Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance

Court of Justice of the European Union, Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*

Tuomas Ojanen*

INTRODUCTION

On 8 April 2014, the Court of Justice of the European Union (the Court or ECJ) ruled that 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 ('Data Retention Directive')[1] is invalid.

The judgment was issued within the preliminary reference procedure under Article 267 Treaty on the Functioning of the European Union in two cases in which the High Court (Ireland) and the *Verfassungsgerichtshof* (Austria) had asked the Court to examine the validity of the Data Retention Directive in light of Article 7 (the respect for private life and communications), Article 8 (the protection of personal data) and Article 11 (respect for freedom of expression) of the Charter of Fundamental Rights of the European Union (the Charter), while taking into account Article 52(1) enumerating conditions for the limitations of the rights enshrined in the Charter.

By its preliminary ruling, the ECJ declared the Data Retention Directive to be invalid, because the EU legislature had 'exceeded the limits imposed by compliance

* Professor of Constitutional Law, University of Helsinki, part-time Professor within the Surveille project, Law Department, European University Institute.

[1] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *OJ* [2006] L 105, p. 54.

European Constitutional Law Review, 10: 528–541, 2014

doi:10.1017/S1574019614001345

with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter'.[2] According to the Court, the Directive failed to lay down 'clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter', as well as entailed 'a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary'.[3] As the Court did not limit the temporal effects of its judgment, the finding of the invalidity takes effect from the date on which the directive entered into force, i.e. on 15 March 2006.

The judgment is by a Grand Chamber of the Court, an enlarged composition of fifteen judges reserved for high-profile cases. Therefore, the judgment will feature as a precedent which sets out the EU law approach with regard to the manner in which the collection and storage of meta-data produced in the course of electronic communications, a well as the issue of electronic mass surveillance in general, should be approached in light of the right to private life and the right to the protection of personal data.

Simultaneously, the judgment is undoubtedly one of the most significant judgments ever given by the Court of Justice on fundamental rights within the EU legal order in general, particularly insofar as judicial review of the compatibility of *EU legislation* with fundamental rights is concerned. Previously, the Court has been criticized for not reviewing EU measures as strictly as national laws[4] but as with judgments in such cases as *Association belge des Consommateurs Test-Achats*[5] and *Volker und Markus Schecke and Eifert*,[6] the judgment now indicates both the ability and willingness of the Court to embark on a very rigorous rights-based review of EU legislative measures in light of the EU Charter of Fundamental Rights. Moreover, the judgment features as a continuation of such constitutional dynamics that have significantly strengthened the status of fundamental rights within the EU legal order in recent years, as well as transformed the overall appearance of the Court from an economic court towards a supranational constitutional court that has actually become a judicial forerunner for the protection of fundamental rights in the area of counter-terrorism.[7]

[2] Joined Cases C-293/12, C-594/12 *Digital Rights Ireland and Seitlinger and Others*, at para. 69.

[3] Joined Cases C-293/12, C-594/12 *Digital Rights Ireland and Seitlinger and Others*, at para. 65.

[4] *See* e.g. J. Coppel and A. O'Neill, 'The European Court of Justice: Taking Rights Seriously?', 19 *C.M.L.Rev.* (1992) p. 669.

[5] C-236/09 *Association belge des Consommateurs Test-Achats and Others,* EU:C:2011:100.

[6] Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert,* EU:C:2010:662.

[7] Other judgments by the ECJ showing its commitment to the protection of fundamental rights in the area of counter-terrorism include, above all, Joined Cases C-402/05 P and C-415/05 P,

The structure of this comment is as follows. The next section places the judgment in a broader context, including describing the main content of the Data Retention Directive, after which it analyzes in depth the judgment by also delving into questions that lay behind certain sweeping observations by the Court. Next, it takes stock of the implications of the judgment for not only mass surveillance in the counter-terrorism context but also privacy and data protection as fundamental rights, as well as the role of legislatures and the courts in regulating the use of surveillance in an evolving technological environment.

Background

The Data Retention Directive is one of the major instruments of the EU counter-terrorism measures that were adopted in the aftermath of 9/11 and the Madrid train bombings in 2006.

