Special Issue – Preliminary References to the CJEU
Part Five

Preliminary Reference and Dialogue Between Courts as Tools for Reflection on the EU System of Multilevel Protection of Rights: The Case of the *Data Retention Directive*

By Ludovica Benedizione & Eleonora Paris[*]

A. Introduction

The aim of this Article is to analyze the peculiar jurisdictional reaction that originated at the level of both the European Union (EU) and the Member States following the introduction, on 15 March 2006, of Directive 2006/24/EC of the European Parliament and the Council, "on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communication networks." [1]

The act, briefly named the *Data Retention Directive* (DRD or 'the Directive'), amended the previous Directive 2002/58/EC.[2] The need for such a legislative intervention on the part of the EU originated in the aftermath of the terrorist attacks that struck some European cities after the major attack in New York City on 11 September 2001. The Directive was in fact aimed at increasing the security of the Member States (and therefore, ultimately, of the EU) by strengthening the powers of the security agencies and police forces in prosecuting and preventing criminal acts of terrorism. A lively debate immediately arose around the adoption of the Directive; at first it focused on whether it should be based on the First or the Third pillar, and following its entry into force, on the serious potential clash of its contents and prescriptions with some fundamental rights protected by both the Charter of Fundamental Rights of the EU (CFR) and the European Convention on Human Rights (ECHR), especially the right to privacy. In reflection of these concerns, from 2008 onwards

[*] Ludovica Benedizione is a PhD Candidate in Comparative Institutions and Policies at the "Aldo Moro" University of Bari, and a TA in Comparative Constitutional Law at Luiss "Guido Carli" University, Rome. Eleonora Paris is PhD in International Political and Social Sciences at the University of Teramo, and a TA in Comparative Constitutional Law, Luiss "Guido Carli" University, Rome. Although this article is the result of the joint work of the two authors, Ludovica Benedizione is the author of Sections C, C II and Section D and Eleonora Paris is the author of Sections B (and subparagraphs), C I, and E. The remaining parts have been jointly written.

[1] EC Directive 2006/24 of 15 March 2006, O.J. 2006 L 105/54.

[2] EC Directive 2002/58 of 12 July 2002, O.J. 2002 L 201/37.

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press

several national courts[3] of the EU Member States started declaring the internal laws transposing the Directive to be unconstitutional.

A crucial turning point finally came in 2012, when the Irish High Court[4] and then the Austrian *Verfassungsgerichtshof* (Constitutional Court) raised doubts about the compatibility of the Directive's transposition laws with the EU normative framework on fundamental rights, and decided to make preliminary references to the Court of Justice of the European Union (CJEU). Some months later, in September 2013, a similar issue was brought to the attention of the Slovenian Constitutional Court, which, having ascertained the correspondence of the pledges presented by the Irish and Austrian plaintiffs with those submitted to its consideration, decided to suspend its proceedings, waiting for the CJEU to pronounce on the two other references. The decision of the CJEU was finally delivered on 8 April 2014. It was a milestone judgment, declaring void the entire Directive (an approach that strikingly differs from the Court's general case law, which tends to simply rule against specific legislative provisions)[5] on the grounds of its incompatibility with fundamental rights.

There are several aspects of utmost interest in this complex series of judgments, starting from the suddenly extensive use of the preliminary reference to the CJEU. From a first point of view, the DRD case cast a new light over the multilevel system of protection of rights, highlighting the importance of balancing fundamental individual rights (privacy, protection of personal data, freedom of expression, personal freedom) with the unavoidable need to provide for common security measures, in order to prevent and counter the threats to the collective right to security caused by the re-emergence of international terrorism. In particular, the entire experience put into evidence the crucial role of the CJEU in verifying the conformity of the balancing solutions elaborated in the law-making process—in which the role of State interests and claims, enhanced by their representation in the European organs, can have a chance to prevail—with the intangible fundamental rights of individuals and the common normative framework provided by EU law.

A second relevant issue is the one related to judicial interaction, intended as the cooperation among national Courts, as the dialogue between them and the CJEU, and

[3] Namely, the Bulgarian Supreme Administrative Court, in 2008, the Romanian Constitutional Court, in 2009, the German Federal Constitutional Tribunal, in 2010, the Czech Constitutional Court, in 2011, and the Cypriot Supreme Court, in 2011.

[4] According to the system of constitutional review of legislation in place in Ireland, the High Court is, together with the Supreme Court, the judicial authority empowered to check the compliance of the legislation enacted with the Constitution.

[5] *See* Franziska Boehm & Mark D. Cole, *Data Retention after the Judgment of the Court of Justice of the European Union* 41 (2014), *available at* http://www.greens-efa.eu/.

