INSIGHT

CASE *PROKURATUUR*: PROPORTIONALITY AND THE INDEPENDENCE OF AUTHORITIES IN DATA RETENTION

SOPHIA ROVELLI*

ABSTRACT: Records of electronic communication metadata allow detailed conclusions about habits of daily life, such as places of residence, activities carried out, or social relations. This data can therefore be useful in criminal investigations. The CJEU elaborated in case *Prokuratuur* (case C-746/18 ECLI:EU:C:2021:152) on the conditions of access to such data. The court interpreted art. 15(1) of the Directive 2002/58/EC on privacy and electronic communications and ruled that access to traffic and location data may be provided to combat severe crime or to prevent serious public security threats. This interference with the fundamental rights enshrined in arts 7 and 8 of the Charter of Fundamental Rights when accessing traffic and location data is grave, regardless of the period granted for data access or the amount of data requested. The prosecution of less serious crimes can therefore not justify such intervention. According to Estonian law, the Public Prosecutor's Office has the task of conducting the criminal investigation and, if necessary, initiating prosecution in court. Consequently, it cannot be regarded as an independent authority to decide on access to traffic and location data for criminal investigations. As a basis for the presentation and discussion of the *Prokuratuur* decision by the CJEU, the facts of the case are briefly outlined before previous case law regarding data retention is summarised.

KEYWORDS: data retention – principle of proportionality – independent authority – evidence – fundamental rights – data protection.

I. FACTS OF THE CASE

The person concerned had been sentenced to two years in custody. The alleged crimes were thefts using another person's bank card and acts of violence against a person involved in the proceedings.[1]

Part of the evidence brought forward was data relating to electronic communications.[2] The Estonian Public Prosecutor's Office gathered this data from an electronic telecommunication service provider. Estonian law requires providers to store traffic and

* Research Assistant, University of Fribourg, sophia.rovelli@unifr.ch.

[1] Case C-746/18 *Prokuratuur* ECLI:EU:C:2021:152 para. 16.

[2] *Ibid*. para. 17.

ISSN 2499-8249
doi: 10.15166/2499-8249/469

location data generally and indiscriminately for one year. This obligation involves the following data: name and address of both parties of the call, date and time of the start and end of the call, the device used, the cell ID at the start of the call, and the geographical location. According to national law, data access can be granted if it is essential for use in criminal proceedings.[3]

Subsequently, the verdict was challenged on the grounds of evidence not legally obtained. The court of appeal rejected the claim. The Estonian Supreme Court (*Riigikohus*) referred the case to the CJEU requesting an interpretation of art. 15(1) of the Directive 2002/58/EC.[4]

II. Directive on privacy and electronic communications

According to Directive 2002/58/EC (the Directive), Member States have to ensure the confidentiality of communication and related traffic data.[5] Traffic data is data that is processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.[6] Location data is data processed in an electronic communications network indicating the geographic position of the terminal equipment of a user of a publicly available electronic communication service.[7] Electronic telecommunication service providers have to erase traffic data or make it anonymous before processing, except when it is necessary for subscriber billing and interconnection payments.[8] Location data other than traffic data may be processed when made anonymous or with the users' consent.[9] The Directive seeks to ensure full respect for the fundamental rights set out in arts 7 and 8 of the Charter.[10]

Art. 15 contains exceptions to those principles laid down by the Directive. According to this article, Member States can adopt legislative measures to restrict rights and obligations. However, those restrictions have to be necessary, appropriate, and proportionate.[11]

[3] *Ibid*. para. 9 ff.

[4] *Ibid*. para. 18 ff.

[5] 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), art. 5.

[6] *Ibid*. art. 2(b).

[7] *Ibid*. art. 2(c).

[8] *Ibid*. art. 6.

[9] *Ibid*. art. 9.

[10] *Ibid*. recital n. 2.

[11] *Ibid*. art. 15.

III. Overview of the existing case-law regarding data retention

This judgment follows widely discussed court decisions concerning data retention regulation[12]. Some of these findings will be presented briefly, as they served as a basis for the referring court's questions and the decision of the CJEU.