The essential aim of the directive is to harmonize member states' legal provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that such data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each member state in its national law. According to the directive, the length of the retention should be between six months and two years starting from the date of the communication.

Article 5 of the Directive obliges the member states to ensure the retention of data which allow or may allow identification of a person, whether as source or destination of a communication, and of his position in space and time, whether by reference to his telephone number in respect of telephony or to his identification number or any another information specific to him such as an IP address in respect of Internet services. However, Article 5(2) of the Directive explicitly provides that no data revealing the *content* of the communication may be retained.

While the directive regulates the obligations of the service providers to retain communications data, it does not regulate the access to such data by the competent authorities of the member states for law enforcement purposes. Hence, the conditions for access to the data in order to counter terrorism and serious crime remains a matter of domestic law of each member state. In 2011, the Commission's Evaluation Report of the Data Protection Directive already displayed that the member states had used their discretion in varying ways, as the national authorities granted access to the data to be retained stretched from the police, security or intelligence

Kadi & Al Barakaat [2008] *ECR* I-6351 and Joined Cases C-584/10 P, C-593/10 P and C-595/10 P, *Council, Commission and United Kingdom* v. *Kadi*, judgment of 18 July 2013, n.y.r.

services and even the military to border and tax authorities.[8] Only eleven member states had required judicial authorisation for each request for access to retained data.[9]

From the very beginning, the Data Retention Directive has been one of the most controversial pieces of the EU's counter-terrorism legislation. Debates over its compatibility with fundamental rights and legality in general have raged since the earliest stages of its drafting to the April 2014 judgment by the Court of Justice at the level of both the EU legal order and the national legal orders of the member states. In 2006, Ireland brought a direct action before the Court seeking annulment of the directive by claiming that the directive was adopted on an incorrect legal basis. In 2009, the Court ruled that the retention of traffic and location data by the telecommunications service providers for law enforcement purposes under the Directive falls within the Community powers and, accordingly, could be adopted on the basis of Article 95 EC.[10] However, this judgment did not involve the examination of the compatibility of the directive with the fundamental rights guaranteed by the Charter.

Meanwhile, the domestic implementation of the directive into the national law raised a number of constitutional challenges in such member states as the Czech Republic, Germany and Romania. The German Constitutional Court, for instance, declared in 2010 the domestic implementing enactment of the directive unconstitutional, noting that the domestic enactment created 'a feeling of surveillance' and failed to put sufficient limits on the use that could be made of stored data.[11] Similarly, its counterparts in the Czech Republic[12] and Romania[13] ruled that the domestic implementing enactments of the directive were unconstitutional.

Finally, the Commission brought actions against some member states before the ECJ for their failure to transpose the directive into national law within the prescribed period. In 2009, for instance, the Commission brought an initial action against Sweden before the Court which held, in 2010, that Sweden had exceeded

[8] Ten member states had defined in their national legislation 'serious crime', with reference to a minimum prison sentence, to the possibility of a custodial sentence being imposed, or to a list of criminal offences defined elsewhere in national legislation. Eight member states require data to be retained 'not only for investigation, detection and prosecution in relation to serious crime, but also in relation to all criminal offences and for crime prevention, or on general grounds of national or state and/or public security'. Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC) COM(2011)225 final, 18 April 2011.

[9] Evaluation Report on the Data Retention Directive, p. 9.

[10] Case C-301/06 *Ireland* v. *European Parliament and Council*, judgment of the Grand Chamber of 10 Feb. 2009.

[11] German Const. Ct. [BVerfG], judgment of 3 March 2010, 1 BvR 256/08.

[12] Czech Const. Ct., judgment of 22 March 2011, Pl. ÚS 24/10.

