 17: 607–635, 2021

doi:10.1017/S1574019621000353

The issue of the admissibility of data retention in the EU can be examined on different levels. In the most general context, the problem is focused on the assessment of the applicability of data retention taking into account the respect for fundamental rights on which the European model of democracy is built. In this case, the assessment is not so much on *how* to apply data retention but whether this measure – regardless of the legal safeguards that are implemented – can be reconciled with the constitutional values of the member states. To rephrase this point: Does data retention *per se* violate the essence of the fundamental right to privacy and the protection of personal data? An affirmative answer would eliminate the need for a proportionality test. In that case, the measure – whatever its aims – should not be applied in the legal order of democratic states.[2]

A separate aspect of the analysis is whether and to what extent the European Union has any competence in imposing restrictions on data retention. Beginning with the introduction of the EU Data Retention Directive[3], a dispute arose among member states as to whether a measure that is used for general security purposes constitutes an element of harmonisation of internal market rules. With the entry into force of the Lisbon Treaty,[4] a number of key legal changes were introduced that altered the interpretative context for EU competences regarding data retention laws. With the removal of the division into three pillars of integration, the Union's competences regarding cooperation in criminal matters – including the fight against serious crimes – were strengthened. At the same time, the area of fundamental rights protection was reinforced, which was achieved by assigning a Charter of Fundamental Rights with the same force as treaties and introducing a separate competence provision that allowed the adoption of a new generation of EU data protection rules.[5] However, these changes were also accompanied by the extension of the national identity clause that *explicitly* grants member states exclusive competence in matters of national security.[6]

In the past 11 years, the Court of Justice has dealt with the compatibility of a general retention obligation with EU law on at least six occasions. At the same time, the issue of the admissibility of such a measure has been the subject of

[2]*Cf* M. Brkan, 'The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core', 14 *EuConst* (2018) p. 332.

[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 2006 L 105/54; act repealed.

[4]Treaty of Lisbon of 13 December 2007 amending the Treaty on European Union and the Treaty establishing the European Community, OJ 2007 C 306/1.

[5]Art. 16(1) TFEU.

[6]Art. 4(2) TEU. *See also* n. 31.

numerous rulings by national constitutional courts.[7] Some of these decisions predate the *Digital Rights Ireland* judgment[8] in which the Court first pointed out the disproportionality of general data retention. In subsequent judgments, constitutional courts have tended to follow the Court's reasoning in overturning national retention laws. However, this has not been the case in all member states; in some of them, the problem of data retention has not been analysed by the constitutional court for years (e.g. Poland),[9] while in others the legislature has expanded retention rules instead of reducing them.[10] In yet other member states, the position of the Court of Justice has led to the invalidation of retention rules only insofar as they concerned law enforcement powers relating to the fight against serious crime.[11]

For years, one of the central – and unsolved – problems concerning the obligation to retain data has been the admissibility of using this measure for the purposes of state security. The Court of Justice addressed these uncertainties in two recent judgments – *Privacy International*[12] and *LQN*[13] – in which it not only clarified the scope of application of the national security clause in relation to domestic data retention regulations but also provided guidelines concerning the admissibility of such regulations when their introduction is necessary for state security

[7]M. Zubik et al. (eds.), *European Constitutional Courts towards Data Retention Laws* (Springer, Cham, 2021).

[8]ECJ 8 April 2014, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238.

[9]Although the Polish Constitutional Tribunal issued a precedent-setting ruling in case K 23/11 in 2014 in which it declared certain national provisions on the application of data retention unconstitutional, it did not explicitly challenge a data retention obligation itself as a responsibility imposed on telecom operators. This was because the assessment of the constitutionality of this measure was beyond the scope of the underlying applications for constitutional review. After the reforms introduced by the new government majority, the Constitutional Tribunal was restructured and is now not considered by many to be a properly staffed constitutional court. Therefore, in 2018, the Ombudsman withdrew his application that aimed, among other things, to examine the constitutionality of domestic surveillance laws. *See* J. Podkowik, 'Privacy in the digital era - Polish electronic surveillance law declared partially unconstitutional: Judgment of the Constitutional Tribunal of Poland of 30 July 2014, K 23/11', 11 *EuConst* (2015) p. 577. 'Adam Bodnar withdrew from the Constitutional Tribunal motion regarding the Act of 10 June 2017 on Counter-Terrorism Measures', Commissioner for Human Rights, 2 May 2018, ⟨https://cli.re/pZboBw⟩, visited 3 November 2021.

[10]An example is Italy, where the legislature has extended – rather than limited – the data retention period to 30 months which is unprecedented in other member states. *See* Art. 132 of the Italian Data Protection Code (Decreto Legislativo 30 giugno 2003, n. 196).

[11]An in-depth analysis of the *Data Rights Ireland* case and its impact on national data retention laws may be found in Zubik et al., *supra* n. 7.

[12]ECJ 6 October 2020, Case C-623/17, *Privacy International*, ECLI:EU:C:2020:790.

[13]ECJ 6 October 2020, Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others,* ECLI:EU:C:2020:791.

objectives. This position – although consistent with previous case law – was interpreted differently by the referring courts. This fact alone is the best evidence of the difficulty of developing a common European standard for the assessment of retention provisions.

The purpose of this article is to present the primary conclusions of the *Privacy International* and *LQN* judgments and the controversy surrounding the implementation of these judgments by the referring courts. In this regard, particular attention has been paid to the argumentation presented by the Conseil d'État – mainly because it indicates the possibility of reconciling the application of general data retention with the limitations defined by the Court of Justice.

Data retention in the case law of the Court of Justice

The Court of Justice first examined data retention legislation in 2010 in a case brought by Ireland that challenged the adoption of Directive 2006/24 (the Data Retention Directive) as a means of harmonising the rules of the internal market.[14] According to Ireland's position, data retention should not be considered as an element of economic cooperation but as a means of cooperation in criminal matters. The Court did not share this view – indicating that, since the Data Retention Directive did not specify the rules for handling retained data (in particular, the procedure of accessing this data by law enforcement agencies), the obligation imposed on telecommunications operators as affecting the functioning of the internal market could itself be regulated by EU legislature.[15] While deciding on the competence of the EU to enact the Data Retention Directive, the Court also indirectly pointed to the possibility of assessing both EU and national data retention regulations for compliance with overriding norms of EU law, including the Charter of Fundamental Rights. As a result, in a subsequent judgment – in *Digital Rights Ireland* – the Court, for the first time, conducted the substantive assessment of a general data retention obligation, in particular the proportionality and necessity of its application in democratic states. Against this background, it held that the capturing of all metadata relating to electronic communications without any connection with ongoing criminal proceedings and in a generalised manner, with regard to all subscribers to telecommunications services, could not be reconciled with compliance with the principle of proportionality.[16]

[14]ECJ 10 February 2010, Case C-301/06, *Ireland* v *Parliament and Council*, ECLI:EU:C:2009:68.

[15]*Ireland* v *Parliament and Council*, *supra* n. 14, para. 84.

[16]*Digital Rights Ireland*, *supra* n. 8, para. 69.

The Court pointed out that respect for fundamental rights – including the right to privacy – requires that derogations must be limited to what is strictly necessary.[17] That requirement cannot be satisfied with a measure that permanently and generally restricts the right to privacy of all users of electronic communications without any genuine connection with the need to pursue public security objectives.[18] As a result, the Court held that the Data Retention Directive, as violating the principle of proportionality, cannot be reconciled with overriding norms of EU law and is therefore invalid.[19]

The *Digital Rights Ireland* judgment led to a series of constitutional court decisions declaring that national retention laws are incompatible with constitutional norms. As the Court pointed out, the actual purpose of the Data Retention Directive was to contribute to the fight against serious crime.[20] Therefore, in the *Digital Rights Ireland* case, it did not examine the admissibility – and, therefore, also the proportionality – of introducing retention measures that serve other purposes, in particular state security.