In C-293/12 and C-594/12 (*Digital Rights a.o.*), the CJEU declared the European Data Retention Directive 2006/24/EG invalid because of its interference with the fundamental rights protected by the Charter.[13] The CJEU's reasoning for its decision was that the interference allowed by the directive was not limited to the strictly necessary.[14] The Directive did not contain clear and precise rules concerning the scope and application of the measure, nor did it impose minimum safeguards to provide sufficient guarantees against unlawful access or use of data. The directive applied to all means of electronic communication and was not restricted to data pertaining to a particular time period, a particular geographic area, or a particular circle of persons.[15] Furthermore, there was no objective criterion to determine when data access should be allowed, as the directive simply refers in a general manner to serious crime as defined by each Member State.[16] The court also highlighted that substantive and procedural conditions relating to the access of the competent national authorities were missing.[17] The directive also failed to establish an objective criterion to limit the number of persons authorised to access data[18] and to set a data retention period.[19]

In *Tele2 Sverige and Watson and Others*, the Court evaluated whether a national regulation that obligates private electronic communication providers to retain data that falls under Directive 2002/58/EC is valid or if art. 1(3) is applicable. According to art. 1(3), the Directive does not apply to activities that fall outside the scope of the Treaty establishing the European Community (such as activities concerning public security, defence, state security and the ac-

[12] 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).

[13] Joined cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* ECLI:EU:C:2014:238 para. 68 ff.

[14] *Ibid*. para. 65.

[15] *Ibid*. paras 56 and 59.

[16] *Ibid*. para. 60.

[17] *Ibid*. para. 61.

[18] *Ibid*. para. 62.

[19] *Ibid*. para. 64. See T Wisman, 'Privacy: Alive and Kicking' (2015) Eur Data Prot L Rev 80; M Abu Bakar, S Mohd Yasin and S Abu Bakar, 'Data Retention Rules: A Dead End' (2017) EUr Data Prot L Rev 71; E Celeste, 'The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios' (2019) European Constitutional Law Review; MP Granger and K Irion, 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling off the EU Legislator and Teaching a Lesson in Privacy and Data Protection' (2014) European Law Review 835.

tivities of the state in areas of criminal law). The court concluded that the article is not applicable because private entities store the data. The directive is also applicable when evaluating the rights to access stored data. Notably, art. 15(1) would be largely meaningless if the directive was not applicable, as this exception could never come into use.[20]

The court found that the general rule of art. 5(1), which ensures the confidentiality of communications, can be deviated from according to art. 15(1). However, according to the court, art. 15(1) must be interpreted strictly; it exhaustively regulates the list of objectives,[21] and restrictions must be limited to the strictly necessary.[22] The court made clear that stored traffic and location data allow for extensive conclusions on individuals' private lives;[23] therefore, access should only be granted for the prosecution of serious crimes.[24] In addition, the court stated that unrestricted data retention without fixed limits is inadmissible. The following must be specified: categories of the data stored, the devices and persons concerned, and the duration of the data storage.[25] The court went on to state that Member States have to put forward sufficient guarantees to prevent abuse of data,[26] and national regulation has to be clear and precise concerning the scope and application of a data retention measure. There must be an objective criterion that establishes a link between the data to be retained and the objective pursued. In a special situation, data access could be justified if there were objective expectations that the data could contribute to the purpose. Such a particular situation could be represented by the state's vital interests, such as combatting severe crime or serious threats to public security.[27] Access to the data has to be authorised by a court or an independent authority.[28]

In decision (C-207/16), *Ministerio Fiscal*, the question brought forward by a Spanish court was whether the investigation of non-serious crime could justify an exception according to art. 15(1) of Directive 2002/58/EC.[29] The investigating authority asked different

[20] Joined cases C-203/15 and C-698/15 *Tele2 Sverige* ECLI:EU:C:2016:970 para. 69 ff. See A Møller Pedersen, H Udsen and S Sandfeld Jakobsen, 'Data Retention in Europe – The Tele 2 Case And Beyond' (2018) 8 International Data Privacy Law 160, 163.

[21] *Tele2 Sverige* cit. para. 89 ff.

[22] *Ibid*. para. 96.

[23] *Ibid*. para. 98 ff.

[24] *Ibid*. para. 102.

[25] *Ibid*. para. 106 ff.

[26] *Ibid*. para. 109.

[27] *Ibid*. para. 110 ff.