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press

finally as the complex relationship between the CJEU and the European Court of Human Rights (ECtHR). In this sense, the peculiar position assumed by the Constitutional Court of Slovenia, that—conditioning its final decision not only to the one of the CJEU, but ultimately also to the Irish and Austrian proceedings—showed a new and potentially groundbreaking openness to the dialogue, could lead the way to the strengthening of a "healthy" and fruitful collaboration among national judges. In addition to the evident importance of this phenomenon *per se* for the development and the application of EU law, it is necessary to consider its potentially decisive role in relieving the burden of pending procedures before the European judges.

It is therefore in such a twofold perspective that this contribution will consider the use of the preliminary reference procedure in the DRD case. Following an analysis of the Directive itself, and an *excursus* of the legal proceedings that led to its referral before the CJEU, an overview of the issues relating to the protection of the involved fundamental rights and to the interpretation of the Treaties raised by the Irish and Austrian preliminary reference rulings and by the Slovenian Court's decision to suspend its proceedings will be provided. This will be followed by a focus on the related answers and solutions offered by the CJEU in its decision. Although not all the concerned national courts have concluded their proceedings, in order to complete the broader picture an attempt to analyze the effects of the CJEU's ruling at the national level will then be briefly undertaken. This will then lead to the concluding remarks on the value of this complex judicial experience for the development and the improvement of both the multilevel protection of fundamental rights and the dialogue among national courts, between them and the CJEU and, potentially, between the CJEU and the ECtHR.

B. The Directive

The EU's DRD establishes an obligation for providers of publicly available electronic communications services and also for providers of public communication networks to retain traffic and location data for a period of time ranging from six months to two years "for the purpose of the investigation, detection and prosecution of serious crime."[6] The provisions of this Directive, as we are going to see, caused significant concerns within the EU. These concerns related to the compatibility of the Directive with fundamental rights such as the right to privacy and to the protection of data. According to the Preamble of the Directive, its adoption was strongly conditioned by the particular political climate of those years; in fact, as is pointed out in the Preamble, the terrorist attacks on Madrid and London (in March 2004 and July 2005, respectively) "reaffirmed [...] the need to adopt

[6] "This Directive aims to harmonize Member States' 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 the 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." EC Directive 2006/24, *supra* note 1, at Art. 1.

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press

common measures on the retention of telecommunications data as soon as possible."[7] The European Commission officially proposed its adoption in September 2005, urged by the European Council following the Madrid terrorist bombing and the London terrorist attacks. However, although EU institutions, security agencies, and police forces consider the retention of traffic data to be a crucial tool in the fight against terrorism, this Directive has also been considered to be one of the most privacy-invasive instruments ever adopted in the EU's framework, and one of the most controversial too.

As anticipated, a debate on the Directive had arisen also prior to its adoption. This was focused on whether the issue of data retention should be regulated by one of the instruments covered by the First Pillar or one of those that fall under the Third Pillar,[8] thus namely if it should be a directive or a framework decision. In 2006, Ireland, supported by Slovakia, appealed to the CJEU[9] asking for the annulment of the Directive on the grounds that "it had not been adopted on an appropriate legal basis."[10] Ireland argued that the correct legal basis for data retention was to be found in "the provisions of the EU Treaty concerning police and judicial cooperation in criminal matters" rather than in the provisions on the internal market.[11] Therefore, it argued, the issue should have been regulated under the Third Pillar's legal bases, that is to say with a framework decision. By contrast, however, in February 2009, the CJEU stated that the DRD regulates operations which:

> are independent of the implementation of any police and judicial cooperation in criminal matters. It harmonizes neither the issue of access to data by the

[7] *Id.* at Preamble, para. 10.

[8] The Treaty of the European Union, adopted in Maastricht in 1992, introduced a new institutional structure for the EU, which remained until the adoption and the entry into force of the Treaty of Lisbon. This institutional structure was composed of three "pillars": the first, so-called Community pillar, which corresponded to the three Communities: the European Community, the European Atomic Energy Community (EURATOM), and the former European Coal and Steel Community (ECSC); the second pillar devoted to the common foreign and security policy (Title V of the Treaty on European Union); finally, the third pillar devoted to police and judicial cooperation in criminal matters (Title VI of the Treaty on European Union).

[9] Case C–301/06, Ireland v. European Parliament and Council of the European Union, 2009 E.C.R. I–00593.

[10] Press Release, Court of Justice of the European Union, No 11/09, 1 (10 February 2009), http://curia.europa.eu/jcms/upload/docs/application/pdf/2009-03/cp090011en.pdf.

