The Court of Justice of the European Union, Data Retention and the Rights to Data Protection and Privacy – Where Are We Now?

Felix Bieker

The Court of Justice of the European Union, Data Retention and the Rights to Data Protection and Privacy – Where are we now?

Felix Bieker

Walther Schücking Institute for International Law at the University of Kiel and ULD (Independent Centre for Privacy and Data Protection) Schleswig-Holstein, Kiel, Germany
fbieker@wsi.uni-kiel.de

Abstract. In a recent judgment the CJEU found the Data Retention Directive to be incompatible with the rights to privacy and data protection under the EU Charter of Fundamental Rights. However, the Court's interpretation of these fundamental rights needs further development, especially with regard to their respective scopes. While the Court declared the EU Directive to be invalid, there remain questions with regard to the Member States' national implementation measures, which remain in force. Nevertheless, they do no longer comply with EU law and therefore need to be repealed or altered substantively. While it should be for the national legislator to achieve this, it might be necessary for service providers and citizens to challenge these provisions before the competent national courts.

Keywords: Data Retention, Privacy, Data Protection, European Union, Fundamental Rights, Court of Justice, Data Retention Directive, Data Protection Directive, e-Privacy Directive.

1 Introduction

In Europe, the retention of traffic data for criminal investigations has been and continues to be a subject for much debate as well as litigation. With the long-awaited and substantive judgment of the Court of Justice of the European Union (in the following: CJEU or the Court) in the cases of *Digital Rights Ireland and Seitlinger*[1], this article argues that the blanket retention of traffic data for the fight against crime and terrorism has been ruled out. However, there remain questions to be answered, most prominently the scope of the right to data protection under Article 8 of the EU Charter on Fundamental Rights (in the following: CFR or the Charter) and the consequences of

[1] Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger*, Judgment of 8 April 2014, not yet reported.

the Data Retention Directive's (in the following: DRD or the Directive)[2] invalidity for Member States' law.

This article explains the genesis and scope of the Data Retention Directive (2), before briefly summarizing the Court's judgment (3). The Court's reasoning is then assessed with a focus on the interpretation of Article 8 CFR and the Court's role in the European system of fundamental rights protection (4). Section 5 analyzes the consequences of the DRD's invalidity for the Member States' own regulations on data retention. The conclusions (6) provide a brief outlook on future developments.

2 The Genesis and Scope of the Data Retention Directive

The regulation of data retention on a European level gained momentum after the terrorist attacks of Madrid and London in 2004 and 2005 respectively. In the aftermath of these tragic events, there was an endeavor to pass a Framework Decision in the then third pillar of the European Union, the Police and Judicial Cooperation in Criminal Matters.[3] The cooperation of police was governed by ex-Articles 30, 31 and 34 TEU. Under these provisions however, a unanimous vote in the Council was required. When, in the early stages of the negotiations, Ireland threatened to use its veto on the proposal, the legislation was in jeopardy.

Nevertheless, while some Member States did not have any form of data retention, there also were many variations of data retention in other Member States. This provided the impetus to further pursue the subject as a harmonization measure under ex-Article 95 TEC (now Article 114 TFEU). The subsequent Data Retention Directive, due to the change in legal basis, could then be adopted by a majority vote in the Council.

The DRD obliged Member States to order providers of publicly available electronic communication services or of public communications networks (in the following: service providers) to retain data to identify the source and destination of fixed network and mobile telephony – including text messages – as well as internet telephony, E-Mail communications and internet access according to its Article 5 para. 1. These data include numbers or user names, date, time and duration, and for mobile telephony the subscriber's IMSI (international mobile subscriber identity), the cell phone's IMEI (international mobile station equipment identity) and the location by Cell ID. These sets of data, at a first glance, might appear rather innocuous, as they do not contain any contents of the communication. In fact, the DRD expressly prohibits the storing of any data which may reveal the contents of a communication in its Article 5 para. 2. However, for two different projects a German and a Swiss politician made

[2] 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.

[3] Terhechte, Rechtsangleichung zwischen Gemeinschafts- und Unionsrecht – die Richtlinie über die Vorratsdatenspeicherung vor dem EuGH, Europäische Zeitschrift für Wirtschaftsrecht 2009, 199.

their data publicly available and had them visualized in an interactive map showing their location. This was correlated with a list of calls, text messages and internet communications to and from other (identifiable) persons.[4] From this combined information, it is possible to draw comprehensive conclusions about the everyday life of these politicians.