[28] *Ibid*. para. 120 ff. See X Tracol, 'The Judgment of the Grand Chamber Dated 21 December 2016 in the Two Joint Tele2 Sverige And Watson Cases: the Need for a Harmonised Legal Framework on the Retention of Data at EU Level' (2017) Computer Law & Security Review 541; A Møller Pedersen, H Udsen and S Sandfeld Jakobsen, 'Data Retention in Europe – The Tele 2 Case And Beyond' cit.; C Docksey and H Hijmans, 'The Court of Justice as a Key player in Privacy and Data Protection: an Overview of Recent Trends in Case Law at the Start of a New Era of Data Protection Law' (2019) Eur Data Prot L Rev 300. E Celeste, 'The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios' cit.

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

electronic communication providers to divulge the name, telephone number, and address related to terminal equipment in order to identify phone thieves. The CJEU ruled that the data request was an infringement of the rights established by the Charter. However, since the requested data was limited and not related to traffic or location data, it would not be possible to draw precise conclusions about the private lives of the persons concerned. Hence, this is not to be classified as a grave infringement and can therefore be justified for the purposes of prevention, investigation, and prosecution of criminal offences. Further, exceptions to art. 15(1) are not limited to the investigation of serious crimes but would also allow an exception for criminal offences in general.[30]

In the decisions *La Quadrature du Net a.o.* and *Privacy International,* the court confirmed its previous case law.[31] Further, it specified that general preventive storage could be admissible to prevent a serious threat to national security. The responsibility for national security lies with each Member State. This responsibility enfolds the primary interest of protecting the essential functions of the state and the fundamental interests of society. It encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic, or social structures of a country and, in particular, of directly threatening society, the population, or the state itself, such as terrorist activities.[32] Those threats can be distinguished from general disturbances that affect public security by their nature and particular seriousness. With the objective of safeguarding national security, there are, therefore, more serious interferences with fundamental rights (in regard to art. 52(1) of the Charter) than with other objectives. [33] The retention of traffic and location data of all users of electronic communications systems for a limited period of time can, therefore, be justified when the Member State is confronted with a serious threat to national security. This threat has to be genuine and present or foreseeable.[34] The intrusion

[30] *Ibid*. para. 59 ff. See C Docksey and H Hijmans, 'The Court of Justice as a Key player in Privacy and Data Protection: an Overview of Recent Trends in Case Law at the Start of a New Era of Data Protection Law' cit.; E Celeste, 'The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios' cit.

[31] Joined cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others* ECLI:EU:C:2020:791; case C-623/17 *Privacy International* ECLI:EU:C:2020:790; J Sajfert, 'Bulk data interception/retention judgments of the CJEU – A victory and a defeat for privacy' (26 October 2020) European Law Blog europeanlawblog.eu; W Maxwell, 'La CJUE dessine le noyau dur d'une future regulation des algorithms' (19 January 2021) Légipresse # 388 www.legipresse.com; P Vogiatzoglou and J Bergholm, 'Privacy International & La Quadrature du Net : the latest on data retention in the name of national and public security, Part I-III, (15-19-27 October 2020) KU Leuven Centre For IT & IP Law www.law.kuleuven.be; L Woods, 'When is mass surveillance justified? The CJEU clarifies the law in Privacy International and other cases' (7 October 2020) EU Law Analysis: Expert insight into EU law developments eulawanalysis.blogspot.com; M Ogorek, 'EuGH: Anlasslose Vorratsdatenspeicherung nur bei erheblicher Gefahrenlage' (2021) NJW 531; A Sandhu 'Datenschutzrecht: Anlassbezogene Vorratsdatenspeicherung nur bei erheblicher Gefahrenlage' (2021) EuZW 209.

[32] *La Quadrature du Net and Others* cit. para. 135.

[33] *Ibid*. para. 136.

[34] *Ibid*. para. 137.

has to be limited to the strictly necessary, and the duration cannot exceed a foreseeable time. Limitations and strict safeguards must be put in place to make it possible to effectively protect the personal data of the persons concerned against the risk of abuse. Data retention of a systematic nature would not be admissible.[35]

IV. Highlights of the CJEU judgment

In C-746/18, the court analyses art. 15(1) of Directive 2002/58/EC in light of arts 7, 8, and 11 and art. 52(1) of the Charter. The court starts by examining whether a provision allowing access to traffic and location data to combat general crime is compatible with the fundamental rights if the access is not significant (both in terms of the type of data and its temporal extent).[36]