In the EU legal model, the Data Retention Directive was a maximum harmonisation measure constituting a *lex specialis* for the rules established for the telecommunications sector – especially Directive 2002/58 (the e-Privacy Directive)[21]. The annulment of the Data Retention Directive led to a situation in which national retention rules not only *could* but, as the Court later pointed out, also *should* be assessed for compliance with the e-Privacy Directive. It was because the e-Privacy Directive also defined permissible restrictions on the rights and obligations of users of electronic communications services. In this respect, the derogation clause contained in Article 15(1) of the e-Privacy Directive was of particular importance. It introduced the competence of member states to adopt national retention regulations if their introduction was 'necessary, appropriate and proportionate' to achieve recognised objectives of a democratic state, inter alia, ensuring national security. In effect, Article 15(1) provided the basis for the introduction of national retention laws in the areas of both the fight against serious crime and national security.

[17]ibid., para. 52.

[18]ibid., paras. 57-59.

[19]In particular, the Court pointed to violations of Art. 7 (right to privacy), Art. 8 (protection of personal data), and Art. 52(1) of the Charter of Fundamental Rights. For a broader discussion of the judgment, *see* Lubello and Vedaschi, *supra* n. 1; T. Ojanen, 'Court of Justice of the European Union, Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12', 10 *EuConst* (2014) p. 528.

[20]*Digital Rights Ireland*, *supra* n. 8, para. 41.

[21]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, OJ 2002 L 201/37.

Cooperation in criminal matters is directly covered by EU regulations with the result that the Union's competences in this area are indubitable. The situation is different in the case of state security: although Article 15(1) literally indicates the possibility of introducing a derogation from the standard of protection established in the e-Privacy Directive, Article 1(3) of the same directive states that its provisions do not apply 'in any case' to activities concerning state security. It is worth remembering that the e-Privacy Directive had entered into force seven years before the Lisbon reform. It is, therefore, obvious that the authors of the directive could not have foreseen the future wording of the national security clause as included in Article 4(2) of the TEU. The above leads to numerous interpretative uncertainties concerning the possibility of simultaneous application of Article 1(3) and Article 15(1) of the directive – this is essentially an attempt to construct an interpretation of the provisions of the e-Privacy Directive which, while maintaining the exemption indicated in Article 1(3), would not make the introduction of Article 15(1) pointless.

The Court of Justice addressed these ambiguities in its judgment in *Tele2 Sverige*.[22] It first explained that the objectives justifying the adoption of national measures restricting individuals rights under the e-Privacy Directive, such as public security, principally refer to activities undertaken by states and are unrelated to the activities of individuals.[23] Applying the principle of effective interpretation of EU law, the Court noted that the adoption of a broad interpretation of Article 1(3) of the e-Privacy Directive – which would have the effect of excluding all activities relating to public security, defence, and state security from the scope of the directive – would *de facto* deprive the derogation clause in Article 15(1) of any force.

Thus, while there was no doubt that the rules imposing an obligation on telecommunications operators to retain data are not excluded from EU law, the question of the applicability of EU law to the assessment of regulations on access to retained data by authorised authorities remained open. In the *Tele2 Sverige* judgment, the Court partially resolved these doubts by pointing out that the purpose of national legislation adopted on the basis of Article 15(1) of the e-Privacy Directive is also to determine the rules for access to retained data – which leads to the conclusion that these measures are not beyond the scope of the directive itself and, consequently, other EU law rules.

The Court of Justice also developed and elaborated on its standard for assessing national retention rules. It reiterated its position that was already expressed in *Digital Rights Ireland.* A generalised and indiscriminate mechanism for the

[22]ECJ 10 21 December 2016, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige*, ECLI:EU:C:2016:970.

[23]*Tele2 Sverige* case, *supra* n. 22, para. 72.

retention of metadata derived from electronic communications that applies to all users and without any relationship whatsoever to whether or not the data are of any – even indirect – interest to the competent authorities cannot be reconciled with the principle of proportionality. In that regard, the Court noted that respect for the principle of proportionality requires that interference with fundamental rights be limited to what is strictly necessary to achieve an intended objective.[24] The collection of data on persons who are of no interest to law enforcement authorities clearly does not fulfil the purpose for which this measure was introduced. It therefore infringes on the principle of necessity and, consequently, cannot be reconciled with respect for the overriding rules of EU law.

At the same time the Court indicated the possibility of interference that is more far-reaching in the area of fundamental rights when it serves national security interests. In such a case, it is possible to collect information on persons about whom the state authorities have no knowledge of their involvement in any criminal activity. However, also in this case, it is necessary to respect the principle of necessity – according to which there should be objective indications that the processed information is genuinely related to general security objectives.[25]

As a result, the interpretation in the *Tele2 Sverige* case conclusively determined that an indiscriminate data retention obligation could not be reconciled with EU law in cases when the measure serves the purpose of fighting crime.[26] At the same time, though, the Court signalled the possibility of adopting a less restrictive interpretation if the measure was to serve state security.[27]

This position requires further comment. There is no doubt that, in cases when data retention is used to fight crime, the scope of data made available to law enforcement authorities should result from the needs of ongoing criminal proceedings. On the one hand, this condition directly serves the implementation of the strict necessity principle;[28] on the other hand, it limits the risk of abuse

[24]ibid., para. 96.

[25]ibid., para. 119.

[26]ibid., para. 107.

[27]For a broader discussion of the *Tele2 Sverige* judgment *see* A.M. Pedersen et al., 'Data retention in Europe – the Tele 2 case and beyond', 8(2) *International Data Privacy Law* (2018) p. 160; E. Celeste, 'The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios', 15 *EuConst* (2019) p. 134.

[28]The condition of *strict necessity* is an element of the standard applied by the European Court of Human Rights in its examination of domestic surveillance laws. Strict necessity should be understood as the cumulative fulfilment of two conditions: first, the need for a measure to protect the democratic institutions of the state (a narrower understanding used in earlier Court's judgments) and, second, the necessity of the measure in a specific case due to the need to obtain relevant operational data on the individuals under surveillance. In the case law of the Court of Justice, this principle is also referred to as 'absolute necessity'. *See* ECtHR 12 January 2016, No. 37138/14, *Szabó and Vissy* v *Hungary*, para. 73.

of power and arbitrariness in conducting surveillance. At the same time, limiting access to retained data only to cases related to ongoing criminal proceedings does not influence the effectiveness of this measure. Data retention is not intended to serve the purpose of surveillance of the entire society but only to secure the availability of information in the event that access to it proves to be necessary for the clarification of specific criminal proceedings.

The situation is different regarding the activities of security services, particularly those dealing with domestic intelligence. One of the tasks carried out by such agencies is to identify future threats – specifically at an early stage when their effects have not yet materialised. As a rule, these threats do not even have to relate to the area of public security; they may be connected, for example, with the protection of the state's economic interests or countering foreign intelligence. In the case of the US National Security Agency, the programme for the mass collection of metadata from electronic communications was intended primarily to detect terrorist threats, and it was aimed at identifying the so-called agents of influence in the United States.[29] From the perspective of security services, limiting access to retained data to only information relating to specific, previously identified individuals would *de facto* render this measure useless for the performance of their statutory tasks. This is because security services focus on predictive analysis that is based on revealing previously unknown relations and communication patterns in a large group of people. In such a case, the collected data are to help identify new threats and not to collect evidence against persons already suspected of involvement in criminal activities. For this reason, the term 'preventive retention' is also used in relation to activities carried out in the field of national security, and it is intended to emphasise that the data collected and processed are employed to identify future threats.

Even so, the question arises as to whether preventive retention can be considered to comply with the condition of necessity. Stated differently, can public authorities collect data on individuals about whom they do not have even indirect evidence or a link with activities threatening the interests of the state? The thought can be rephrased as follows: Can the state suspect everyone of being a potential terrorist? Additionally, how can it be assessed whether the undisclosed data processing procedures carried out by secret services do indeed facilitate identifying new threats for which the disclosure would be impossible with less intrusive means?