[13] Romanian Const. Ct., Decision No. 1258 of 8 Oct. 2009.

the time-limit for adopting domestic legislation necessary to comply with the directive and, accordingly, had failed to fulfil its obligations under the directive. As Sweden did not comply with the judgment of 2010, the Commission brought a further action against Sweden before the Court of Justice in 2011. On 30 May 2013, the Court held that Sweden had not adopted all the necessary measures to ensure compliance with its initial judgment of 2010. As Sweden had failed to fulfil its obligations under EU law, the Court ordered Sweden to make a lump sum payment of EUR 3,000,000.[14] Meanwhile, the Commission had also initiated infringement proceedings against Germany in 2012, requesting the Court to impose financial penalties as Germany had still not complied with the Directive.[15] The case was removed from the register of the Court in June 2014 due to the judgment by the Court in the current case.[16]

Analysis of the judgment

General observations

The judgment is a neat example of the rights-based judicial review of legislation for its compatibility with fundamental rights, including the application of the permissible limitations test under Article 52(1) of the Charter. After depicting the legal context of the case and the questions referred by the national courts for a preliminary ruling, the reasoning of the Court progresses systematically through the following three major phases towards an overall conclusion:

(i) What fundamental rights are affected?
(ii) Whether the directive constitutes an interference with the applicable fundamental rights?
(iii) Whether such interferences are justified under Article 52(1) of the Charter?

According to Article 52(1),

> (a)ny limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

[14] Case C-270/11 *Commission* v. *Sweden*, judgment of 30 May 2013, n.y.r.
[15] Case C-329/12 *European Commission* v. *Federal Republic of Germany*.
[16] Order, 5 June 2014, *Commission* v. *Germany*.

https://doi.org/10.1017/S1574019614001345 Published online by Cambridge University Press

On a closer analysis, this provision can be seen as including the following distinct, yet inter-related conditions for the determination whether an interference with fundamental rights is justified:

(i) Limitations must be provided by the law, in legislation which must be accessible to the individual concerned and protect that individual from arbitrariness through, inter alia, precision and foreseeability.[17]
(ii) The essence of a fundamental right is not subject to limitations.
(iii) Limitations must have a legitimate aim in that it corresponds with the objectives of general interest recognized by the EU or the need to protect the rights and freedoms of others.
(iv) Limitations ought to be necessary for genuinely reaching the legitimate aim.
(v) Limitations must conform to the principle of proportionality.

Each condition listed above has an autonomous function to fulfill. As these conditions are also *cumulative*, one failure suffices to result in a negative conclusion that an interference amounts to a violation of the Charter. Given all these characteristics, the permissible limitations test under Article 52(1) is also one of those concrete arrangements that generates both substantive as well as doctrinal coherence between the Charter and the ECHR an other human rights treaties, notably the International Covenant on Civil and Political Rights (the ICCPR),[18] as well as the domestic systems for the protection of fundamental rights.[19]

The fundamental rights affected by the Data Retention Directive

The Court of Justice could easily conclude that the obligation on providers of publicly available electronic communications services or of public communications networks to retain the data listed in Article 5 of the directive for the purpose of making them accessible, if necessary, to the competent national authorities raised

[17] According to the European Court of Human Rights, this condition 'not only requires that the impugned measure should have some basis in domestic law, but also refers to the quality of the law in question, requiring that it should be accessible to the person concerned and foreseeable as to its effects'. *Rotaru* v. *Romania* judgment of 4 May 2000 (Appl. No. 28341/95), § 52. For the requirements of foreseeability and precision, *see* e.g. *Malone* v. *the United Kingdom*, judgment of 2 Aug. 1984, Series A No. 82, p. 32, § 67 and *Rotaru* v. *Romania*, judgment of 4 May 2000 (Appl. No. 28341/95), § 57.

[18] For the permissible limitations test under the ICCPR, *see The right to privacy. Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, Martin Scheinin (A/HRC/13/37, Dec. 2009), para. 17.

[19] For instance, the permissible limitations test under Finnish constitutional law includes seven distinct, yet inter-related and cumulative conditions that largely, if not exlusively, are parallel with Art. 52.1 of the Charter.

'questions relating to respect for private life and communications under Article 7 of the Charter, the protection of personal data under Article 8 of the Charter and respect for freedom of expression under Article 11 of the Charter'.