[11] "Ireland submits that the choice of Art. 95 EC as the legal basis for Directive 2006/24 is a fundamental error. Neither Article 95 EC nor any other provision of the EC Treaty is, in its view, capable of providing an appropriate legal basis for that directive. Ireland argues principally that the sole objective or, at least, the main or predominant objective of that directive is to facilitate the investigation, detection and prosecution of crime, including terrorism. Therefore, the only legal basis on which the measures contained in Directive 2006/24 may be validly based is Title VI of the EU Treaty, in particular Articles 30 EU, 31(1)(c) EU and 34(2)(b) EU." *Ireland*, Case C–301/06 at para. 28.

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press

> competent national law-enforcement authorities nor that relating to the use and exchange of those data between those authorities. […] It follows that the substantive content of Directive 2006/24 is directed essentially at the activities of the services provided in the relevant sector of the internal market, to the exclusion of State activities coming under Title VI of the EU Treaty. In light of that substantive content, Directive 2006/24 relates predominantly to the functioning of the internal market.[12]

According to the CJEU, the Directive was, therefore, correctly adopted as a First Pillar legal instrument, under Article 95 of the EC Treaty. As we noted earlier, the Directive, adopted with the purpose of harmonizing the legislation of EU Member States on the conservation of personal data collected through electronic communication services, requires operators to retain certain categories of data, that is: "[…] the source and the destination of communications; the data, time and duration of communication; the type of communications; user's communication equipment and the location of mobile communication equipment […]."[13] Data must be retained for a period of time ranging from a minimum of six months to a maximum of two years. Each Member State could establish the exact duration as well as the conditions under which data may be accessed. Moreover, Member States should make the data retained available, on request, to law enforcement authorities for the purposes of investigating and prosecuting serious crime.

I. The European Legal Framework

Coming to the analysis of the legal framework in which the Directive has been adopted, it is necessary to underline that at EU level, the issue of retention and use of data for the purposes of law enforcement was first established in Directive 97/66/EC concerning "the processing of personal data and the protection of privacy in the telecommunications sector."[14] For the first time, the Directive provided for the possibility to adopt measures similar to those covered later on also by the DRD for the maintenance of public order and the protection of public security.[15] Following Directive 97/66/CE, its provisions were developed in the so-called *e-Privacy* Directive,[16] which provides for the possibility for

[12] *Id.* at paras. 83–85.

[13] *See* EC Directive 2006/24, *supra* note 1, at Art. 5 for further technical details.

[14] EC Directive 97/66 of 15 December 1997, O.J. 1998 L 024/01.

[15] In particular, the Directive prescribed that traffic data had to be deleted or made anonymous at the very end of each communication; it also generally prohibited the extensive retention of data.

[16] EC Directive 2002/58, *supra* note 2.

Member States to adopt legislative measures for public order and public security purposes, including in some cases the retention of data. In fact, Article 15 of the *e-Privacy* Directive allows Member States to restrict privacy rights and obligations "when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defense, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system."[17] Article 15 of the *e-Privacy* Directive has been amended by the DRD,[18] establishing that Article 15 does not apply to data retained under the DRD. Thus, Member States could still derogate from the principle of confidentiality of communications under the provisions established in the *e-Privacy* Directive, because the DRD governs the retention of data only for the purpose of investigating, detecting, and prosecuting serious crimes. Moreover, in both of the Directives mentioned, the definition of the notion of 'serious crime' is completely absent, making it difficult to distinguish measures taken by the States under the DRD from measures taken in application of the more general data retention regime regulated by Article 15 of the *e-Privacy* Directive.

In addition, the DRD left it to Member States to specify the procedures to follow in order for the national authorities to access the retained data. What has to be stressed here is that these procedures have to be defined in accordance with the requirements of necessity and proportionality, in the light of the ECHR and the CFR.[19]

The process of the transposition of the DRD allows us to consider one of the most controversial aspects of the whole data retention issue. Member States were required to transpose the provisions of the Directive into national law by 15 September 2007, with the option of postponing the implementation of retention obligations relating to internet access, internet email, and internet telephony until 15 March 2009.[20] From the beginning, the transposition of the Directive met with considerable resistance in several countries and its application has proved problematic and lengthy in many Member States. Even with the possibility of postponing the application for internet data retention, six EU Member

[17] *Id.* at Art. 15.

[18] EC Directive 2006/24, *supra* note 1, at Art. 11 ("the following paragraph shall be inserted in Article 15 of Directive 2002/58/EC: 1a. Paragraph 1 shall not apply to data specifically required by 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 to be retained for the purposes referred to in Article 1(1) of that Directive.").

[19] *Id.* at Art. 4.