Soon after the Directive's adoption, Ireland filed an annulment action according to Article 263 TFEU before the CJEU, solely attacking the choice of legal basis, which was rejected by the Court in 2009.[5] Simultaneously, the Member States' implementation measures for the DRD were challenged before numerous national constitutional courts and declared invalid in Romania, Germany and the Czech Republic.[6] None of these courts made a preliminary reference to the CJEU under Article 267 TFEU, arguing that the national legislator had not exercised the margin granted by the Directive in a way compatible with the national constitution.[7] While a German Administrative Court in 2009 asked the Court about the Data Retention Directive's validity, the CJEU found the question inadmissible, as it did not bear any relation to the case referred.[8] In 2012 however, the Austrian Constitutional Court as well as the Irish High Court referred questions concerning the compatibility of the DRD with fundamental rights to the CJEU, which resulted in the present judgment.

3 The Court's Judgment

In its judgment, the Court stressed that the Directive's wide scope allowed detailed insights into the daily life of all citizens. Even though no contents of the communications were stored, the retention of the data might change the use of these services, which affected the users' and subscribers' right to freedom of expression under Article 11 CFR. The question whether the data of users and subscribers could be retained had to be assessed with regard the right to privacy according to Article 7 CFR. Fur-

[4] Biermann, Betrayed by our own data, Zeit Online of 26 March 2011, available at: http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz/komplettansicht; Digitale Gesellschaft, The life of National Councillor Balthasar Glättli under surveillance, available at: https://www.digitale-gesellschaft.ch/dr.html.

[5] Case C-301/06 *Ireland v Parliament and Council* [2009] ECR I-593.

[6] Constitutional Court of Romania, Decision no. 1258 of 9 October 2009, available at: http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf; Federal Constitutional Court of Germany, Judgment of 2 March 2010, 1 BvR 256/08, English press release available at: http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011en.html; Constitutional Court of the Czech Republic, Judgment of 22 March 2011, Pl. ÚS 24/10, available at: http://www.slidilove.cz/sites/default/files/dataretention_judgment_constitutionalcourt_czech republic.pdf.

[7] Cf. for example Federal Constitutional Court of Germany (note 6), paras. 183 and 185-187.

[8] Joined Cases C-92 and 93/09 *Schecke and Eifert* [2010] ECR I-11063, paras. 35 and 42.

ther, Article 8 of the Charter, the right to protection of personal data, imposed requirements on the protection of personal data.[9]

3.1 Interference with Fundamental Rights

However, when assessing the interference, the Court no longer referred to Article 11 of the Charter. Instead, it affirmed that for the right to privacy, there was no requirement of sensitivity of the data or any inconvenience for the users or subscribers. In accordance with its own and the jurisprudence of the European Court for Human Rights (in the following: ECtHR), it held that the obligation to retain the data as well as the granting of access for national authorities to this data constituted two independent interferences with Article 7 CFR. Additionally, the processing of personal data in itself interfered with Article 8 CFR. The Court emphasized that due to the mass scale of the data retention, this measure was likely to create a feeling of constant surveillance.[10]

3.2 Justification of the Interference

Under the horizontal justification clause of Article 52 para. 1 of the Charter, interferences with all rights granted may be justified when they are provided for by law, respect the essence of the rights and are proportionate. The Court started with an assessment whether the DRD respected the essence of the rights concerned. Before the Charter entered into force, the CJEU stated that interferences may not impair the very substance of fundamental rights, but has since adopted the Charter's wording.[11] In an earlier decision the Court defined the essence of a right as its 'core content'[12] and thus interpreted it as a principle separate from proportionality.[13] In the case at hand, the Court found that while the retention was a particularly serious interference, it respected the essence of Article 7 CFR as it did not include the retention of any contents of communication. With regard to Article 8 CFR the Court argued that the essence of this right was not concerned, as the Directive itself contained rules on the integrity and protection of the data retained.[14]

In the review of the Directive's proportionality the Court found the fight against terrorism and serious crime to be its 'material objective'[15]. Yet, due to the sensitivity of personal communications and the large scale of the retention, the Court held that this measure called for strict judicial review.

---

[9] Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger* (note 1), paras. 28-30.

[10] *Ibid*., paras. 34-37.

[11] Cf. Case C-5/88 *Wachauf* [1989] 2609, para. 18.

[12] Case C-283/11 *Sky Österreich*, Judgment of 22 January 2013, not yet published, para. 49.

[13] This line of assessment was also conducted in a judgment after *Seitlinger* in Case C-129/14 PPU *Spasic*, Judgment of 27 May 2014, not yet published, para. 58.

[14] Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger* (note 1), para. 40.

[15] *Ibid*., para. 41.