The court recalls that access to traffic and location data must fulfil the obligation according to art. 15(1).[37] In conformity with fundamental rights, art. 15(1) precludes general and indiscriminate traffic and location data retention. Access can only be justified by an objective that serves the public interest.[38] Since the Directive's rights and obligations are limited, the severity of the interference by the limitation must be assessed and verified according to whether the public interest pursued by the limitation is proportionate to the seriousness of the interference.[39]

The relevant Estonian provision obligates electronic communication providers to generally and indiscriminately retain traffic and location data for one year. The data in question allows the identification of persons participating in phone communications. Further modalities such as date, time, duration of the phone call, communication device, and location are stored. Additionally, the frequency of phone calls with a certain person can be established with the help of the data.[40] When investigating a crime, the competent authorities can request the retained data regardless of the severity of the alleged offence.

The court refers to its case law, stating that the retention of traffic and location data is a severe interference with the fundamental rights of the Charter. Severe interference occurs regardless of whether the storage is of a general, indiscriminate, or targeted nature. Accordingly, only objectives related to combatting serious crime and preventing serious threats to public security can justify such infringement on fundamental rights.[41] Otherwise, the principle of proportionality would not be respected, as it constitutes a

[35] *Ibid*. para. 138.

[36] *Prokuratuur* cit. para. 27 ff.

[37] *Ibid*. para. 29.

[38] *Ibid*. para. 31.

[39] *Ibid*. para. 31 ff.; *La Quadrature du Net and Others* cit. para. 131; *Ministerio Fiscal* cit. para. 55; *Tele2 Sverige* cit. para. 99; *Digital Rights* cit. para. 27.

[40] *Prokuratuur* cit. para 28.

[41] See also *La Quadrature du Net a.o.* cit. paras 140 and 146.

serious infringement into the fundamental rights enshrined in arts 7 and 8 of the Charter.[42] However, if the encroachment on fundamental rights is not severe, the aim of combatting general crime can justify the interference.[43]

The traffic and location data to be stored *in casu* allow precise conclusions about the individuals' private lives. Conclusions can be reached regarding daily habits, permanent or temporary places of residence, daily or other regular changes of location, activities carried out, and information on social relations and the social environment.[44]

Other factors relating to the proportionality of an access request cannot justify access to investigate general crime. However, the competent national authority must examine the category of data and the period thereof to be disclosed in each case. These modalities do not play a role when questioning the admissibility of access to a set of traffic and location data itself, since there is always a severe encroachment on the data subjects' fundamental rights, irrespectively of the period, amount, or type of data. Even access over a short period or a limited amount of data can reveal detailed private information about the user. The precise information that can be drawn from the data and its scope can only be assessed after the access. Therefore, the concrete danger to private life is not known beforehand. Instead, the general danger associated with such an intrusion has to guide the decision.[45] Therefore, the court concludes that access to retained traffic and location data cannot be justified when investigating general crimes.

In the judgment, the CJEU also evaluates the requirements of an independent authority according to Union law,[46] namely, whether a public prosecutor's office conducting the investigation and, if necessary, undertaking the public prosecution would comply with these requirements.

As has been pointed out in the previous CJEU decisions, the conditions concerning data access circumstances are to be regulated by national law.[47] However, the requirement of proportionality demands that the regulation clearly and precisely provides for the scope and application of the measure, describing the minimum requirements. Only in this way will the persons concerned receive sufficient guarantees to ensure adequate protection against abuse. The national regulation must be binding.[48]

Not only must the purpose comply with art. 15(1), but the material and procedural conditions for the use of data must also be established.[49] General access to all stored

[42] *Ibid*. para. 33.
[43] *Ibid*.
[44] *Ibid*. para. 35 ff.
[45] *Ibid*. para. 37 ff.
[46] *Ibid*. para. 46 ff.
[47] *Ibid*. para. 48.
[48] *Ibid*. para. 48.
[49] *Ibid*. para. 49.

data is not limited to what is strictly necessary. Therefore, national regulation must ensure that the determination of the circumstances and conditions for access to data be based on objective criteria Access to traffic and location data may only be granted for the purpose of the prosecution of serious criminal offences, national security interests, national defence, or public safety.[50]