[20] This option was adopted by Austria, Belgium, Cyprus, Czech Republic, Estonia, Finland, Germany, Greece, Latvia, Lithuania, Luxembourg, the Netherlands, Poland, Slovenia, Sweden, and the UK. For the specific legislation through which Member States transposed the Directive see the EUR-Lex register, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX.

States[21] found themselves subjected to infringement proceedings brought by the European Commission due to the failure to implement the Directive within the time allowed.

II. Critical Aspects

The difficulties experienced in the application of the DRD are mainly due to the question of its compatibility with certain fundamental human rights, first of all the right to privacy (Article 7 CFR[22]), the right to protection of personal data (Article 8 CFR[23]), and the right to freedom of expression (Article 11 CFR[24]). The Directive also seems to be incompatible with Article 16 of the Treaty on the Functioning of the European Union (TFEU), which enshrines everyone's right to the "protection of personal data concerning them."[25] When dealing with the legality of the Directive with regard to fundamental rights, it is important to stress that the Directive's provisions did not establish anything about the conditions under which access to the retained data may be granted. The Directive only provides that the purpose of data retention is the "investigation, detection and prosecution of serious crime."[26]

Before analyzing the critical aspects of the Directive that emerged in the sentences of some of the national constitutional courts, which had the possibility of pronouncing on the limits that national constitutions establish for the supremacy of EU law over national law, it seems important to underline that the protection and the defense of the right to privacy in the framework of the EU is no more an exclusive prerogative of Member States. With the entry into force of the Lisbon Treaty on 1 December 2009, the CFR was introduced in the EU normative sources. Article 6 of the Treaty on the European Union (TEU), as amended by the Lisbon Treaty, states that "the Union recognizes the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union [...] which shall have the same legal value as the Treaties." The Charter is part of EU primary law and, therefore, all

[21] Namely, Austria, the Netherlands, and Sweden in May 2009; Greece and Ireland in November 2009; and Germany in May 2012.

[22] Art. 7 CFR: "Respect for private and family life - Everyone has the right to respect for his or her private and family life, home and communications."

[23] Art. 8 CFR: "Protection of personal data - 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority."

[24] Art. 11 CFR: "Freedom of expression and information - 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers [...]."

[25] TFEU Art. 16, para. 1.

[26] *See* EC Directive 2006/24, *supra* note 1, at Art. 1.

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press

acts of secondary EU law, directives in particular, have to comply with it. Consequently, national constitutional courts do not enjoy the power to check the accordance of EU directives with fundamental rights.

Prior to the aforementioned proceedings of the national courts, the European Commission itself, in submitting its proposal for the Directive in 2005, had highlighted the possible impact of data retention on the rights to privacy and protection of personal data. As reported in the Proposal for a directive on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC,[27] the Commission noted that the Directive could have consequences for the rights to privacy and protection of personal data, as set out in Articles 7 and 8 of the CFR. However, the Commission considered interference with these rights to be justified in the light of the provisions of Article 52 of the Charter.[28] Therefore, the measures provided for in the DRD were considered to be proportionate and necessary in order to pursue the objective of combating terrorism.

Criticism concerning the Directive, however, has been highlighted by the judgments of national supreme and constitutional courts, which have detected the inconsistency of domestic legislation implementing the Directive with national Constitutions. More specifically, since 2008, some Member States' Supreme Courts have declared unconstitutional provisions of the national laws transposing the DRD, due to alleged infringement of the right to privacy and the right to protection of data. These national Courts include: the Bulgarian Supreme Administrative Court (2008),[29] the Romanian Constitutional Court (2009),[30] the German Constitutional Tribunal (2010),[31] the Czech Constitutional Court (2011),[32] and the Cyprus Supreme Court (2011).[33] Moreover, a similar case—that is extremely interesting for our purposes—was pending before the Constitutional Court of Slovenia. Finally, when the CJEU gave its judgment on the DRD last April, other cases were pending in Member States. For example, in Hungary, a case was

[27] COM(2005) 438 final, 21 September 2005.

[28] Art. 52(1) CFR: "1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made 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."

[29] Bulgarian Supreme Administrative Court, No 13627, 11 December 2008, *at*http://www.capital.bg/getatt.php?filename=o_598746.pdf.

[30] Romanian Constitutional Court Decision no. 1258 of 8 October 2009, R.O.M. No. 789, 23 November 2009.

[31] German Constitutional Court, 1 BvR 256/08, Judgment of 2 March 2010.

[32] Czech Constitutional Court, Decision of 22 March 2011, Official Gazette of the Czech Republic 1 April 2011.