Assessing the appropriateness, the CJEU argued that the retained data was a valuable tool for criminal investigation, which was unchanged by the fact, that the measures could be circumvented by taking recourse to anonymous forms of communication. However, the fight against serious crime, did not in itself justify the retention of all communication data with regard to necessity. Rather, the restriction had to be limited in so far as it was strictly necessary, due to the right to data protection's particular importance for the right to private life. As the DRD encompassed traffic data from all means of electronic communication and all subscribers and users, it affected, without any exception, all European citizens using electronic communication. This called for legislation with a precisely defined scope as well as safeguards against abuse and unlawful processing of the data.[16] In particular, the CJEU criticized four aspects:

Firstly, the collection of data neither required a nexus with a threat to public security, nor did it demand any temporal, geographical or personal limitations. Secondly, access to and use of the data retained was not limited: the definition of serious crime as well as the substantive and procedural conditions were left to the Member States. Further, the Directive required no limitation on the persons who were granted access and there was no prior review by a court or other independent body. Thirdly, the range of data retention from a period of six to 24 months was not justified by any reasons and thus arbitrary. These three points constituted grave interferences with Articles 7 and 8 of the Charter.[17]

Lastly, the Court criticized the lack of safeguards against abuse and rules for protection of the data retained. The organizational measures to protect the data against loss and misuse were to be weighed against economical interests of the service providers and there was no obligation to store the data within the territory of the EU and thus no supervision by an independent body. This did not conform to the requirements of Article 8 CFR.[18] Therefore, the CJEU found that the data retention was disproportionate and the interference not justified. Consequently, the Court ruled that the DRD was invalid.

4 Assessment of the Judgment

Keeping in mind the controversy surrounding data retention for years now, which included the CJEU in two instances, it seems as though the Court needed a push to finally assess the validity of the DRD. However, with a view to previous judgments concerning EU legislation and the strict proportionality review conducted by the Court,[19] the judgment does not come as a surprise.

The CJEU assesses the rights of the Charter extensively and for the first time scrutinizes Article 8 CFR as a right independent from Article 7 of the Charter. In previous

[16] *Ibid*., paras. 49-58.
[17] *Ibid*., paras. 59-65.
[18] *Ibid*., paras. 66-68.
[19] Case C-291/12 *Schwarz v Stadt Bochum*, Judgment of 17 October 2013, not yet published; Joined Cases C-92 and 93/09 *Schecke and Eifert* (note 8).

cases, the Court assessed the rights jointly, under the premise that Article 8 para. 1 and Article 7 CFR were closely connected and their scope of protection was a right to respect for private life with regard to the processing of personal data.[20] When stating in *Digital Rights Ireland and Seilinger*, that the question of the retention of the data affects the scope of Article 7 CFR, while Article 8 of the Charter sets out data protection requirements,[21] the Court allows for a nuanced shift in the assessment of the scopes of these rights.

As far as the interference is concerned though, the Court relies on its own jurisprudence to hold the storing of the data to interfere with Article 7 CFR and refers to the ECtHR's case law when finding the access to this data as a separate interference with this very provision.[22] While it is to be welcomed that the Court refers to the jurisprudence of the ECtHR, which has developed extensive and long-standing case-law on the right to privacy under the European Convention on Human Rights (in the following: ECHR), the CJEU's adoption of this strand of case law leads to problems with regard to Article 8 CFR. This is due to the fact that the ECHR contains no separate right to data protection. Interpreting the obligation of service providers to store the data and the subsequent access of national authorities to this data as interferences with Article 7 CFR is in line with the ECtHR's jurisprudence on interferences with Article 8 ECHR.[23] As Article 7 CFR guarantees a right corresponding to Article 8 ECHR in the sense of Article 52 para. 3 CFR according to the Explanations to the Charter[24] such an interpretation is sensible. Even though the Explanations are not a legally binding document, they are awarded interpretative force for the Charter by Article 52 para. 7 CFR and Article 6 para. 1 TEU.

When, however, the Court goes on to consider the processing of the data as interference with Article 8 CFR, this leads to overlaps between the scopes of these rights. In order to interpret the notion of processing as laid down by Article 8 para. 2 CFR, recourse can be taken to the Explanations to the Charter. For Article 8 CFR, they refer to the Data Protection Directive (in the following: DPD)[25] for conditions and limitations of the right to data protection. According to the definition of Article 2 lit. b Data

---

[20] Joined Cases C-92 and 93/09 *Schecke and Eifert* (note 8), paras. 47 and 52; Case C-468/10 *ASNEF* [2011] I-12181, paras. 41 *et seq*; Case C-291/12 *Schwarz v Stadt Bochum* (note 19), paras. 24 *et seq*; However, in one case between private parties, where according to Article 51 para. 1 CFR the Charter does not apply, the Court mentioned – without any assessment of its scope or an interference – the right to data protection safeguarded by Article 8 CFR without reference to Article 7 of the Charter, cf. Case C-70/10 *Scarlet Extended* [2011] I-11959, para. 50.