[29]Indeed, the history of the NSA's STELLARWIND programme, carried out under its authority under s 215 of the FISA Act, provides a glimpse into how the power to collect strictly foreign intelligence-related data – in the absence of effective court oversight and proper government interpretation – can lead to an environment for surveillance of a large portion of a country's own population. *See* R. Barnett, 'Why the NSA Data Seizures Are Unconstitutional', 38 *Harvard Journal of Law & Public Policy* (2015) p. 3; C.J. McGowan, 'The Relevance of Relevance: Section 215 of the USA Patriot Act and the NSA Metadata Collection Program', 82 *Fordham Law Review* (2014) p. 2399.

This is an important issue to which the Court did not provide a distinct answer in *Tele2 Sverige*. In this respect, it contented itself with pointing out that preventive retention *per se* is not incompatible with EU law, provided that it actually makes it possible to contribute to combatting the most serious threats to state security.

National security and new questions referred for a preliminary ruling

Scope of application of EU law

The background of the *Tele2 Sverige* case was the requests for a preliminary ruling made by the Swedish and British courts in the context of the examination of national retention rules applied in the area of criminal procedures. Therefore, the Luxembourg Court focused its considerations on this problem and disregarded detailed discussions on the admissibility of data retention in the field of national security.

In practice, however, separating these two areas of activity of state bodies is not a simple task. First, in many member states, security services are competent both to conduct criminal proceedings and to pursue national security objectives.[30] In such a case, it would render external oversight impractical and difficult if it was accepted that the services can access retained data when carrying out only some of their tasks. Moreover, a number of serious threats – such as terrorism – are linked to both state security and criminal law.

This subsequently leads to questions about the scope of the EU's competence in the fight against serious crime. Although the EU may introduce minimum standards, *inter alia*, in relation to terrorist offences pursuant to Article 83(1), it should not be overlooked that this provision must not prevent the effectiveness of the tasks undertaken by individual member states in the field of national security (which accords directly from Article 4(2) of the TEU).[31]

[30]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*). *See also* 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II, Field perspectives and legal update', *European Union Agency for Fundamental Rights* (Publications Office, 2017) p. 28.

[31]It should be borne in mind that the exclusion of national security resulting from Art. 4(2) of the TEU is also accompanied by the provisions of Art. 73 and Art. 276 of the TFEU (regarding actions taken to protect internal security).

The assumption that national retention regulations fall within the scope of EU law in any case – including when the collected data are used by secret services – would naturally lead to doubts as to the compatibility with the national security clause defined in the treaties. In the case of the *Tele2 Sverige* judgment, the Court was required to clarify how to interpret Article 1(3) and Article 15(1) of the e-Privacy Directive so as not to deprive any of these norms of practical meaning. In the case of the application of data retention rules in the area of national security, it was also necessary to provide an interpretation of Article 4(2) of the TEU that, while respecting the national identity of states, would not constitute an obstacle to the standardisation of telecommunication rules applied within the internal market.

Domestic law

These ambiguities led to requests for a preliminary ruling being referred to the Court of Justice by national courts of the United Kingdom (*the Privacy International* case) as well as France and Belgium (the *LQN* case). The subject of all of the requests was the application of national retention laws in the legal circumstances arising after the *Tele2 Sverige* judgment, including in relation to the pursuit of state security objectives. Given the differences between national legislations, the referring courts made a point of stressing the varying elements of the data retention rules in their applications.

Regarding the United Kingdom, the Telecommunications Act 1984 introduced a general power for the Secretary of State to issue binding orders in all cases that are 'necessary in the interests of national security or relations with the government of a country or territory outside the United Kingdom'.[32] In particular, these orders could concern the obligation to transmit all metadata aggregated by telecommunications operators to designated security and intelligence services.[33] As a result, the secret services were able to access bulk volumes of data from electronic communications – and to do so bypassing the legal safeguards established in the area of criminal retention.

Similar powers were not granted to Belgian secret services. Following the *Digital Rights Ireland* judgment, the Belgian Constitutional Court declared the Electronic Communications Act[34] invalid to the extent that it transposed the

[32]*See* the wording of s 94 of the UK Telecommunications Act 1984 as in force before 22 August 2018. The provision was withdrawn with the coming into force of the Investigatory Powers Act 2016, Sch 10, para 99.

[33]In the context of the referred case it was GCHQ, MI5 and MI6. For a complete list of security and intelligence agencies by member state *see* 'Surveillance by intelligence services . . . .', *supra* n. 30, p. 157.

[34]Loi du 13 juin 2005 relative aux communications électroniques, ⟨https://cli.re/pZAqWJ⟩, visited 3 November 2021.

https://doi.org/10.1017/S1574019621000353 Published online by Cambridge University Press

Data Retention Directive.[35] In lieu of the challenged provisions, a new regulation was adopted – the drafting of which took into account both the arguments presented in the Court of Justice judgment and the earlier constitutional court ruling. Although the updated regulations still provided for mandatory data retention with regard to all users of all communication services, they introduced a number of procedural safeguards imposed on telecommunications operators and specified in detail the circumstances under which access to the data could be obtained by authorities. Such access was also possible for secret services – with the understanding that, under Article 18/8 of the Intelligence and Security Services Act, they could obtain data no older than, respectively, six, nine, or twelve months – depending on the seriousness of the threat.[36] In each case, access to the data was not preceded by any judicial review and was based on a decision by the head of the service.

In contrast, the French regulatory model combined features of unlimited access as applied in the UK and targeted access as applied in Belgium. In principle, French telecommunications law also retained a general data retention obligation requiring providers to record metadata on all users of all electronic communications services and store them for 12 months.[37] As with the Belgian legislation, the French regulations – enshrined in the Internal Security Code[38] – also granted the possibility for specialised services to access retained data for the purposes of carrying out state security tasks (detailed in Article L 811-3 of the Code). This access was also generally not preceded by a judicial review (*cf* Article L 851-1 of the Code).

However, a special feature distinguishing the French legislation from the British or Belgian provisions discussed earlier is the possibility of applying a specific procedure for the algorithmic processing of bulk data. Unlike in the British model, French telecommunications operators are not under a permanent obligation to transmit all retained data to designated security services. Instead, they may be required to implement 'an automated processing operation aimed at detecting communications that may indicate a terrorist threat'.[39] In effect, the use of this measure may have helped to limit the scope of information provided to secret services only to data that meet predetermined criteria. The intention of the

[35]Cour constitutionnelle judgment of 11 July 2015 in case 84/2015, ⟨https://cli.re/xmQayJ⟩, visited 3 November 2021.

[36]Loi du 30 novembre 1998 organique des services de renseignement et de securité, ⟨http://www.ejustice.just.fgov.be/eli/loi/1998/11/30/1998007272/justel⟩, visited 3 November 2021.

[37]Art. R 10-13(III) of the French Postal and Electronic Communications Code.

[38]Code de la sécurité intérieure, ⟨https://www.legifrance.gouv.fr/codes/id/LEGITEXT000025503132⟩, visited 3 November 2021.

[39]Art. L 851-3 of the Internal Security Code, *supra* n. 38.

legislature was thus to ensure that preventive retention could be used – yet without the necessity of transmitting all of the data collected to the secret services.

All the UK, Belgian, and French laws in question allowed secret services to access retained data. This access, unlike the powers of law enforcement authorities, was largely based on the decision of the service itself and was not preceded by judicial review. Moreover, due to the preventive nature of the analysis, the persons whose data were accessed were not informed of this fact (not even *post factum*) which meant that they were deprived of the right to challenge this decision in court.

The main difference between the UK and French legislations concerned the way in which the bulk data were processed. In the British model, processing was the sole responsibility of secret services and was carried out without any real external oversight, and the role of telecommunications operators was solely to ensure the continuous transmission of retained data. In the French model, secret services defined the processing criteria in order to identify persons likely to be associated with terrorist activities. Data processing was then performed by the telecommunications operator, and only the data meeting the criteria were transmitted to the authorised services.