[33] Supreme Court of Cyprus, Civil applications 65/2009, 78/2009, 82/2009, 15/2010, 22/2010, Judgment of 1 February 2011, available in Greek *at* http://www. supremecourt.gov.cy.

initiated in 2008 by the Hungarian Ombudsman, but after the adoption of the Fundamental Law, which entered into force in January 2012, the procedures before the Hungarian Constitutional Court changed and pending cases, submitted by entities that were not entitled under the new provisions, were removed from the docket.[34]

As has been remarked,[35] the main criticism of the DRD underlined by national courts was related to the violation of fundamental rights of privacy and free correspondence, because of the collection of data of persons that were completely unaware about the storing of their personal data. Moreover, another aspect that has emerged from the judgments is the one linked to protection of personal data and to the circumstance that a mass data retention may cause the feeling of being constantly observed, thus limiting the freedom of expression and communication.

Taking into consideration the above-mentioned Constitutional Courts' judgments, it could be observed that the Courts basically highlighted the same critical points of the Directive. First of all, blanket data retention measures have been considered problematic in view of fundamental rights guarantees in most of the Courts' pronunciations. Furthermore, the main criticisms concerned both the vagueness and imprecision of the national legislative provisions with regard to who could access the retained data and for which purposes, the lack of a specific cause to justify the retention, and the fact that the retention could be applied to all the people using electronic communications. These aspects have been seen as a reason for a finding of incompatibility with constitutional requirements.

However, surprisingly, none of these Courts have decided to involve the CJEU by way of the preliminary reference procedure. They have rather chosen to concentrate fully on the critical aspects of national transposition acts, highlighted in some courts' pronunciations in a very detailed way. The preliminary reference procedure would have allowed the CJEU to rule earlier on the Directive and has, as a result, led to disappointment.

> […]Therefore the decisions – albeit after lengthy considerations – of first the Irish High Court and subsequently the Austrian Constitutional Court were welcomed with relief as they gave the CJEU the chance to revisit the fundamental rights questions left open in its initial (competency) judgment on the DRD. In view of the fact that the Court clearly and without room for interpretation stated that "by adopting Directive

[34] For more detailed information about the Hungarian case and other pending ones on the DRD, see Eleni Kosta, *The way to Luxemburg: national Court decision on the compatibility of the Data Retention Directive with the rights to privacy and data protection*, 10/3 SCRIPTED, 339 (2013).

[35] Boehm & Cole, *supra* note 5, at 14.

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press

> 2006/24, 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" it is, retrospectively speaking, an even stronger disappointment that the national Courts did not act earlier and thereby contributed to a more swift clarification of the validity (or actually invalidity) of this important piece of EU secondary law.[36]

Through the examination of the rulings of the Courts, it can be noted how these have primarily emphasized the impact of the legislation transposing the DRD on the fundamental rights to privacy and protection of personal data. As regards the fundamental right to privacy, the first court to underline its violation by the domestic measure transposing the DRD was the Bulgarian Supreme Administrative Court.[37] In the opinion of the applicants, Article 5 of the concerned Regulation[38] constituted a violation of the right to privacy, as it allowed passive technical access to all retained data for broad purposes through a dedicated computer terminal. Access to data was permitted for operative investigation activities, and allowed investigation, prosecution, and judicial authorities to access the data for trials. It also allowed security services to access the retained data for national security reasons. These provisions were formulated in a very vague and imprecise way; thus the NGO argued that sufficient safeguards for the protection of the private lives of citizens were not provided by the Regulation, as required by Article 32 of the Bulgarian Constitution.[39] The Court found that the provisions of Article 5 violated the right to privacy as enshrined in Article 32 of the Bulgarian Constitution and in Article 8 of the ECHR, and annulled it because of the lack of any guarantees provided.[40] The Court highlighted the

[36] *Id*. at 19.

[37] Bulgaria transposed the Directive in the Regulation No. 40 of the Ministry of Interior of 7 January 2000 (available at http://lex.bg/laws/ldoc/2135577924). The NGO "Program Action to Information" filed a complaint at the Bulgarian Supreme Administrative Court, after the transposition of the Data Retention Directive, claiming the violation of the right to privacy caused by the Regulation.

[38] Art. 5, Regulation No.40 of the Ministry of Interior of 7 January 2000 (note 37).

[39] Art. 32, Constitution of the Republic of Bulgaria, Jul. 1991, SG 56/13: "(1) The privacy of citizens shall be inviolable. Everyone shall be entitled to protection against any illegal interference in their private or family affairs and against encroachments on their honour, dignity and reputation. (2) No one shall be followed, photographed, filmed, recorded or subjected to any other similar activity without their knowledge or despite their express disapproval, except when such actions are permitted by law."