However, the Court only focused on the right to privacy and the protection of personal data because the directive 'directly and specifically affects private life' and because the retention of data 'constitutes the processing of personal data' and, therefore, 'necessarily has to satisfy the data protection requirements arising from that article'.[20]

Data Retention Directive as an interference with fundamental rights

To establish the existence of an interference with privacy and data protection, it largely, if not exclusively, sufficed for the Court to note that the retention of data for the purpose of possible access to them by the competent national authorities 'derogates from the system of protection of the right to privacy established by Directives 95/46 and 2002/58 with regard to the processing of personal data in the electronic communications sector'.[21] Moreover, the Court observed with reference to its previous judgment in the cases of *Österreichischer Rundfunk and Others*[22] that an interference with privacy is constituted irrespective of 'whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way'.[23]

However, these judicial observations remain quite sweeping as regards the important distinction between sensitive data and other data. After all, sensitive data can be seen as constituting such a 'core area' of both privacy and data protection where no restrictions should be allowed. Similarly, fundamental rules pertaining to the protection of personal data offer a higher level of protection to the processing of 'sensitive data'. This is indicated by e.g. Article 8(1) of the Directive 95/46,[24] prohibiting the processing of sensitive data, such as those revealing 'racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and […] concerning health or sex life'. Similarly, Article 6 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, explicitly prescribes that personal data 'revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning

[20] Joined Cases C-293/12, C-594/12 *Digital Rights Ireland and Seitlinger and Others*, at paras. 28 and 29.

[21] Joined Cases C-293/12, C-594/12 *Digital Rights Ireland and Seitlinger and Others*, at para. 32.

[22] Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* EU:C:2003: 294, para. 75.

[23] Joined Cases C-293/12, C-594/12 *Digital Rights Ireland and Seitlinger and Others,* at para. 33.

[24] Directive 95/46/EC, *OJ* [1995] L 281/31 [hereinafter: Data Protection Directive].

health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards'.

Furthermore, the Court can even be criticized for not saying clearly enough that such metadata as location data and traffic data may easily reveal much sensitive information about the individual, particularly when combined with information obtained from other sources. In addition, the Court could have observed that such metadata can reveal such categories of sensitive data as sensitive personal information (e.g. health, religion and sexuality) or certain highly sensitive relationships (e.g. lawyer-client, priest-parishioner and husband-wife).[25]

As the Data Retention Directive explicitly provides for 'the processing of personal data',[26] the Court could easily affirm that there was an interference with the protection of personal data. After all, all forms of processing of personal data automatically and invariably amount to an interference of that right.

However, the Court could have delineated in more detail the exact instances of the processing of personal data by the Data Retention Directive within the legislative framework of which it forms part. From the perspective of fundamental rights, it is important to distinguish carefully between the following three layers of an interference with the protection of personal data with different fundamental rights requirements. The first layer is constituted by the initial collection and generation of data by providers of publicly available electronic communications services or of public communications networks. The second layer emerges out of the maze of the obligation on providers of publicly available electronic communications services or of public communications networks to retain the data. The third and final layer of the processing of personal data relates to the further processing of data by law enforcement authorities for countering terrorism and serious crime.

Two points now deserve special emphasis. On the one hand, it should be clear that wholly uniform rules and principles cannot guarantee the appropriate observance of fundamental rights insofar as all these three layers of processing of personal data are concerned. In particular, the rules and safeguards applicable to the initial generation and other forms of the processing of data by providers of publicly available electronic communications services or of public communications networks purposes cannot evidently be applied as such to the further processing of this data for law enforcement purposes, simply because of the special characteristics of law enforcement. As already noted, the Data Retention Directive merely aims at harmonizing national rules which impose obligations on providers of publicly available electronic communications services or of public communica-

[25] *See also* Statement by Martin Scheinin, LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, Hearing, European Parliament, 14 Oct. 2013, at p. 4.

[26] Joined Cases C-293/12, C-594/12 *Digital Rights Ireland and Seitlinger and Others*, at para. 36.

tions networks to retain the traffic and location data 'for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law',[27] whereas the access to such data by the competent authorities of the member states for law enforcement purposes is supposed to be regulated in accordance with national law.