Questions referred for a preliminary ruling

Due to the differences in the retention rules functioning in individual countries, the questions posed by domestic courts aimed to clarify various doubts related to the application of the Court of Justice's standard. Importantly, they were also asked by courts with different constitutional positions: the constitutional court (Belgium), the highest administrative court (France),[40] and the specialised court authorised reviewing the application of surveillance powers (the United Kingdom).

The most important issue formulated by the UK Investigatory Powers Tribunal[41] and the French Conseil d'État[42] was whether national retention laws

[40]The Council of State's position goes beyond the role ascribed in other legal orders to the administrative judiciary. For the purposes of this paper, the Council of State will be presented as the highest administrative court. For more on the constitutional position of the Council of State and the Constitutional Council, *see*: P. Delvolvé, 'Le Conseil d'État, cour suprême de l'ordre administratif', 123 *Pouvoirs* (2007) p. 51; A. Dyevre, 'The French Constitutional Council' in A. Jakab et al. (eds.), *Comparative Constitutional Reasoning* (Cambridge University Press, 2017) p. 323-355.

[41]*See* the first question defined in 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⟩, visited 3 November 2021.

[42]*See* the first question defined in the request for a preliminary ruling of 3 August 2018 referred by the Conseil d'État (France), C-511/18, ⟨https://cli.re/rw383k⟩, visited 3 November 2021. The Council of State made two requests for preliminary rulings – in Cases C-511/18 and C-512/18. From the perspective of this article, the questions referred in Case C-511/18 were relevant;

applied in the field of national security fall within the scope of EU law. If the answer to this question was in the affirmative, the UK court expected the Court of Justice to clarify whether the bulk collection and transfer of data to secret services for the purpose of subsequent preventive analysis could be regarded as a measure meeting the conditions of necessity and proportionality as defined in the Charter of Fundamental Rights.[43] If the first question was answered in the affirmative, the Conseil d'État, in turn, awaited an interpretation as to whether a preventive retention measure as resulting from the Internal Security Code (and thus consisting, *inter alia*, of the processing of data by the telecommunications operator rather than secret services) could be reconciled with the requirements under EU law.[44] In other words, both courts first intended to determine whether data retention in the area of national security actually falls within the scope of EU law and, if so, whether national legislation establishing a framework for the bulk processing of such data and making it available to secret services can be considered compatible with EU law.

In its request, the Conseil d'État additionally addressed the problem of the application of the information obligation to persons subject to surveillance.[45] In the *Tele2 Sverige* judgment, the Court of Justice pointed out that compliance with this obligation is crucial to ensuring the right to a remedy – and, consequently, respect for the right to a fair trial.[46] The Council sought to determine whether the introduction of other procedural safeguards for which the overall assessment would lead to the conclusion that the right to a remedy is respected could imply that security services are not required to fulfil the information obligation in respect of individuals whose data is processed.[47]

As Belgian legislation did not provide for the possibility of bulk (algorithmic) data processing by the secret services, the Cour constitutionnelle did not address the issue in its questions of whether such measures are at all within the scope of EU law.[48] Instead, in its first question, it sought to clarify whether the Court of Justice's finding that a general data retention obligation applied in the area of the fight against serious crime is incompatible with EU law also predetermines the fact that this measure cannot be used for other purposes such as national security

therefore, in the remaining part of the paper (unless otherwise noted), references to the questions asked by the Council will be to Case C-511/18.

[43] *Supra* n. 41, question 2.

[44] *Supra* n. 42, question 2.

[45] *Supra* n. 42, question 3.

[46] *Tele2 Sverige*, *supra* n. 22, para. 121.

[47] *Supra* n. 42, para. 31.

[48] However, the problem was flagged in the request – *see* the request for a preliminary ruling of 2 August 2018 referred by the Cour constitutionnelle (Belgium), C-520/18, ⟨https://cli.re/vzv44J⟩, visited 3 November 2021, paras. 101-104.

https://doi.org/10.1017/S1574019621000353 Published online by Cambridge University Press

or defence.[49] Two further questions from the Belgian Constitutional Court focused on the use of retention in the area of criminal matters, including particularly the consequences of declaring the examined measures to be incompatible with EU law for ongoing criminal proceedings.[50] These are obviously important issues but, as they are beyond the scope of this article, they will not be discussed further.

In addition to the legal issues raised by preliminary questions, the reasoning and legal arguments proposed by the referring courts were equally interesting. In its request, the Investigatory Powers Tribunal emphasised that allowing secret services access to retained data was 'essential to the protection of the national security of the United Kingdom, including in the fields of counter-terrorism, counter-espionage and counter-nuclear proliferation'.[51] Moreover, it pointed out that, as it had established, the application of that measure did not lead to a violation of the European Convention on Human Rights. The Tribunal also stated that the application of the data retention rules defined in the *Tele2 Sverige* judgment to the activities of secret services would, in fact, 'frustrate the measures taken to safeguard national security (...) and thereby put the national security of the United Kingdom at risk'.[52]

By doing so, the referring court *de facto* indicated that, in its view, preventive retention is necessary and required to achieve state security objectives and that, if the retention has to be improved in order to meet to the standards of the *Tele 2 Sverige* judgment, it will not be possible to use it effectively, which will adversely affect state security. The Conseil d'État made similar arguments in its reasoning, pointing out that preventive retention 'demonstrates incomparably greater utility than collecting the same data only from the moment the data subject has been identified as likely to pose a threat to public security, defence or state security'.[53]

A similar argument, formulated by the Belgian Council of Ministers, was also cited by the Cour constitutionnelle. According to the government, replacing generalised retention by a targeted form would be 'simply impossible' and would not achieve the intended purpose of the processing.[54] In turn, the applicants in the Belgian case pointed out that the adoption of such an interpretation *per se* could not justify the application of a measure so seriously interfering with citizens' private lives. In such a case – in their view – 'it seems logical not to implement such a measure'.[55]

[49] *Supra* n. 48, question 1.
[50] *Supra* n. 48, questions 2 and 3.
[51] *See* explanatory note in *supra* n. 41.
[52] ibid.
[53] *Supra* n. 42, para. 23.
[54] *Supra* n. 48, para. 117.
[55] *Supra* n. 48, para. 38.

https://doi.org/10.1017/S1574019621000353 Published online by Cambridge University Press

The extremity of the presented assessments proves that the jurisprudence has thus far not contributed to the development of a universally accepted standard of assessment of national provisions and that the problem discussed – due to its supranational character – required a more precise interpretation of EU law to be provided by the Court of Justice.

Court of Justice judgments in the *Privacy International* and *LQN* cases

The core element of the submitted questions was to determine whether retention regulations established in the area of national security should be subject to the same standard as the one that the Court had previously defined when examining regulations applied in the area of combatting crime. A negative answer would lead to the conclusion that the member states are free to shape their national law – and that the only standard of review should be compliance with constitutional norms and obligations under the European Convention on Human Rights.

In clarifying these issues, the Court first addressed the scope of the national security exemption in relation to a general data retention obligation. It confirmed that, in principle, national security remains the exclusive responsibility of each member state.[56] However, this does not mean that measures taken in this area are entirely outside the scope of EU law.[57] Indeed, it follows from the well-established case law that limitations on rights and freedoms must be interpreted narrowly.[58] Furthermore, the power of a member state to avail itself of a derogation under the treaty does not preclude judicial review of measures taken under that derogation.[59] This is the only way to ensure that the meaning given to particular terms is not determined unilaterally by individual member states.[60]

Examining the relationship between the national identity clause (Article 4(2) TEU) and the derogation clause in the e-Privacy Directive (Article 1(3)), the Court noted that, in principle, all activities listed therein belong to activities undertaken by public authorities and are unrelated to private entities. On that basis – in accordance with the principle of effectiveness of EU law – it pointed out that the national security exception should be interpreted as applying only to activities carried out directly by public authorities and not by entities fulfilling a

[56]*LQN*, *supra* n. 13, para. 135.

[57]ECJ 4 March 2010, Case C-38/06, *EC* v *Portugal*, ECLI:EU:C:2010:108, para. 62.