[21] Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger* (note 1), paras. 29 *et seq*.

[22] *Ibid*., paras. 33-35.

[23] *Leander v. Sweden*, Judgment of 26 March 1987, no. 9248/81, para. 48; *Rotaru v. Romania*, Judgment of 4 May 2000, no. 28341/95, para. 46.

[24] Explanations Relating to the Charter of Fundamental Rights, OJ 2007 C 303/17.

[25] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31.

Protection Directive, the processing of personal data consists inter alia of their collection, storage and use. Thus, when analyzing the judgment with due regard to the secondary law, the term 'processing' which is used to describe an interference with Article 8 of the Charter has to be interpreted as the collection, storage and subsequent use of the personal data. Then however, the interference with Article 8 CFR is exactly the same as the interferences by retention of the communication data with Article 7 CFR, i.e. the obligation of service providers to store the data and the subsequent access to the data by national authorities.

Although the Court apparently tried to differentiate between the right to privacy and the right to data protection in this case, it ended up with identical definitions for both rights. Consequently, whenever data is stored or accessed, this constitutes simultaneous interferences with the right to privacy and the right to data protection. If this had been an intended outcome, the Court would not have bothered to differentiate between the rights. Therefore, the CJEU's interpretation of the scope of the rights of Article 7 and 8 CFR is not yet convincing and requires further elaboration by the Court.

However, if the current approach of the CJEU is followed and the rights to privacy and data protection are interpreted in the same manner, Article 8 CFR could be regarded as a lex specialis to the more general provision of Article 7 CFR.[26] As the ECHR does not include a separate right to data protection, the ECtHR employed the right to private life in order to develop the right to privacy as one of its facets. With time, the case law evolved and the ECtHR also covered aspects of data protection, as detailed above. While the CJEU could just adopt this case law for its own jurisprudence before the Charter, there is now an express right to data protection, which has to be taken into account. In this regard, the specific right to data protection of Article 8 CFR could be awarded precedent over the more general right to private life in Article 7 of the Charter, which – in its verbatim – does not contain any reference to either privacy or data protection. This lex specialis interpretation would ensure consistency with the ECHR, while allowing a broader scope for Article 8 of the Charter with regard to the extensive individual rights granted by the DPD. Nevertheless, the existence or non-existence of a distinction between privacy and data protection is a contentious issue in doctrine.[27] The ultimate resolution of this problem is not within the scope of this article, which is instead focused on the discussion of the CJEU's judgment in the *Digital Rights Ireland and Seitlinger* case.

Yet, the judgment at hand does include a new aspect concerning the right to data protection: that is the Court's interpretation of Article 8 para. 3 CFR – which states that an independent authority supervises adherence to the provision – as requiring

---

[26] Kingreen, Article 8, in: Calliess/Ruffert, EUV/AEUV, 4th ed., Munich 2011, MN. 1.

[27] Cf. inter alia Tzanou, Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right, International Data Privacy Law 3 (2013), 88; Kranenborg, in: Peers et al. (eds.), The EU Charter of Fundamental Rights – A commentary, Oxford/Portland 2013, MN. 08.21-08.27; Kokott/Sobotta, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law 3 (2013), 222; and even AG Villalón, Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger*, Opinion of 12 December 2013, paras. 62-67.

storage of the data within the European Union. This is a very welcome statement. The CJEU thereby demonstrates that it takes the revelations about mass-surveillance by US and UK intelligence services seriously and is not willing to let European law turn a blind eye to these substantial threats to privacy and data protection. In the way the Court assesses this provision as a part of the right to data protection, it adds an element of an individual right to Paragraph 3 of Article 8 CFR, which could have been seen as a merely formal requirement.

Although the interpretation of the rights to privacy and data protection may not be followed in its reasoning, the Court is to be commended for its extensive assessment of the privacy implications of data retention. However, the issue that it took eight years to arrive at the conclusion that the DRD gravely violated fundamental rights remains. Yet, it should be borne in mind that it is a legal obligation of the legislator to draft regulations in a way consistent with fundamental rights. The DRD in its Article 14 para. 1 contained a clause requiring an evaluation of its impact and effectiveness. In the subsequent report the Commission, evaluating its own work, suggested several changes, inter alia to the storage of the data and the reimbursement of service providers, but found the Directive in general to conform to fundamental rights.[28] However, with regard to the measure's fundamental rights implications the report merely summarized the case law of the CJEU and the ECtHR without applying it to the Directive itself.[29] In this regard, improvement is necessary: the Commission needs to take the assessment of fundamental rights implications of regulations more seriously. A two page description of the fundamental rights concerned cannot be sufficient for measures interfering with the rights of the entire European population.