On the other hand, since the initial processing of data by providers of publicly available electronic communications services or of public communications networks has primarily taken place for commercial and consumer protection purposes, any further processing of the same data for law enforcement purposes actually constitutes a significant exception to the fundamental data protection principle of purpose specification.

As a final dimension of the interference analysis, the Court emphatically underscored that the interference with the rights to privacy and the protection of personal data should be regarded as being 'wide-ranging' and 'particularly serious'. Echoing the concern originally formulated by the German Constitutional Court, the Court emphasized that the fact that 'data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance'.[28] In this regard, the reasoning of the Court can be understood as advancing the view that such a serious interference with privacy and data protection as that by mass surveillance also has an adverse effect on the overall relationship between the individual and the state.

Justification of the interference with the applicable fundamental rights

The bulk of the judgment deals with the justification of the interference by data retention with the rights guaranteed by Articles 7 and 8 of the Charter, i.e. whether the directive complies with the permissible limitations test under Article 52(1) of the Charter.

In practice, the Court's assessment predominantly revolves around the proportionality of the interference whereas other conditions attracted less judicial attention. In particular, the judgment does not separately address the requirement that any limitations must be provided by law although some passages of the Court's reasoning can be understood as paraphrasing some dimensions of this requirement. The absence of the explicit application of the 'quality of the law' requirement is all the more striking as the Advocate-General's Opinion in the case included a lengthy discussion of this requirement.[29]

[27] *See* Recital 21 in the preamble to Data Protection Directive and Art. 1(1) thereof.
[28] Joined Cases C-293/12, C-594/12 *Digital Rights Ireland and Seitlinger and Others*, at para. 37.
[29] Opinion of A-G Cruz Villalón, delivered on 12 Dec. 2013, at paras. 108-132.

The essence of a fundamental right cannot be subject to restrictions. The Court rejected the argument raised by the some of the parties that the Data Retention Directive entails the violation of the essence of the fundamental rights to privacy and data protection. Even if the retention of extensive metadata by the directive does constitute a particularly serious interference with those rights, the Court noted that the directive 'does not permit the acquisition of knowledge of the content of the electronic communications as such'.[30]

Thus, the Court's reasoning seems to suggest that the interference came close to the core area of privacy and data protection rights but did not cross that border, thereby alluding to a possible interpretation that the content of electronic communications would only entail intrusions into the core area of privacy and data protection where no restrictions should be allowed. In that regard, the Court's view can be regarded as quite conventional. After all, the distinction between the content of the electronic communications and such metadata as traffic data and location data is rapidly fading away in a modern network environment. A lot of information, including sensitive information, about an individual can easily be revealed by monitoring the use of communications services through traffic data collection, storage and processing. Hence, the processing of metadata cannot any longer be invariably seen as falling within such 'peripheral areas' of privacy and data protection where limitations would be permissible much more easily than in the context of the content of electronic communications. Indeed, the more systematic and wide the collection, retention and analysis of metadata becomes, the closer it can be seen as moving towards the core area of privacy and data protection with the outcome that at least the most massive, systematic forms of collection and analysis of metadata can be regarded as constituting an intrusion into the inviolable core of privacy and data protection.[31]

Legitimate aim. According to the Court, it was 'apparent' from its previous case law that the material objective of the directive, namely 'the fight against international terrorism in order to maintain international peace and security', as well as 'the fight against serious crime in order to ensure public security' constituted an objective of general interest within the meaning of Article 52(1) of the Charter. In addition, the Court noted that the Directive served to protect the rights and freedoms of others as 'Article 6 of the Charter lays down the right of any person not only to liberty, but also to security.'[32] However, this justification is not necessarily entirely unproblematic to the extent that it involves a kind of justificatory turn of rephrasing the collective security interests with their strong persuasive

[30] Joined Cases C-293/12, C-594/12 *Digital Rights Ireland and Seitlinger and Others*, at para. 39.
[31] *See* Scheinin, *supra* n. 25, at p. 4.
[32] Joined Cases C-293/12, C-594/12 *Digital Rights Ireland and Seitlinger and Others*, at para. 42.

appeal in terms of the pressing need to protect the individual right to security and the rights of the potential victims in general.