[58]*Privacy International*, *supra* n. 12, para. 67 and the case law referred to therein.

[59]ECJ 4 December 1974, Case C-41/74, *van Duyn* v *Home Office*, ECLI: ECLI:EU: C:1974:133.

[60]ECJ 14 October 2004, Case C-36/02, *Omega Spielhallen- und Automatenaufstellungs*, ECLI: EU:C:2004:614.

legal obligation imposed on them.[61] This reasoning – consistent with the position of the Advocate General Campos Sánchez-Bordona[62] – led to the conclusion that activities undertaken directly by public entities, including security services, and concerning national security objectives, are excluded from the scope of EU law, including Directive 2002/58. However, this exclusion does not apply to the activities of private entities such as telecommunications operators. This is because, in their case, the obligation to retain data is part of the regulation of the telecommunications market not related to fulfilling national security objectives.

The Court's argumentation is convincing. It allows the scope of application of the national security clause to be narrowed in a way that leaves freedom of action to security services. It also does not lead to the risk of member states setting arbitrary standards for the protection of electronic communications under the pretext of ensuring national security. At the same time, this reasoning enables a coherent response to the specific questions posed by referring courts.

Thus, in the case of the evaluation of the UK retention model – which is based on the obligation for telecommunications operators to transmit all retained data to intelligence services on a permanent basis – it becomes clear that such a measure, being disproportionate, cannot be reconciled with the principle of proportionality and leads to a violation of the rights under the Charter.[63] The rationale for this assessment is the same as that for the assessment of generalised retention in the area of the fight against crime: collecting data of all persons, including those who have no connection with activities of interest to secret services, clearly exceeds what can be considered necessary in a democratic society.[64]

Against this background, it is worth noting the evolution of the Court of Justice's standard: in earlier cases, the collection and processing of bulk amounts of metadata was not equated with other forms of electronic surveillance. In the *Privacy International* judgment, the Court explicitly indicated that the analysis of metadata may allow the disclosure of sensitive information and enable 'establishing a profile of the persons concerned' – which leads to the conclusion that metadata should be protected at the same level as the content of the communication.[65] This is a pertinent observation that also determines the need to apply similar legal and technical measures to the protection of metadata as those that are applied to the secrecy of telecommunications. In this respect, the position of the

[61] *Privacy International*, *supra* n. 12, para. 48.

[62] Opinion of AG Campos Sánchez-Bordona delivered on 15 January 2020, Joined Cases C-511/18 and C-512/18, para. 79.

[63] *Privacy International*, *supra* n. 12, para. 78.

[64] ibid., para. 81.

[65] ibid., para. 71.

Luxembourg Court differs significantly from the view expressed in recent Strasbourg Court judgments.[66]

As early as the *Tele2 Sverige* case, the Court of Justice indicated the possibility of applying measures leading to a more far-reaching interference with privacy if they serve national security objectives. In the *LQN* judgment, the Court developed this position. It recalled that the protection of national security goes beyond other purposes justifying the use of data retention, such as the fight against crime, including serious crime, as well as the protection of public order.[67] Therefore, in principle, the implementation of generalised data retention based on the collection of data with regard to all users is not *per se* incompatible with EU law – and such incompatibility arises when the manner in which the measure is implemented exceeds what is strictly necessary.[68] As the Court has pointed out, the application of a measure such as generalised data retention may be regarded as proportionate when it is limited in time and occurs in relation to a specific and serious threat to state security.[69] It must be stressed that the interpretation expressed in the *LQN* case in no way contradicts with the position taken in the *Privacy International* judgment: in both cases, the Court held that generalised data retention – applied on a permanent and systematic basis and unrelated to actual threats – cannot be reconciled with the principles of proportionality and necessity.

The assessment of the British provisions should not be unexpected to careful observers of the Court of Justice jurisprudence. It was more difficult to assess the dilemma raised by the Conseil d'État concerning the admissibility of using algorithmic processing of metadata carried out directly by the telecommunications operator and not by a secret service (as in the British variant).[70]

In addressing this issue, the Court first pointed out two significant inaccuracies in the argumentation presented by the government. First, any operation on data constitutes processing. This processing is independent of the subsequent collection of data concerning individuals who are identified following an automated analysis. This means that the fact that only a part of the data (fulfilling established criteria) is further processed does not reduce the scale of the interference related to the initial processing of all traffic data.[71] Furthermore, the mere data filtering

[66]*See* n. 114.

[67]*LQN*, *supra* n. 13, para. 136.

[68]ibid., para. 137.

[69]ibid., para. 165. But it should be noted that a measure limited in this way would then meet the definition of targeted retention, as the Court itself also notes (*see* ibid., para. 147).

[70]It should be borne in mind that these provisions had already been assessed by the Constitutional Council which recognised their constitutionality: Conseil constitutionnel 23 July 2015, Case 2015-713 DC, English translation available at ⟨https://www.conseil-constitutionnel.fr/en/decision/2015/2015713DC.htm⟩, visited 3 November 2021.

[71]*LQN*, *supra* n. 13, para. 172.

process cannot be considered as data anonymisation – since, according to the relevant provisions of French law, the secret services still have the possibility of subsequently establishing the identity of targeted individuals.[72]

As a result, the Court has defined guidelines that should be met in order for such an automated processing to be considered not to infringe EU law. Such processing should take place on the basis of a decision by a court or other independent authority which would make it possible to confirm that the manner in which data filtering is carried out, its scope, and the procedural safeguards that are implemented are adequate and proportionate.[73] It is necessary to ensure that the processing is not based solely on special categories of data such as racial or ethnic origin, political opinions, or religious beliefs.[74] Furthermore, it is necessary to implement measures protecting individuals against erroneous decisions which are an inevitable consequence of carrying out automated processing on a large scale. To achieve this, it is necessary to introduce a complaint procedure that provides for the possibility of reviewing the decision that is taken and to ensure periodic verification of the algorithms used in data processing.[75]

In practice, the use of automated analysis methods depends on whether it is possible to waive the information obligation towards data subjects. Otherwise, it would be necessary to provide relevant information to all users of electronic means of communication considering the fact that, by definition, the discussed measures are supposed – at least in an initial stage – to process all available metadata. As explained by the Court, in such a case, it should be sufficient to 'publish information of a general nature relating to that analysis without having to notify the persons concerned individually'.[76] The position refers to the concept of 'foreseeability' of the law, one of the key elements of the standard applied by the European Court of Human Rights when examining national surveillance laws.[77] The solution proposed by the Court of Justice, on the one hand, does not allow for conducting an algorithmic analysis according to unknown and non-transparent rules (e.g. in terms of its duration, scope of processed data, etc.). On the other hand, it does not require that the filtering rules themselves be disclosed to the public (although they should be authorised by the court).

[72]Art. L 851-3(IV) of the Internal Security Code, *supra* n. 38.
[73]*LQN*, *supra* n. 13, para. 179.
[74]ibid., para. 180.
[75]ibid., para. 182.
[76]ibid., para. 191.
[77]The criterion of foreseeability should not be equated with the transparency of actions taken by security services in a particular case. Foreseeability of the law concerns the possibility for an individual to determine which of his or her actions may entail the implementation of surveillance activities – and thus the interference with his or her fundamental rights. *See*, e.g. ECtHR 4 December 2015, No. 47143/06, *Roman Zakharov* v *Russia*, para. 229.

The Court of Justice thus determined that the principles of data retention serving national security objectives are not, in general, excluded from the scope of EU law, including the restrictions arising from the Charter of Fundamental Rights. At the same time it clarified its earlier position by indicating the possibility of adopting measures that interfere with fundamental rights to a greater extent when their application is objectively justified by the pursuit of national security objectives.

Reasoning presented by the French Conseil d'État: a new gold standard of data retention?