[40] As it has been pointed out, "[…] the decision is important, as it was the first decision of a national court that examined data retention in relation to the right to privacy of citizens, albeit on an issue that the Directive left to the Member States to regulate. Moreover, the direct reference to Art. 8 ECHR rather than merely to the relevant provision of the Bulgarian Constitution illustrates the importance of data retention aspects with regard to the right to privacy." *See* Kosta, *supra* note 34, at 346.

importance of the procedure for receiving access to the retained data and declared the act to be in breach of the Constitution,[41] partly because it did not specify this procedure sufficiently. As a result, the Court declared void some provisions of the Bulgarian data retention act, but not the act as a whole.

Another important reaction to the transposition of the DRD could be seen in the Decision of the Romanian Constitutional Court of October 2009,[42] which annulled in total the national transposition act[43] on grounds of unconstitutionality. The Court, referring to the case law of the ECtHR,[44] found the scope and purpose of the transposing law to be ambiguous and lacking sufficient safeguards, and it highlighted the incompatibility of the legal obligation to retain all traffic data for six months with the rights to privacy, referring to Article 8 of the ECHR.[45] In addition to this violation of the right to privacy (as enshrined in Article 26 of the Romanian Constitution),[46] the Court found a number of reasons as to why the transposition act was not in conformity with the Constitution, namely the inviolability of domicile (Article 27), the right to free development of human personality (Article 1(3)), and the right to secrecy of communications (Article 28).

The violation of the fundamental right to privacy by a national provision implementing the DRD was also underlined by the German Federal Constitutional Court,[47] which annulled essential parts of the German telecommunications law amendments transposing the

[41] Bulgarian Supreme Administrative Court, Decision No 13627 (note 29).

[42] Romanian Constitutional Court Decision no. 1258 (note 30).

[43] Law No. 298/2008, Official Monitor No. 780 of 21 November 2008.

[44] Eur. Court H.R., *Rotaru v. Romania*, Judgment of 4 May 2000, Reports of Judgments and Decisions 2000–V; Eur. Court H.R., *Sunday Times v. UK*, Judgment of 26 April 1979, Series A, No. 30; Eur. Court H.R., *Prince Hans-Adam of Liechtenstein v. Germany*, Judgment of 12 July 2001, Reports of Judgments and Decisions 2001–VIII.

[45] Art. 8, ECHR, "1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

[46] As underlined by the Court: "[…] the continuous limitation of the privacy right and the secrecy of correspondence makes the essence of the right disappear by removing the safeguards regarding its execution. The physical and legal persons, mass users of the public electronic communication services or networks, are permanent subjects to this intrusion into their exercise of their private rights to correspondence and freedom of expression, without the possibility of a free, uncensored manifestation, except for direct communication, thus excluding the main communication means used nowadays." Romanian Constitutional Court Decision no. 1258.

[47] "The adoption of a law implementing the Data Retention Directive in Germany faced immense public outcry. After the transposition of the Directive into German law, the German Constitutional Tribunal was called upon to decide on the compatibility of specific provisions of the legislation with the right to the secrecy of communications and the right to informational self-determination." *See* Kosta, *supra* note 34, at 349.

DRD,[48] but not the legislation entirely. More precisely, the Court considered the act under scrutiny to violate Article 10 of the *Grundgesetz* (Basic Law for the Federal Republic of Germany)[49] which protects the privacy of correspondence, post, and telecommunications. In the opinion of the Court, "Data Retention for LE[50] purposes is not per se incompatible with this provision of the Constitution [...] but the measures to protect citizens against massive infringement of their fundamental rights were seen to be insufficient."[51] As underlined by the Court, through the data collected it is possible to establish the profiles of all citizens and therefore to know all their movements and habits, thereby violating the fundamental right to privacy. Such a restriction on the right to privacy could only be admissible under particular and strictly limited circumstances that "would necessitate very high standards for data security, transparency of the processing and legal protection against violations including the possibility of effective sanctions."[52]

In February 2011, the Supreme Court of Cyprus also focused on the issue of access to the retained data, stressing the importance of the right to private and family life and the right to the protection of secrecy of correspondence.[53] The court had to decide on the validity of orders for access to retained data based on Articles 4 and 5 of the Cypriot law 183(1)/2007 about the retention of telecommunications data for investigation of serious crimes, adopted in order to transpose the DRD. The applicants questioned the compatibility of the abovementioned Articles 4 and 5 with the right to private and family life and with the right to the protection of secrecy of correspondence, protected under Articles 15 and 17 of the Cypriot Constitution, respectively.