Proportionality of the interference. The Court began its proportionality assessment by recalling that the acts of the EU institutions 'be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives'.[33] The Court also emphasized that the judicial review of the EU legislature's discretion 'should be strict' because of 'the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by Directive 2006/24'.[34] In addition, the Court emphasized that even highly important objectives such as the fight against serious crime and terrorism cannot justify measures which lead to forms of interference that go beyond what is 'strictly necessary'.[35]

Next, the Court identified five distinct, yet interrelated defects of the Data Retention Directive that combined to justify the overall conclusion that 'the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter'. First, the Directive failed to set any limit on the personal scope of application as it 'affects, in a comprehensive manner, all persons using electronic communications services' and, accordingly, 'applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime'.[36] Second, the Directive remained too vague regarding how the legitimate objective of countering terrorism and serious crime could precisely be served by the directive. In particular, the Directive failed to restrict the scope of application of a retention in relation

> (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.[37]

Third, the Directive fell short of limiting appropriatetely the access of national authorities to the data retained by private companies. In particular, the directive did not make access dependent 'on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data

[33] Joined Cases C-293/12, C-594/12 *Digital Rights Ireland and Seitlinger and Others*, at para. 46.
[34] Joined Cases C-293/12, C-594/12 *Digital Rights Ireland and Seitlinger and Others*, at para. 48.
[35] Joined Cases C-293/12, C-594/12 *Digital Rights Ireland and Seitlinger and Others*, at para. 51.
[36] Joined Cases C-293/12, C-594/12 *Digital Rights Ireland and Seitlinger and Others*, at para. 58.
[37] Joined Cases C-293/12, C-594/12 *Digital Rights Ireland and Seitlinger and Others*, at para. 59.

and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities'.[38] Fourth, the Directive merely required the data to be retained for a period of at least six months, 'without any distinction being made between the categories of data set out in Article 5 of that directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned'.[39] Fifth and finally, the Directive did not provide for sufficient safeguards relating to the security and protection of data retained by private providers of electronic communications.

In light of all these flaws, the Court concluded that the Data Retention Directive failed to 'lay down clear and precise rules governing the extent of the interference' with the rights affected and, accordingly, 'entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary'.[40]

Conclusion: Consequences and implications of the judgment

The immediate impact and value of the judgment relate to the privacy and surveillance interface. The judgment certainly features as a landmark decision marking a constitutional moment in striking a balance between fundamental rights and security in the digital age. The judgment condemns excessive and sweeping data retention by private parties for law enforcement purposes by showing unequivocally that a disproportionate infringement of the right to respect for private life and the protection of personal data cannot be permitted, even for the sake of achieving highly important objectives. In doing so, the judgment also features as a strong vindication of privacy and data protection as genuine fundamental rights. The erosion of these rights in the fight against terrorism and in respect of increasing surveillance has been a matter of concern in recent years but the judgment now demonstrates that these rights must be taken seriously while countering terrorism and serious crime in general.[41] By emphasizing the importance of these fundamental rights in the context of mass surveillance and security concerns in general, the judgment will provide a strong impulse to reconsider critically legal

[38] Joined Cases C-293/12, C-594/12 *Digital Rights Ireland and Seitlinger and Others*, at para. 62.
[39] Joined Cases C-293/12, C-594/12 *Digital Rights Ireland and Seitlinger and Others*, at para. 64.
[40] Joined Cases C-293/12, C-594/12 *Digital Rights Ireland and Seitlinger and Others*, at para. 65.
[41] *See* e.g. Martin Scheinin, Report by the Special Rapporteur on the Promotion and Protection Human Rights and Fundamental Freedoms while Countering Terrorism, A/HRC/13/37, para. 17 (28 Dec. 2009).

regimes for data retention and forms of electronic mass surveillance more generally not only in the EU but also elsewhere in the world.[42]