The Council's decision

The reasoning presented in the *Privacy International* and *LQN* judgments was negatively assessed by the French authorities. The government representatives argued that the uncritical adoption of the Luxembourg Court's interpretation would lead to the weakening of the effectiveness of security services – including in terms of counteracting terrorist threats.[78] It was also argued that the Court had misinterpreted the scope of the national security clause and, as a result, its ruling went beyond the scope of its competences. Hence, the government, based on *ultra vires* doctrine, requested that the Conseil d'État recognise the Court of Justice's decision as having no effect in the French legal model.[79] This argumentation was met with criticism from the legal community, as questioning the competence of the Court of Justice is regarded as a threat to the unity of EU law.[80] Against this backdrop, it is worth remembering the discussion – still ongoing – related to the German Constitutional Court's ruling of 2020 regarding the PSPP and numerous voices criticising the German court's decision.[81]

[78]L. Kayali, 'Tension mounts ahead of key ruling on French data retention', *Politico*, 14 April 2021, ⟨https://www.politico.eu/article/france-ruling-decision-data-retention/⟩, visited 3 November 2021.

[79]M. Pollet, 'Données de connexion: le Conseil d'État va devoir choisir entre froisser le gouvernement ou les institutions européennes', *Euractiv France*, 16 April 2021, ⟨https://cli.re/jYrVp1⟩, visited 3 November 2021.

[80]In fact, until the judgment of the German Constitutional Court of 5 May 2020 in the *PSSP* case, the national constitutional court of an EU member state had only once considered the ruling of the Court of Justice as *ultra vires*: R. Zbíral, 'Czech Constitutional Court, judgment of 31 January 2012, Pl. ÚS 5/12 – A Legal revolution or negligible episode? Court of Justice decision proclaimed ultra vires', 49(4) *Common Market Law Review* (2012) p. 1475.

[81]F.C. Mayer, 'The Ultra Vires Ruling: Deconstructing the German Federal Constitutional Court's PSPP decision of 5 May 2020', 16 *EuConst* (2020) p. 733; M. Wendel, 'Paradoxes of Ultra-Vires Review: A Critical Review of the PSPP Decision and Its Initial Reception', 21 *German Law Journal* (2020) p. 979.

The Conseil d'État did not take the government's position. In its reasoning, it recalled that, in accordance with previous case law, the constitution is the supreme legal act that is the source of fundamental rights. Therefore, in the event that the application of EU law as interpreted by the Court of Justice could not be reconciled with respect for constitutional rights, the national court would be obligated to adopt an interpretation that fully respects the constitution.[82] The position of the Conseil d'État on the relationship between constitutional order and EU law is similar to that expressed by the French Constitutional Council[83] and constitutional courts of other EU countries.[84] On the other hand, regarding the allegation that the Luxembourg Court acts outside the scope of EU treaties (*ultra vires*), it was held that EU law does not grant the Council the competence to assess the judgments of the Court of Justice, in particular by analysing whether the Court's judgments contain a correct interpretation of EU law.[85]

Turning to the merits, the Conseil d'État pointed out that the *LQN* judgment does not prejudge the incompatibility with EU law of generalised data retention that is applied in the area of national security. According to the Council, the introduction of such a measure is permissible 'when a state is faced with a serious threat to national security that is real and present or foreseeable'.[86] Based on this observation, the Conseil d'État conducted an analysis proving that France is under a constant and genuine terrorist threat. During the adoption of the legislation under review, this threat was real, as evidenced, *inter alia*, by the tragic attack on the Charlie Hebdo offices. This threat – in the opinion of the Conseil d'État – has not diminished and is still serious as shown by both the recurring counter-terrorist actions taken by secret services and statistics indicating that, in 2020, there were six incidents of this type in the country with seven people killed and eleven others injured.[87] Furthermore, according to the Council, France also faces a serious threat to public order as a result of the growing activities of radical and extremist groups.

The Conseil d'État also analysed whether the use of generalised retention is necessary and therefore whether it constitutes criterion of the least intrusive type

[82]Conseil d'État 21 April 2021, Case 393099, ECLI:FR:CEASS:2021:393099.20210421, para. 5.

[83]J. Bell, 'French Constitutional Council and European Law', 54 *International and Comparative Law Quarterly* (2005) p. 735.

[84]L.S. Rossi, 'How Fundamental are Fundamental Principles? Primacy and Fundamental Rights after Lisbon', 27 *Yearbook of European Law* (2008) p. 65.

[85]Conseil d'État 21 April 2021, *supra* n. 82, para. 6. *See also* J. Ziller, 'The Conseil d'Etat refuses to follow the Pied Piper of Karlsruhe', *Verfassungsblog*, 24 April 2021, ⟨https://cli.re/qD9dw5⟩, visited 3 November 2021.

[86]Conseil d'État 21 April 2021, *supra* n. 82, para. 30.

[87]ibid., para. 44.

of interference. In this regard, it explained that the use of targeted forms of data retention is ineffective for identifying new threats.[88] The Council pointed out that targeted retention does not enable, *inter alia*, the detection of the so-called 'lone wolves', i.e. persons previously not connected with organised crime, as well as perpetrators who frequently change means of communication, for instance, using mobile prepaid cards. Moreover, the Conseil d'État highlighted that the introduction of geographic limitations[89] to the use of generalised retention also faces both obstacles of a technical nature and difficulties in pinpointing the location of terrorist threats in a situation where they may arise throughout the country.[90]

These considerations led the Conseil d'État to conclude, first, that generalised retention meets the condition of necessity and is therefore the least intrusive form of data retention to achieve state security objectives. Secondly, its use is in accordance with the guidelines established by the Court of Justice, in particular in view of the permanent and ongoing threat to national security. The Conseil d'État held that the provision under review should not be repealed provided that it will be amended no later than within six months. The aim of this amendment is to introduce a measure of periodic verification of the persistence of a serious, genuine, and continuous threat to national security – as a condition for the continuing use of the generalised data retention.[91]

While the Council did not question the use of data collection procedures in principle, it partially annulled the provisions governing the possibility of algorithmic processing. In this regard, it emphasised the importance of applying *ex ante* control to ensure that this measure is applied only for counter-terrorism purposes and with the use of objective and non-discriminatory data filtering criteria. To ensure independent oversight of the application of this measure, the National Commission for the Supervision of Intelligence Techniques (Commission Nationale de Contrôle des Techniques de Renseignement) was established. However, in the case of algorithmic processing, a decision to use such a measure that was not in line with the Commission's opinion could not be subject to judicial review in every case. Therefore, in the Council's view, the provisions should be modified in such a way that, whenever the Commission expresses a negative position on the application of an algorithmic measure, a judicial review of the decision taken is possible.[92]

[88]ibid., para. 54.

[89]The introduction of geographical limitations was identified by the Court of Justice as one way of adapting the scope of data retention to the actual needs of countering threats to public security. *See Tele2 Sverige*, *supra* n. 22, para. 111; *LQN*, *supra* n. 13, para. 150.

[90]Conseil d'État 21 April 2021, *supra* n. 82, paras. 53-54.

[91]ibid., para. 46.

[92]ibid., para. 77.

https://doi.org/10.1017/S1574019621000353 Published online by Cambridge University Press

In conclusion, the Conseil d'État thus read from the *LQN* judgment the possibility of introducing a permanent data retention measure into national law – deriving its position from the existence of an ongoing terrorist threat in the French territory.

Critical assessment

The reasoning proposed by the Conseil d'État must raise serious concerns. There is no doubt that public authorities have the possibility – or even the obligation – to take extraordinary measures in the event of a threat to state security. The constitutions of European states (including the Constitution of France[93]) and the norms of international law[94] provide for such a situation of introducing specific powers of public authorities applicable in cases of emergency.[95] Understandably, in emergency situations, it is necessary to take measures that may also result in greater inconvenience to individuals. Both the Luxembourg Court and the Strasbourg Court have repeatedly pointed out that the introduction of states of emergency may entail more far-reaching restrictions on fundamental rights and a distinct assessment of the proportionality of the measures taken by the authorities.[96] Moreover, the French authorities have also used these powers in the past.[97] The constitutional provisions, while providing for extraordinary powers of authorities in crisis situations, also delineate a number of legal safeguards that are intended to ensure that the state of emergency does not become the norm. They also guarantee that the extraordinary powers are not abused and only applied to the extent necessary to restore the normal functioning of the state.[98]

It seems that this interpretation of states of emergency should clarify the meaning of the 'real and present or foreseeable' threat to national security referred to by the Court of Justice in the *LQN* judgment. Indeed, to accept the contrary

[93]S. Plato, 'From One State of Emergency to Another: Emergency Powers in France', *Verfassungsblog*, 9 April 2020, ⟨https://cli.re/vz93br⟩, visited 3 November 2021.