In safeguarding fundamental rights the CJEU comes into play only on a secondary level, when it interprets Union law and rules on the validity of the acts adopted by the legislator according to Article 19 para. 3 TEU. As any other court, the CJEU cannot render decisions by its own motion, but is limited to the cases brought before it. In the aftermath of its first decision on the proceedings instigated by Ireland, the CJEU attracted wide-spread criticism.[30] However, it could have been anticipated that the Court would only assess the choice of Article 114 TFEU (ex-Article 95 TEC) as legal basis as this was the only claim made by Ireland.[31] As the infringement proceedings under Article 263 TFEU are based on the French legal system, there is a long-

[28] European Commission, Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC) of 18 April 2011, COM(2011) 225 final.

[29] *Ibid*., 28 *et seq*.

[30] Cf. inter alia, Simitis, Der EuGH und die Vorratsdatenspeicherung oder die verfehlte Kehrtwende bei der Kompetenzregelung, Neue Juristische Wochenschrift 2009, 1782; Petri, Rechtsgrundlage der EG-Richtlinie zur Vorratsdatenspeicherung, Europäische Zeitschrift für Wirtschaftsrecht 2009, 212, 214 *et seq*; Braum, „Parallelwertung in der Laiensphäre": Der EuGH und die Vorratsdatenspeicherung, Zeitschrift für Rechtspolitik 2009, 174; Terhechte (note 3).

[31] Case C-301/06 *Ireland v Parliament and Council* (note 5), para. 24.

standing practice of the Court to limit its review to the claims of the applicants, rather than conduct an extensive ex-officio scrutiny.[32]

The issue of fundamental rights was, however, raised by the Slovak Republic, which supported Ireland's action before the CJEU and questioned the retention's compatibility with Article 8 ECHR.[33] Under Article 130 of the Rules of Procedure of the Court, Member States may be granted leave to join proceedings, but this is limited to supporting the claims of the party according to Article 129 para. 1 cl. 2 of the Rules of Procedure. Even though the CJEU's case law on claims and defences is not always consistent,[34] the Court does not allow interveners the right to seek forms of order unconnected to those of the party.[35]

While the Court's judicial self-restraint in this context as a whole has been[36] and continues to be subject to criticism, especially when it comes to the compatibility of a measure with fundamental rights,[37] the CJEU's limited review cannot be ascribed to an attempt to circumvent an assessment of fundamental rights. Rather, the suggestion that Ireland's annulment action was motivated by the aspect concerning EU competence and the circumvention of a unanimous vote in the third pillar can be considered an explanation for the absence of any claim concerning the compatibility of the DRD with fundamental rights.[38] After this judgment, as noted above, there were several instances where national courts were concerned with the compatibility of the DRD with fundamental rights. Yet, until the reference by the Austrian Constitutional Court and the Irish High Court none of the courts submitted a reference to the CJEU. This is a further point for improvement: in a multi-level system for the protection of fundamental rights, such as the EU, all depends on the cooperation of the various actors.[39]

5 Consequences of the Judgment

As an immediate consequence of the judgment, the infringement proceedings instigated by the Commission against Germany under Article 258 TFEU for failure to implement the Data Retention Directive were dropped, as this obligation no longer exists.[40] Additionally, the Commission will reimburse Sweden, which had already been ordered to pay the costs for the infringement proceedings instigated against it.[41]

---

[32] Case C-367/95 P *Commission v Sytraval and Brink's France* [1998] ECR I-1719, para. 67.
[33] Case C-301/06 *Ireland v Parliament and Council* (note 5), para. 34.
[34] Cf. Pechstein, EU-Prozessrecht, 4th ed., Tübingen 2011, MN. 212.
[35] Case C-155/91 *Commission v Council* [1993] I-939, paras. 23 *et seq*.
[36] Everting, Überlegungen zum Verfahren vor den Gerichten der Europäischen Gemeinschaft, in: Colneric et. al, Une communauté de droit, Berlin 2003, 537.
[37] Giegerich, Spät kommt Ihr, doch Ihr kommt: Warum wird die Grundrechtskonformität der Vorratsdatenspeicherung erst nach acht Jahren geklärt?, Zeitschrift für Europarechtliche Studien 2014, 3, 9 *et seq*.
[38] Terhechte (note 3), 201.
[39] Cf. Giegerich (note 37), 14-17.
[40] Case C-329/12 *Commission v Germany*, case closed.
[41] Case C-185/09 *Commission v Sweden*, [2010] ECR-14.