At the same time, however, the judgment is probably a disappointment for those who have argued in recent years that there is a fundamental distinction between privacy rights and the right to data protection and, specifically, that Article 8 of the Charter enshrines the protection of personal data as an autonomous right.[43] The judgment reflects this distinction, but only to a limited degree, as the essence of the Court's reasoning starts from the premise that the protection of personal data is 'especially important for the right to respect for private life enshrined in Article 7 of the Charter'[44] However, the positive side of this stance is that it for its part reinforces the substantive coherence between the Charter and the ECHR, as well as other human rights treaties, notably the International Covenant on Civil and Political Rights (the ICCPR), as in these treaties the right to the protection of personal data is treated as one of the substantive attributes of the generic right to the protection of private life under Article 8 of the ECHR and the right to privacy under Article 17 of the ICCPR Article 17.[45]

Finally, it deserves emphasis that the judgment is not necessarily a total knockout by the Court to mandatory data retention. While the judgment displays that electronic mass surveillance based on vaguely defined provisions is not compatible with the right to respect for private life and the protection of personal data, the undertone of the judgment nonetheless seems to be that some form of mandatory data retention in order to combat serious crime and terrorism might indeed be compatible with fundamental rights. It falls beyond the scope of this comment to ponder in detail the question of how to regulate data retention in compliance with privacy and data protection. Thus, it suffices here to note that the judgment seems to delineate quite clearly such points that should be taken into account by

[42] The judgment also supports the essential findings of the multidimensional assessment by the SURVEILLE consortium to the extent that they result in wide rejection of current methods of electronic mass surveillance on legal and ethical grounds. *See* Tom Sorell et al., SURVEILLE Deliverable D2.8: Update of D2.7 on the basis of input of other partners. Assessment of surveillance technologies and techniques applied in a terrorism prevention scenario. Submitted to the European Commission on 29 May 2014 (awaiting publication).

[43] For the relationship between the two CFREU provisions, *see* e.g. Maria Tzanou, *The Added Value of Data Protection as a Fundamental Right in the EU Legal Order in the Context of Law Enforcement* (2012 PhD thesis at the European University Institute). *See also* Opinion of A-G Cruz Villalón, delivered on 12 Dec. 2013, at paras. 55-67, analyzing 'the combination of the right to privacy and the right to protection of personal data'.

[44] Joined Cases C-293/12, C-594/12 *Digital Rights Ireland and Seitlinger and Others,* at para. 53.

[45] For a comprehensive survey of the legal instruments, and mechanisms, for the protection of privacy in the multi-layered fundamental and human rights systems, *see* the report Martin Scheinin et al., prepared for the EU Fundamental Rights Agency, Data Protection in the European Union: the Role of National Data Protection Authorities (2010), available at: <http://fra.europa.eu/en/publication/2012/data-protection-european-union-role-national-data-protection-authorities>.

the EU legislature (or national legislatures acting within the scope of application of EU law) when curtailing legislative framework on data retention to what is 'strictly necessary'. These points can largely, if not exclusively, be inferred from those flaws of the Data Retention Directive that jointly triggered the invalidity of the Data Retention Directive. However, as it is beyond the powers of the Court to establish the legislative framework required, a positive obligation is now imposed on the EU legislature and, later, the authorities of the member states to organize such a legal regime for mandatory data retention that appropriately complies with the Charter, as now interpreted by the Court. Indeed, the judgment by the Court can actually be seen as an instance of such dialogue between the Court and the legislature(s) in which the Court does not only invalidate a legal measure but also indicates how the legislator(s) could enact a valid legislation accomplishing the major objective of the invalidated law. Easier said than done perhaps, but it is nonetheless important to emphasize the positive obligations of the legislature(s) to provide the appropriate legislative framework for data retention by taking careful notice of the ECJ's judgment. It should be added that this positive obligation is also imposed on national legislatures. After all, with a view of the overall EU data protection framework,[46] the member states can still be understood as acting within the scope of EU law and, accordingly, being obliged to apply the Charter, as now interpreted by the Court in this landmark judgment.

[46] This legislative framework is primarily made up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281, p. 31; and of 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, p. 37.