[94]Art. 4 of the International Covenant on Civil and Political Rights and Art. 15 of European Convention on Human Rights. *See also* G. Ulrich and I. Ziemele (eds.), *How International Law Works in Times of Crisis* (Oxford University Press 2019).

[95]The problem of introducing emergency powers is also discussed in terms of EU competences: *see* C. Kreuder-Sonnen, 'Does Europe Need an Emergency Constitution?' (2021) *Political Studies* 003232172110053.

[96]A. Greene, 'Separating Normalcy from Emergency: The Jurisprudence of Article 15 of the European Convention on Human Rights', 12 *German Law Journal* (2011) p. 1764.

[97]J. Müller, 'European human rights protection in times of terrorism – the state of emergency and the emergency clause of the European Convention on Human Rights (ECHR)', 28 *Zeitschrift für Politikwissenschaft* (2018) p. 581.

[98]D. Dyzenhaus, 'States of Emergency', in M. Rosenfeld and A. Sajó (eds.), *The Oxford Handbook of Comparative Constitutional Law* (Oxford University Press 2012).

interpretation put forward by the Conseil d'État would mean that the right to privacy *de facto* could be permanently eliminated from the area of fundamental rights because, in the 21st century, there will always be some future, more or less verifiable threat qualifying as a terrorist action. The position of the Council in this respect seems to completely disregard the rich jurisprudence of the Court of Justice indicating that any limitation in the area of fundamental rights must be applied as an exception – and not as a norm. It is difficult to accept that the day-by-day surveillance of millions of housewives, gardeners, bakers, and children is a measure that, in the opinion of France's highest administrative court, is necessary to protect the state from terrorist threats.

The Court of Justice has also clearly indicated that the use of generalised retention must be strictly limited in time.[99] It is then difficult to agree with the position of the Conseil d'État that this condition is met by a measure that applies indefinitely, and the validity for which will be periodically renewed (confirmed) by an authority empowered to do so. It is worth remembering that such a model of oversight over metadata collection and making it available to the secret services was applied in the US and was rightly criticised by the US federal court of appeal.[100]

As part of what is referred to as the War on Terror that was initiated after the 2001 World Trade Center attacks, surveillance laws in the US have been modernised several times over the years, including a framework for the bulk interception of communications.[101] The legislation adopted allowed communications data to be made available to the secret services on the basis of blanket court decisions, *de facto* not subject to scrutiny[102] and not conditioning access to data on meeting the principles of necessity or proportionality.[103] As a result, the National Security Agency, the US electronic intelligence service, had unrestricted access for many years to metadata on a significant number of telephone calls made within the US.

[99]*LQN*, *supra* n. 13, para. 137.

[100]J. Gerstein, 'Court rules NSA phone snooping illegal – after 7-year delay', *Politico*, 9 February 2020, ⟨https://cli.re/RwYB2e⟩, visited 3 November 2021.

[101]L.K. Donohue, (Oxford University Press, 2016). *See* n. 29; *also* K. Donohue, *The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age* (Oxford University Press 2016).

[102]Formally, decisions issued by the US Foreign Intelligence Surveillance Court – a special court set up, *inter alia*, to hear applications for authorisation of surveillance measures by the secret services – were subject to appeal to the Foreign Intelligence Surveillance Court of Review. However, in practice, because of the way the applications were processed, orders authorising the bulk interception of communications were not appealed because there was no one present during the court hearing that could bring such an appeal: L. Donohue, 'Bulk Metadata Collection: Statutory and Constitutional Considerations', 37 *Harvard Journal of Law and Public Policy* (2014) p. 757.

[103]*Cf.* e.g. the order disclosed in the public domain to hand over to the FBI and NSA all the metadata of millions of Verizon network subscribers – with no justification, *see* ⟨https://cli.re/9DzmY4⟩, visited 3 November 2021.

Subsequent analyses, including by independent oversight bodies, have shown that these data did not reveal new, previously unknown threats to national security.[104] As the Conseil d'État did not cite any verifiable studies, it is not clear on what basis it concluded that French intelligence services would be able to make better use of bulk data retention than their US counterparts.

Third, the arguments regarding the uselessness of targeted retention and the need for a generalised form of data collection are also unconvincing. The French Government, like governments in other democracies, should not assume that all citizens are (or at any time may be) criminals. If there are forms of communication that, as the Conseil d'État argues, involve more serious risks to public security (such as prepaid mobile cards), there is nothing to prevent separate data retention rules being established for them. It is incomprehensible how the risk that potential terrorists communicate with each other using prepaid cards can be mitigated by surveillance of users who employ all other means of communication. It seems that the answer to the disadvantages of targeted retention is not untargeted retention but algorithmic retention – which has not been rejected in principle by the Court of Justice and, with the necessary changes, may represent a reasonable compromise for data collection.

Finally, there is a genuine danger not only that the arguments adopted by the Council distort the idea contained in the judgment of the Court of Justice but that they are also counterproductive in terms of the evolution of the mechanisms of European integration. Despite declarations of applying a pro-European interpretation of the regulations, the argumentation presented by the Conseil d'État – leading to the establishment of a permanent derogation from the obligation to observe fundamental rights – sets a dangerous precedent. It encourages populist governments of certain member states (in particular, Poland and Hungary) to apply similar arguments. According to media information, while discussing the most important provisions of the judgment, representatives of the Council indicated that they did not decide to recognise the *LQN* ruling as *ultra vires* mainly due to the way in which such a position would be perceived in EU states struggling with a crisis of democratic governance.[105] Nevertheless, the legal construction adopted by the Council seems to exacerbate the instability of the legal order in these states. It affords opportunity for constitutional courts dependent on those

[104] *See* '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⟩, visited 3 November 2021.

[105] J.B. Jacquin, 'Le Conseil d'Etat autorise la poursuite de la conservation généralisée des données', *Le Monde,* 21 April 2021, ⟨https://cli.re/Vbaq19⟩, visited 3 November 2021.

in power[106] to question the EU standard for surveillance of a country's own citizens based on criteria of threat to internal security that are difficult to verify and not transparent.

Positions of the Belgian Cour constitutionnelle and the UK Investigatory Powers Tribunal

The day after the Conseil d'État announced its judgment, the Belgian Constitutional Court also announced its own ruling on the national retention legislation. Referring to the reasoning presented in the *LQN* case, the constitutional court noted that the adoption of the Court of Justice's interpretation requires a change in the perspective of the national legislature so that data retention constitutes an exception rather than a rule for interference with the rights of users of electronic communications.[107] The application of such a measure should therefore be subject to clear and precise restrictions setting limits both on the scope and on the duration of the measure.

Since the Belgian retention model did not establish a framework of bulk transfer of metadata to security services, this aspect of the Court of Justice's decision remained outside the detailed analysis of the Cour constitutionnelle. At the same time, the constitutional court focused on assessing whether the generalised form of data retention present in the national legislation – also used for national security purposes – met the criteria defined by the Luxembourg Court.

In principle, the Belgian legislation established a 12-month data retention period, and its distinction between identification data, access and connection data, and communication data was introduced solely to define the event from which the period should be calculated.[108] Therefore, in the view of the constitutional court, since the *LQN* judgment has predetermined that the establishment of a general obligation to retain traffic data and location data on a permanent and preventive basis is not permissible, such an interpretation must lead to the annulment of the national retention rules. Significantly, in its reasoning, the constitutional court also pointed out that it was not possible to delay the entry into force

[106] *See* a recent ruling by the European Court of Human Rights in which the Court found that the judgment of the Polish Constitutional Tribunal issued by a panel of judges that had been elected in a manner inconsistent with the constitution led to a violation of the right to a fair trial: ECtHR 7 May 2021, No. 4907/18, *Xero Flor* v *Poland*; M. Szwed, 'What Should and What Will Happen After Xero Flor', *Verfassungsblog*, 9 May 2021, ⟨https://cli.re/KarKdx⟩, visited 3 November 2021.