In its reasoning, the Court focused on the legal provisions that were put in place with the law 183(1)/2007 and the transposition of the Directive in the national legislation, and stated that the Directive "does not impose any obligation of the Member States to set down provisions on the access to the retained telecommunications data of the citizens or

---

[48] German Constitutional Court (*Bundesverfassungsgericht*), 1 BvR 256/08, Judgment of the of 2 March 2010, http://www.bverfg.de/pressemitteilungen/bvg10-011en.html

[49] Art. 10 Basic Law for the Federal Republic of Germany: "(1) The privacy of correspondence, posts and telecommunications shall be inviolable. (2) Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a Land, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature."

[50] Law Enforcement.

[51] Boehm & Cole, *supra* note 5, at 17.

[52] *Id.*

[53] Civil Applications 65/2009, 78/2009, 82/2009, 15/2010 and 22/2010, *supra* note 33. *See* Christiana Markou, *The Cyprus and other EU court rulings on data retention: The Directive as a privacy bomb,* 28 COMPUTER L. & SECURITY REV. 468 (2012).

on their transmission to the competent authorities."[54] Thus, the issues of access to the retained data, and of the transfer of these data to the authorities, were left to the Member States to regulate in national legislation and did not fall within the scope of the DRD. The provisions of Articles 4 and 5 of the Cypriot Law in question were not covered by Article 1A of the Constitution of Cyprus.[55] The Court, having clarified that it did not have competence to question the validity of the DRD and the Cypriot law adopted to implement it, examined whether the orders for access to retained data based on Article 4 and 5 of the Cypriot Law transposing the DRD were compatible with Articles 15 and 17 of the Cypriot Constitution. In three of the four cases on which the Court had to rule it found that there was actually an interference with the rights to privacy and secrecy of communications, as protected in the Constitution and, consequently, it annulled the relevant order for access to retained data. In the fourth case, the Court found that there was an interference but that this was justified on the bases foreseen in the Constitution.

Finally, and again in 2011, the Czech Constitutional Court annulled the DRD's transposition law because of its insufficient precision and insufficient clarity in its formulation, the law being a measure which interfered with fundamental rights. Considering the scope of the data retention provisions, the Court criticized the purpose limitation of the Directive as being insufficiently detailed. According to the Court, in the Directive there are insufficient guarantees and safeguards against the possibility of abuses of power by public authorities. Furthermore, in an *obiter dictum* doubts are expressed about the necessity, efficiency, and appropriateness of the retention of traffic data as an instrument to fight against serious crime, taking into account the emerging phenomenon of new methods of criminality, such as, for example, through the use of anonymous SIM cards.

However, although some of the decisions presented above were very precise and strict in judging the unconstitutionality of domestic legislation transposing the Directive, none of these Courts, as we said before, made a reference to the CJEU about the possibility that the original DRD itself was not in conformity with EU fundamental rights. This happened only with the preliminary reference to the CJEU made by the Irish High Court and the Austrian Constitutional Court which, rather than proceeding directly to the judgment of

[54] *See* Kosta, *supra* note 34, at 353. For a complete analysis of the issue see Supreme Court of Cyprus, Decision of civil applications 65/2009, 78/2009, 82/2009, 15/2010, 22/2010, 1 February 2011, *available at* http://www.supremecourt.gov.cy.

[55] Art. 1A of the Constitution of Cyprus was amended in 2006 and provides that: "[n]o provision of the Constitution shall be deemed as overriding any legislation, acts or measures enacted or taken by the Republic that are deemed necessary due to its obligations as a Member State of the European Union, neither does it prevent Regulations, Directives or other Acts or binding measures of a legislative character, adopted by the European Union or the European Communities or by their institutions or competent bodies thereof on the basis of the Treaties establishing the European Communities or the Treaty of the European Union, from having legal effect in the Republic."

national laws transposing the Directive, considered preventive cooperation with the CJEU as being a necessary step to solving the cases.

C. Questioning the *Data Retention Directive*: The Three Core Judgments of the Irish, Austrian, and Slovenian Courts

The "judicial domino" of preliminary references regarding the DRD had its origins in 2006, when Digital Rights Ireland—an Irish company committed to the promotion and protection of civil and human rights in the field of modern communication technologies—filed a complaint before the High Court of Ireland[56] against the Minister for Communication, Marine and Natural Resources, the Minister of Justice, Equality and Law Reform, the Commissioner of the Irish Police Force, Ireland, and the Attorney General. The Company, that had had a major role in the public debate on the updating of Ireland's national laws in the telecommunications, interceptions, and metering areas,[57] claimed that the acquisition

[56] Irish High Court, *Digital Rights Ireland Ltd. v. Minister for Communication & Others*, Judgment of 5 May 2010, [2010] IEHC 221.