To comply with these conditions, access to data must be subject to prior control by a court or a competent administrative authority. This prior control requires that the competent body have all powers and guarantees necessary to ensure that conflicting interests can be taken into consideration. This means that in the case of a criminal investigation, the court or body must be able to strike a fair balance between the interest in investigating crime and the fundamental rights of respect for private life and protection of personal data.[51] Thus, the body must perform its task objectively and impartially without influence from other parties.[52] On the one hand, this means that the competent authority must not be involved in the investigation procedure and, on the other hand, that it is has a neutral stand towards the parties to the criminal proceedings.[53]

The Estonian Public Prosecutor's Office, which conducts preliminary investigations and represents the public in prosecutions, is not independent as required by EU law. It cannot make independent decisions regarding evidence when it is expected to pursue a case in court. The office is obliged to examine the incriminating and exculpating aspects of the evidence and is only bound by the law. However, these constraints are insufficient to adequately consider the interests as if weighed by a third party.[54] Furthermore, subsequent judicial review cannot compensate for this lack of independent review since prior control aims to ensure that only necessary data is disclosed.[55] The judgment is, therefore, that a body such as the Public Prosecutor's Office, which conducts preliminary investigations, lacks the necessary independence to ensure an unbiased preliminary review of data access.

V. Commentary

With this ruling, the CJEU has further clarified its case law on data retention regarding which objectives can justify access to stored traffic and location data and which bodies are competent to decide on the question of access.[56] The court confirms that access to

[50] *Ibid*. para. 50.
[51] *Ibid*. para. 52.
[52] *Ibid*. para. 53.
[53] *Ibid*. para. 54.
[54] *Ibid*. para. 50 ff.
[55] *Ibid*. para. 58.
[56] See I Revoloidis, 'H.K. v Prokuratuur: On Balancing Crime Investigation and Data protection' (2020) 6 Eur Data Prot L Rev 319; J Lund 'CJEU upholds strict requirements for law enforcement access to electronic communications metadata' (10 March 2021) EDRi edri.org; A Förster 'Eurparechtliche Vorgaben für die Vorratsdatenspeicherung' (2021) GRUR-Prax 212.

stored traffic and location data is a severe interference with fundamental rights and, therefore, can only be justified when serving the prosecution of severe crimes. The court confirmed that the period of data access and the categories of data requested must be considered when evaluating the proportionality of an interference. However, the data access modalities cannot lead to a situation where severe intrusions could be justified for the prosecution of general criminal offences. Here, the arguments of the court differ from those of the Advocate General. According to the Advocate General, very limited access, ranging from only a few hours to days, cannot be compared to retrieving data over several months. He argues that the conclusions that can be drawn from the data are likely more extensive when the period covered by the access is longer.[57] Very limited access could, therefore, be justified by the prosecution of general criminal offences as the infringement would not be severe. The length of the required access and the type of data concerned would need to be taken into account when deciding whether data access for the prosecution of general offences is justified.[58]

Here, the Court of Justice's arguments are convincing, as they confirm that various factors must be assessed in each case when deciding whether to allow the requested data. Thus, the competent authority has to examine *ex-ante* whether the requested period and data categories are necessary to investigate a criminal offence. However, traffic and location data are generally sensitive because they allow for far-reaching conclusions about private life. It is impossible to know what information can be derived from the data in advance, which is why access to this data must generally be considered a severe intrusion.

While the court's first decisions clearly upheld the necessity of protecting privacy, the subsequent decisions specified and relativised the conditions for data retention. This decision, however, prevents softening the requirements even further. Instead, the interpretation of art. 15 regarding access to traffic and location data is restricted to investigating serious crimes. Traffic and location data may include information on sensitive areas such as sexual orientation, political opinions, religious, philosophical, social or other beliefs, and health status, with such data otherwise enjoying special protection under Union law. Moreover, these data can lead to accurate conclusions concerning private life when combined (i.e., a personality profile). In terms of respect for private life, this profile is information that is just as sensitive as the content of the communication. In this respect, the limitation to data access for the prosecution of serious crimes is to be welcomed.

However, defining what constitutes a serious crime is still up to the Member States. As with the concept of national security, there is a risk that Member States will interpret

[57] Case C-746/18 *Prokuratuur* ECLI:EU:C:2020:18, opinion of Advocate General Pitruzzella, para. 82.
[58] *Ibid*. para. 82.

it broadly.[59] Interestingly, constitutional courts that have treated similar questions did not always specify what constitutes a serious crime.[60]

The other aspect of the judgment regarding the Estonian Public Prosecutor's Office, which is in charge of the investigation and, if appropriate, the public prosecution in court (i.e., the premise that it cannot be considered an independent authority with access to the stored data), is also convincing. The requirement of a court or an independent body to review access is the most important procedural requirement.[61] This requirement would be undermined if the authority in charge of investigating the crime could decide on data access.