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

[108] *See* Art. 126(3) of the Act of 13 June 2005 on electronic communications, *supra* n. 34.

https://doi.org/10.1017/S1574019621000353 Published online by Cambridge University Press

of the judgment – which means that the contested regulations were repealed as of the date on which the judgment was published in the Official Journal.[109]

The Belgian Constitutional Court thus interpreted the position expressed in the *LQN* judgment in a manner diametrically opposed to that of the French Council of State. Not only did it make no attempt to suggest that a generalised data retention obligation could be applied because of the permanent state of emergency in which the state operates, it also supported the Court of Justice's reasoning by emphasising that the application of a measure such as data retention needs to be considered as an exception rather than a norm characterising the activity of public authorities.

As a result, one day apart, in two neighbouring European countries sharing the same legal culture and being members of both the European Union and the European Convention on Human Rights, the highest courts came to fundamentally different conclusions when interpreting the same judgment of the Court of Justice.

The Court of Justice's judgment was interpreted in a similar way by the Investigatory Powers Tribunal in the UK. In the context of UK's case, the purpose of the questions referred was primarily to establish whether the regime of bulk metadata collection falls within the scope of application of EU law. In its judgment of 22 July 2021, the IPT noted that 'in the light of the judgment of the CJEU, which is binding on this Tribunal, it is now clear that section 94 of the 1984 Act was incompatible with EU law'.[110] It should be noted that, in the light of arguments presented by the Luxembourg Court, the British government also recognised the flaws in the domestic regulation – indicating, inter alia, the excessive powers of the Secretary of State in making decisions justified by national security, the lack of time limit on measures introduced using these powers and the failure to establish oversight mechanisms exercised by courts or by an independent administrative authority.[111]

Though the declaration of the Investigatory Powers Tribunal related to legislation that is no longer in force, this should not diminish its relevance. In the UK there has been discussion for years on the scope of national surveillance regulations. Suffice it to say that the provisions of the Telecommunications Act 1984 challenged in the *Privacy International* case have been replaced by the Investigatory Powers Act 2016, which was also found in 2018 to be partially incompatible with EU law.[112] Therefore, although the Investigatory Powers

[109] *See* Cour constitutionnelle 22 April 2021, *supra* n. 107, para. B.24.2.

[110] *Privacy International* v *Secretary of State for Foreign and Commonwealth Affairs* [2021] UKIPTrib IPT_15_110_CH, para. 28.

[111] ibid., paras. 19-21.

[112] *Liberty* v *Home Office* [2018] EWHC 975 (Admin).

Tribunal declaration does not have the effect of repealing applicable regulations, it will certainly be an important contribution to the discussion on secret service competences to conduct domestic surveillance.

Conclusions

With the *Privacy International* and *LQN* judgments, the European Court of Justice detailed the conditions under which national data retention measures can be considered compatible with EU law. By clarifying uncertainties regarding the scope of the national security exception, the Court determined that the pursuit of public security objectives *per se* does not justify taking disproportionate measures. The Court, responding to the criticism of its earlier judgments, also entered into a discussion on the conditions that would have to be met for the application of generalised data retention to be reconciled with fundamental rights.

The reception of the judgments by the referring courts demonstrates that the interpretation provided by the Court of Justice will not contribute, in the short term, to developing a universally accepted standard for the assessment of national retention rules. In the long run, this problem may hinder not only the development of the digital single market but also the modernisation of the EU from an organisation focused on economic cooperation into a union of values based on respect for human rights. Indeed, the risk of the spread of two incompatible standards of implementation of retention rules in the member states is becoming a reality. In the first of them, data retention will be an exception applied according to the principles of necessity and proportionality. In this model, generalised data retention will be a measure reserved for emergencies. A different standard will apply in states justifying the use of extensive surveillance powers on the ground of a continuing terrorist threat. As the scale of serious crime (in which the Council of State also included cybercrime) is not expected to decrease over time, these states will easily be able to justify the need for further extensive data retention measures.[113]

It seems that the interpretation provided by the Court of Justice is not enough to ensure harmonisation of national laws. The Court has clearly explained both the conditions for the application of data retention and the reasons why extensive forms of its application cannot be considered compatible with the European model of fundamental rights. Some member states are already arguing that the

[113] *Cf* M. Cayford and W. Pieters, 'The effectiveness of surveillance technology: what intelligence officials are saying', 34 *The Information Society* (2018) p. 88.

https://doi.org/10.1017/S1574019621000353 Published online by Cambridge University Press

position of the Court of Justice is too restrictive and even exceeds the standard applied by the European Court of Human Rights. It is true that the Strasbourg Court – especially in its recent judgments – has found the use of some forms of bulk surveillance to be in accordance with the Convention.[114] However, it should be borne in mind that the European Convention sets a minimum standard, not a maximum one, for the interpretation of the rights and freedoms set out in the Charter of Fundamental Rights. Therefore, the fact that the Strasbourg Court accepts extensive surveillance measures as permissible under the Convention should not predetermine the fact that these measures should also be applied uncritically within the EU.[115]

The increasing polarisation of views on data retention requires the search for new alternative solutions. The Court of Justice itself proposed such a third way when examining the admissibility of the use of algorithmic data analysis. In principle, the Court did not consider such a measure to be incompatible with EU law even if it was intended to process bulk data. Therefore, it appears that the construction of a mechanism that would impose the obligation on telecom operators to pre-filter metadata according to rules established by authorised services and under court supervision may be a starting point for further discussion. The aim would be to develop a new form of retention combining the features of targeted and generalised retention that would be both compatible with the information needs of secret services and acceptable in terms of human rights protection standards. A measure of this type is already used in some countries. An example is the Swedish electronic intelligence service, which has the power to intercept and record communications that are selected with the aid of search terms established according to objective and non-discriminatory criteria.[116] Hence, the Swedish

[114]This is particularly the case in ECtHR 19 June 2018, No. 35252/08, *Centrum för rättvisa* v *Sweden*, in which the European Court of Human Rights found no violation of the Convention by a national measure of bulk collection of telecommunications data on the basis of approved filtering criteria and under court oversight. In its opinion, the Strasbourg Court held, *inter alia*, that the retention of data for a period of 12 months does not constitute an interference with the right to privacy because the data are not processed (*see* para. 146). This conclusion was also repeated in the Grand Chamber judgment (25 May 2021, para. 343).

[115]Against this background, it should also be remembered that the scope of application of the Convention covers a much wider circle of states – in particular, also countries not belonging to the EU. It is therefore understandable that the Strasbourg Court, in its search for a common standard on the basis of the Convention, goes beyond the legal model applied in the EU.

[116]For a broader discussion of the case *see* P. Vogiatzoglou, 'Centrum för Rättvisa v Sweden: Bulk Interception of Communications by Intelligence Services in Sweden Does Not Violate the Right to Privacy', 4 *European Data Protection Law Review* (2018) p. 563.

model may serve as an inspiring example of how to find workable solutions to the problem of data retention in order to provide state security services with adequate capacity for action and, at the same time, ensure respect for the case law of both the Court of Justice and the European Court of Human Rights.[117]

[117]In May 2021, the Grand Chamber of European Court of Human Rights issued its long-awaited judgment in the case of *Centrum för rättvisa* v *Sweden*, *supra* n. 114, partially changing the Court's previous ruling and pointing out elements of Swedish surveillance legislation that are not in accordance with the Convention. The Grand Chamber's verdict should be regarded as leading to improvement of the Swedish surveillance model and not pointing to its uselessness or the need for a thorough change.