More importantly however, should the EU legislator opt for a new approach to data retention, it will not be able to employ Article 114 TFEU as a legal basis. As the Court has required it to lay down the details of storage and access to the data, a definition for serious crime as well as procedural safeguards, this is evidently not a measure to harmonize national legislation for the benefit of the internal market. Rather, the measure will have to be based on the police cooperation rules, which with the entry into force of the Lisbon Treaty have been integrated into the former first pillar. Most likely, data retention could be based on Article 87 TFEU, which allows joint measures for police cooperation.[42]

Aside from this question of competence, it needs to be assessed, whether Member States, which do not have rules on data retention such as Germany, are now free to pass national legislation. Further, as the CJEU's jurisdiction only covers EU law the national rules implementing the DRD remain in force in many Member States. For these Member States, it is important to know whether they can uphold their national laws. With the DRD declared invalid, the national transposition measures can no longer transpose European law. As the competence of the EU in the Area of Freedom, Justice and Security is a shared competence according to Article 4 para. 2 lit. j TFEU and there no longer is EU legislation with regard to data retention, the Member States are in principle free to exercise their own competences and legislate on the matter. However, as the Court pointed out, the DRD was a derogation from the general EU data protection regime, i.e. the DPD and the e-Privacy Directive (in the following: ePD)[43], which according to its Article 1 para. 2 complements the DPD for the electronic communications sector.[44] The Court further held that data retention concerns the detection and prosecution of serious crime. For measures concerning cooperation in the area of police and judicial cooperation in criminal matters, there is an exemption clause in Article 1 para. 3 ePD. An almost identically phrased clause is contained in Article 3 para. 2 DPD. In a previous judgment, the CJEU interpreted the latter provision to apply to the transfer of data collected by private operators to a third country.[45] The transfer fell within a framework established by public authorities that related to public security. Applied to the case of data retention this implies that the access of public authorities serves the aim of fighting serious crime and improving public safety. Thus, the exemption clauses apply. However, the 'mere' collection, which served the harmonization of the internal market, is not covered by Article 1 para. 3 ePD and Article 3 para. 2 DPD. While this differentiation might seem artificial, it is

[42] Cf. in greater detail Wendel, Wider die Mär von Grundrechtsblinden: Der EuGH und die Vorratsdatenspeicherung, Verfassungsblog, available at: http://www.verfassungsblog.de/wider-maer-vom-grundrechtsblinden-eugh-und-vorratsdatenspeicherung/.

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

[44] Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger* (note 1), para. 32.

[45] Joined Cases C-317/04 and 318/04 *Parliament v Council and Commission* [2006] ECR I-4721, paras. 56-59.

the only interpretation consistent with Article 15 para. 1 cl. 2 ePD, which exceptionally allows Member States to impose an obligation on service providers to retain communication data for a limited period. If the storage of data by service providers was covered by the exemption clauses, there would be no scope of application for Article 15 para. 1 cl. 2 eDP.[46] Furthermore, the Court already stated in its judgment on the action brought by Ireland that national measures on data retention before the DRD fell under Article 15 para. 1 ePD.[47] Therefore, the storage of communication data falls under the scope of the ePD and the Member States may derogate from the confidentiality of communications guaranteed by Article 5 ePD and the obligation to have traffic data deleted or anonymized by the service providers once they are no longer required under Article 6 ePD. However, the derogation clause of Article 15 para. 1 ePD allows such exceptions only where these restrictions serve public security, the prevention, investigation, detection and prosecution of criminal offences. While this is certainly the case for any national legislation on data retention, the provision further calls for the restriction to be limited to necessary, appropriate and proportionate measures needed in a democratic society. Further, the third clause of Article 15 para. 1 ePD calls for the measures to be in concordance with the general principles of EU law, including those of Article 6 para. 1 TEU. This refers to the fundamental rights of EU law, which are enshrined in the Charter, which has gained binding legal force with the coming into force of the Lisbon Treaty according to Article 6 para. 1 cl. 2 TEU.

With the present judgment of the Court, it has been ruled that the DRD did not conform to the fundamental rights of EU law. From this judgment, it follows immediately, that national measures, which – as it has been demonstrated still fall under the ePD and therefore come within the scope of EU law – have been adopted in order to implement the DRD, do not meet the standards of the ePD and therefore violate Union law. Even where the national legislator has restricted access to and use of the data, the retention period will still be set arbitrarily and there will be no restriction as to the personal scope of the retention. If that would be the case, the national measure would have violated the very provisions it was supposed to implement. Therefore, Member States with rules on data retention are under a legal obligation to repeal them.