Another point touched on by the Advocate General that might be examined in prospective proceedings was whether an independent internal authority could be considered to have the necessary independence to make decisions on data access. In the discussed case, the investigating authority was organised hierarchically. Even if there was a clear internal distinction between investigation and deciding on data access, this would probably not be easily visible from the outside. It can therefore be questioned if this would constitute a sufficiently independent authority.[62]

One can observe the difficulty of balancing different legitimate goals in these decisions on data retention by the highest courts of Europe.[63] After all, when evaluating data retention, the interest in public security and law enforcement's efficacy must be weighed against fundamental rights and principles of the rule of law, especially the principle of proportionality.[64] Both sides are important public interests in a democratic constitutional state.[65] The balancing and assessment of the significance of the conflicting interests are subject to change with time. Notably, after major events such as terrorist attacks, there has been a shift towards a demand for more security measures and, therefore, also for

[59] See J Sajfert, 'Bulk data interception/retention judgments of the CJEU – A victory and a defeat for privacy' cit.

[60] *Ibid*. 241 ff.

[61] M Zubik, J Podkowik and R Rybski, 'Judicial Dialogue on Data Retention Laws in Europe in the Digital Age: Concluding Remark' cit. 242.

[62] See *Prokuratuur*, opinion of Advocate General Pitruzzella, cit. para. 123 ff.

[63] See E Pache, 'Art. 52 GRch' in M Pechstein, C Nowak and U Häde (eds), *Frankfurter Kommentar AUV, GRC, AEUV* (Mohr Siebeck 2017) para. 24 ff.; ECtHR *Big Brother Watch v. UK* App. n. 58170/13 [13 September 2018]; ECtHR *Breyer v. Germany* App. n. 50001/12 13 [30 January 2020].

[64] M Zubik, J Podkowik and R Rybski, 'Judicial Dialogue On Data Retention Laws in Europe in The Digital Age: Concluding Remark' in M Zubik, J Podkowik and R Rybski (eds), *European Constitutional Courts towards Data Retention Laws* (Springer Nature 2021) 230; S Stallla-Bourdillon, J Phillips and M Ryan, *Privacy vs. Security* (Springer 2014) 65 ff.; A Epiney 'Staatliche Überwachung versus Rechtsstaat: Wege aus dem Dilemma?' (2016) AJP 1503 ff.

[65] S Stallla-Bourdillon, J Phillips and M Ryan, *Privacy vs. Security* cit. 65 ff.; A Epiney 'Staatliche Überwachung versus Rechtsstaat: Wege aus dem Dilemma?' cit.

data retention.[66] Data retention is also seen as a useful instrument to prevent or investigate serious crime such as drug trafficking or sexual exploitation of children.[67] Depending on how access is implemented, bulk data retention could be less intrusive into private life than targeted interceptions.[68]

However, it is worth noting that laws that were made for the purpose of combatting terrorism and organised crime have been used afterwards for different purposes.[69] As discussed here in the case of *Prokuratuur*, these laws have been used, at times, to combat ordinary crime.[70] As already mentioned, electronic communication metadata is likely to result in a high risk to the rights and freedoms of natural persons. The storage of data may prevent people from exercising their opinions.[71] Also, arts 7 and 8 of the Charter are an embodiment of the universal human need for privacy. [72]

Privacy and data protection are fundamental to democratic decision-making and a precondition for exercising other fundamental rights.[73] Simultaneously, however, the CJEU recognised positive obligations to take legal measures to combat crime to protect fundamental rights (arts 3, 4, and 7 of the Charter).[74] This means that not only public interests but also guarantees protected by fundamental rights must be weighed against each other.

Directive 2002/58/EC, discussed in this judgment, will prospectively be replaced with the e-privacy regulation, which is currently being negotiated.[75] The e-privacy regulation

[66] M Zubik, J Podkowik and R Rybski, 'Judicial Dialogue on Data Retention Laws in Europe in The Digital Age: Concluding Remark' cit. 230 ff.