In case Member States do not repeal the national laws themselves, affected service providers and citizens can challenge these provisions before national courts claiming a violation of EU law in order to have these provisions set aside in accordance with the primacy of EU law.[48] With the judgment at hand, there should not be any issues as to the interpretation of the DPD's and eDP's provisions. However, if a national court

---

[46] Cf. Wagner, Die Vorratsdatenspeicherung in der Grundrechtsunion, Ju-Wiss Blog, available at: https://www.juwiss.de/54-2014/; Lehofer, Nochmals zum VDS-Urteil: auch "autonome" nationale VDS (auf Basis des Art 15 Abs 1 RL 2002/58) muss den Anforderungen des Urteils genügen, available at: http://blog.lehofer.at/2014/04/noch-zwei-kurze-anmerkungen-zum.html; dissenting Wendel (note 42).

[47] Case C-301/06 *Ireland v Parliament and Council* (note 5), para. 67.

[48] Cf. Genna, Messy Consequences for National Legislation following Annulment of EU Data Retention Directive, LSE Media Policy Project, available at: http://blogs.lse.ac.uk/mediapolicyproject/2014/04/08/messy-consequences-for-national-legislations-following-annulment-of-eu-data-retention-directive/.

had any doubts or wished to derogate from the CJEU's judgment, at least a court of last resort would be under an obligation to submit a reference for a preliminary ruling under Article 267 para. 3 TFEU. When a national court refuses to make a reference or deliberately deviates from the case law of the CJEU it violates EU law. Thus, the Commission may instigate proceedings under Article 258 TFEU against the Member State. Additionally, the refusal to refer to the CJEU may be a violation of national constitutional law. If in Germany, for instance, a court arbitrarily fails to refer a case to the CJEU, it violates the individual's right to the jurisdiction of his or her lawful judge under Article 101 para. 1 cl. 2 of the Basic Law.[49] Such an interpretation of the national law conforms to the Member States' obligation to provide effective remedies in areas concerning Union law under Art. 19 para. 1 cl. 2 TEU.

However, even where Member States repeal their implementing measures, critical review of new data retention legislation is needed. The United Kingdom, in the wake of the CJEU's judgment, has already passed new legislation to continue the retention of users' and subscribers' data with the Data Retention and Investigatory Powers Act 2014 (in the following: DRIP).[50] Under Section 1 paras. 1 and 2 DRIP, retention may be ordered by the Secretary of State relating to one or multiple service providers. According to Section 1 para. 5 DRIP the maximum period of retention must not exceed twelve months. With regard to details of the retention the Secretary of State is authorized by Section 1 paras. 3 and 4 DRIP to further specify these by means of regulations. Despite its recent enactment, this legislation has already been subject to severe criticism by Members of the UK Parliament, who announced that they would challenge the act before national courts[51] as well as several legal scholars, who argued in an open letter to the Home Office that the law was incompatible with the CJEU's criteria for data retention.[52] Indeed, while it does not require default storage of all communications data, the DRIP allows storage of the entire data of one or more service providers, which still entails a very wide range of persons affected without any suspicion or link to criminal activities. Nevertheless, the scope of the retention depends on the subsequent regulations, which shape the requirements for the retention notice and its contents under Section 1 paras. 3 and 4 DRIP. Until these rules are set up, a final assessment of the measure's compatibility is hardly possible, although the wide scope of the DRIP does not seem to be reconcilable with the CJEU's requirements.

---

[49] Federal Constitutional Court of Germany, Reports of Decisions (BVerfGE) 75, 223.

[50] Data Retention and Investigatory Powers Act 2014 of 17th July 2014, available at: http://www.legislation.gov.uk/ukpga/2014/27/pdfs/ukpga_20140027_en.pdf, the Act also broadens investigatory powers of UK agencies and contains a clause on extra-territoriality, which are, however, outside the scope of this article.

[51] Travis, Drip surveillance law faces legal challenge by MPs, The Guardian of 22 July 2014, available at: http://www.theguardian.com/world/2014/jul/22/drip-surveillance-law-legal-challenge-civil-liberties-campaigners.

[52] Basu et al., An open letter from UK internet law academic of 15th July 2014, available at: http://www.law.ed.ac.uk/__data/assets/pdf_file/0003/158070/Open_letter_UK_internet_law_academics.pdf.

Concerning Member States which still wish to implement data retention it is hard to see how this could be accomplished. Although it is unclear to what extent the requirements of the Court are cumulative,[53] i.e. whether all of them have to be fulfilled or whether the CJEU would be willing to allow measures, which comply with a minimum core, it seems hardly possible to reconcile the idea of data retention with the requirements set up by the Court. While it stated that the fight against serious crime is of great importance and for this purpose communication data may be retained under certain conditions, it has been made clear, that the blanket retention of data of all citizens without any occasion or relation to serious crime is not in conformity with EU fundamental rights.[54] Therefore, Member States will have to settle for alternatives such as the 'quick freeze' process, where law enforcement authorities need to obtain a court order, which obliges a service provider to retain specified data of an individual or a group of individuals linked to criminal or terrorist activities. In a second step, the relevant authorities have to provide evidence within a limited time-frame, to obtain another court order, which obliges service providers to transfer the traffic data to them.[55] This concept addresses the Court's main point of criticism: the blanket retention of data of all European citizens. If implemented with the appropriate procedural and technical safeguards, this process has the potential to conform to the CJEU's requirements.

6 Conclusions

It follows from the foregoing considerations that the present judgment of the Court has effectively ended the blanket retention of traffic data in the European Union. Although it may take additional time and litigation before national courts to implement this judgment, a system like that envisaged by the DRD has been clearly identified as the grave violation of fundamental rights that it is.

This case is also a step forward in the exploration of the innovative and, from the perspective of EU jurisprudence, yet uncharted right to the protection of personal data as laid down by Article 8 CFR. However, the Court's reasoning in this regard needs further development. So far, the relationship of Article 8 CFR with the right to privacy according to Article 7 of the Charter remains opaque.

---

[53] For reading the requirements as cumulative cf. Kühling, Der Fall der Vorratsdatenspeicherungsrichtlinie und der Aufstieg des EuGH zum Grundrechtsgericht, Neue Zeitschrift für Verwaltungsrecht 2014, 681, 683; Reading the requirements as 'essential elements': Priebe, Reform der Vorratsdatenspeicherung – strenge Maßstäbe des EuGH, Europäische Zeitschrift für Wirtschaftsrecht 2014, 456, 458.

[54] Roßnagel, Neue Maßstäbe für den Datenschutz in Europa – Folgerungen aus dem EuGH-Urteil zur Vorratsdatenspeicherung, Multimedia und Recht 2014, 372, 375.

[55] Cf. The Federal Commissioner for Data Protection and Freedom of Information, Peter Schaar: "Quick Freeze" instead of data retention, Press Release of 15 June 2010, available at: http://www.bfdi.bund.de/EN/PublicRelations/PressReleases/2010/22_%22QuickFreeze%22.html?nn=410156.

Additionally, the relationship of the fundamental right to data protection with the general data protection regime of the Union remains to be explored with regard to the individual rights such as the right to access to data granted by Article 12 DPD. Yet, as this very data protection regime of the EU is currently in a process of reform, the future cannot be ascertained with certainty. While attention has largely focused on the envisaged General Data Protection Regulation[56], which is currently under discussion in the Council,[57] there is also a proposal for a directive concerning data protection with regard to criminal investigations,[58] which has been partially agreed on after a first reading by the European Parliament and is now under deliberation in the Council.[59]

While the last Commissioner for Home Affairs, Cecilia Malmström, announced that she had no plans to introduce any new legislation concerning data retention,[60] her successor in office, Dimitris Avramopoulos, after the tragic attacks of Paris in January 2015 stated that the Commission is monitoring the situation in the Member States and assesses the need for data retention.[61] Similarly, German chancellor Angela Merkel endorsed traffic data retention in conformity with the CJEU's requirements.[62] Thus, the possibility of a recurrence of some form of data retention on the EU level cannot be excluded with certainty. However, the Member States, at least for the time being, are under a legal obligation to implement the Court's ruling immediately.

The enforcement of the present judgment against Member States who are unwilling to abolish or revise their national laws will presumably require more litigation and is thus unlikely to be achieved in the near future. Moreover, as the example of the United Kingdom illustrates, even where a Member State adopts new legislation, the changes may not reflect the spirit of the judgment and also require further scrutiny by the judiciary. Despite these limitations with regard to the short term implementation

---

[56] European Commission, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) of 25 January 2012, COM(2012) 11 final.

[57] On the state of the legislative process cf. http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=201286.

[58] European Commission, Proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and free movement of such data of 25 January 2012, COM(2012) 10 final.

[59] Cf. http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=201285.

[60] Eder/Schiltz, EU will keine neuen Regeln für Vorratsdaten, Die Welt of 4 June 2014, available at: http://www.welt.de/politik/ausland/article128698101/EU-will-keine-neuen-Regeln-fuer-Vorratsdaten.html.

[61] European Commission, Speech by Commissioner Avramopoulos on Counter-Terrorism, SPEECH/15/3860 of 28 January 2015, available at: http://europa.eu/rapid/press-release_SPEECH-15-3860_en.htm.

[62] Statement by Chancellor Merkel of 15 January 2015, available at: http://www.bundeskanzlerin.de/Content/DE/Regierungserklaerung/2015/2015-01-15-regierungserklaerung.html.

of the judgment, the ruling at hand, in the long term, further advances the Court's role as a supreme court of the European Union which ensures the protection of individuals' fundamental rights.