[67] ECtHR *Big Brother Watch v. UK* App. n. 58170/13 [9 January 2014] para. 314.

[68] *Ibid*, para. 316.

[69] *Ibid*. 230 see overview on page 234 and 241 ff.

[70] *Ibid*.

[71] *Digital Rights* cit. para. 28; *Tele2 Sverige* cit. para. 101. See A Roberts, 'Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v. Minister for Communications' (2015) 78 Mod L Rev 535, 542 ff.

[72] Privacy includes the freedom to live and shape one's life autonomously and protects communication. art. 7 provides a right to defence against governmental interference with privacy. This includes having control over the disclosure of information about one's identity. A Weber 'Kommentar art. 7' in K Stern, M Sachs (eds), *Europäische Grundrechte-Charta GRCh Kommentar* (CH. Beck 2016) para. 1 ff.

[73] See A Epiney 'Staatliche Überwachung versus Rechtsstaat: Wege aus dem Dilemma?' cit. para. 1506.

[74] *La Quadrature du Net and Others* cit. para. 126.

[75] Proposal for 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, Brussels, 10 February 2021). See A Møller Pedersen, H Udsen and S Sandfeld Jakobsen, 'Data Retention in Europe – The Tele 2 Case And Beyond' cit. 173; X Tracol, 'The Judgment Of The Grand Chamber Dated 21 December 2016 In The Two Joint Tele2 Sverige And Watson Cases: the Need for a Harmonised Legal Framework on the Retention Of Data at EU Level' cit. 551.

should align the existing legal bases with the GDPR.[76] However, the goal to replace the Directive by 2018 was missed by far. After different drafts, the Council finally agreed on a proposal on 5 January 2021.[77] This proposal allows the start of a trilogue between the Commission, the Council, and the Parliament. In this new proposal, some changes were made compared to the original proposal of 2017, although no material changes were made to the articles relevant to this *Insight*. The confidentiality of electronic communications is upheld in art. 5. According to art. 11 of the proposed regulation, the Union or a Member State can adopt legislative measures to restrict the obligations and rights provided for in arts 5 through 8. These restrictions may be made under the condition that they respect the essence of fundamental rights and freedoms. They must also be necessary, appropriate, and proportionate measures to safeguard the public interest in a democratic society according to art. 23(1)(c) to (e), (i) and (j) of Regulation (EU) 2016/679 (GDPR).

The European Data Protection Board (EDPB) has expressed its opinion on the proposal,[78] emphasising how important it is to adapt the GDPR framework.[79] After all, the e-privacy regulation is not intended to diminish the protection provided by the current Directive.[80] Therefore, the EDPB is advocating that the e-privacy regulation not deviate from the aforementioned CJEU case law. Accordingly, current or future legal bases that provide for non-targeted data retention for purposes of law enforcement and safeguarding national security would not be compatible with the Charter. Further, the EDPB emphasises that legislation should not derogate from the obligation for strict temporal and material limitations and a review by a court or an independent authority.[81]

Therefore, the principles outlined in this judgment should not change under the new regulation. However, the discussion and mitigation of colliding interests will continue in the future. Further preliminary ruling proceedings concerning this question are pending,[82] and there are Union level political efforts for a new data retention regulation.[83]

[76] Other than the directive the regulation would be directly applicable in Member States. See X Tracol, 'The Judgment of the Grand Chamber Dated 21 December 2016 in the Two Joint Tele2 Sverige And Watson Cases: The Need for a Harmonised Legal Framework on the Retention of Data at EU Level' cit. 551; C Etteldorf, 'EDPB on the Interplay between the ePrivacy Directive and the GDPR' (2019) Eur Data Prot L Rev 224.

[77] Proposal for 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, Brussels, 10 February 2021).

[78] Statement 03/2021 of the European Data Protection Board on the ePrivacy Regulation Adopted on 9 March 2021.

[79] *Ibid*. 1.

[80] *Ibid*.

[81] *Ibid*. 1 ff.

[82] Case C-793/19 *SpaceNet* pending; case C-794/19 *Telekom Deutschland* pending; case C-817/19 *Ligue des droits humans* pending; case C-140/20 *Commissioner of the Garda Síochána u.a.*; case C-397/20 *SR*.

[83] A Fanta, 'France, Spain push for new EU data retention law' (5 March 2021) Netzpolitik.org.