[57] The proposal for an updating of the EU legislation in the matter of data retention and security provisions to counter terrorism, from which the DRD eventually originated, was put forward by Ireland during its turn of Presidency of the EU in April 2004. In submitting its proposal for a Framework Decision on Data Retention (Council Document 8958/04, ADD1, of 28 April 2004), the Irish Government was both officially pushing for a concrete response to the terrorist attacks that occurred in Madrid a month earlier and searching for a supranational normative solution to a critical situation that had arisen in its internal legal order. Ireland had set up a comprehensive telecommunication law relatively early, in 1983 (*Postal and Telecommunication Services Act*, 1983. For the complete text of this and the other quoted Irish laws, see http://acts.oireachtas.ie/en.toc.decade.html), and then perfected it with the *Data Protection Act* of 1988, (approved in order to harmonize the Irish normative framework with the requirements of the Convention for the protection of individuals with regard to automatic processing of personal data, signed in Strasbourg on 28 January 1981), that regulated the management of communication data and instituted the Data Protection Commissioner, in charge of the supervision and monitoring over the respect of the Convention. The effectiveness of these normative efforts was seriously impaired by the absence of a comprehensive discipline of metering, that is to say the collection and disclosure of telephonic traffic and location data. In particular, although the access of public security authorities to communication data in case of State security and offence prosecution needs was somehow limited and subdued to formal prescriptions, no preemptive independent authorization was prescribed for collecting the data, nor specific monitoring over their use established; such use was not bound to necessity or proportionality requirements, and it was not circumscribed to serious offences; no time limit was furthermore set for the collection and retention of traffic and location data (*see* T.J. McIntyre, *Data retention in Ireland: Privacy, policy and proportionality*, in 24 COMPUTER L. & SECURITY REP. 326, 327 (2008)). The parallel development of the then European Community's discipline in the field of telecommunication, with the approval of the Directive 97/66/EC, *supra* note 14, gave Ireland a chance to complete its legislative coverage of metering, but again no transposing law was passed until 2002, thus substantially leaving telecommunication operators free to decide whether to retain traffic data; the only requirements were that the retained information to be somehow relevant and by no means excessive, and their storage was generally allowed for no longer than necessary to its purpose. In late 2001, an enquiry revealed the Irish mobile telephone companies would retain traffic and location data for a period of six years, making them available to the public security authorities when requested (see *Irish, know where you've been*, WIRED NEWS, Nov. 9, 2001). The issue was brought to the attention of the Data Protection Commissioner, who concluded that the length of the storage period was inconsistent with both the *Data Protection Act* and the relevant EU normative framework, and set it to a maximum of six months. The Commissioner's decision was opposed by the institutions (and in particular, by the Department of Justice, which

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press

and retention, on the basis of national norms and Directions (namely, the 2001 Direction issued by the Minister for Public Enterprise,[58] the *Criminal Justice (Terrorist Offences) Act* of 2005, and the subsequent Direction of the Commissioner of the Police Force to the telecommunication service providers, ordering them to retain data),[59] of data belonging to it, its members, and other users of mobile phones, had been conducted by the Defendants in breach of several law provisions, both at the national and at the EU level. In particular, the processing and storage of data that were related to Digital Rights Ireland, its members, and other mobile phone users were allegedly not consistent with Articles 40.3.1, 40.3.2, and 40.6.1 of the Irish Constitution, protecting the rights to privacy, to travel, and to

---

rather sustained that the maximum retention period should have been established at three years in case of security exigencies), that in an attempt to circumvent it, relying upon section 110 of the *Postal and Telecommunication Act* 1983, created a secret direction in which the said companies were ordered to instead keep any kind of traffic data for three years. The provision, severely limiting the right to privacy, was in manifest contradiction with both the dispositions of Directive 97/66/EC and Art. 8 of the ECHR, stating that any interference by a public authority with the exercise of the right to respect for private and family life, home and correspondence is only admissible when it happens in accordance with the law. A character of the said direction was evidently missing, in this—moreover—illegitimately overstepping the powers and prerogatives of the Irish Parliament and, as a consequence, also those of the judiciary in the exercise of its power of reviewing legislation. Eventually informed of the direction, the Data Protection Commissioner challenged it on the basis of these legal standpoints, obtaining the commitment of the Minister of Justice to submit to the Parliament a Bill properly regulating the issue within some months, by the end of 2002. In the meantime, the direction would have worked as a provisional measure. The originally proposed deadline of late 2002 was eventually missed, and the Irish Government decided to postpone the whole proceeding, "lifting" it within the EU context with the proposal of a Framework Decision on Data Retention. In parallel, an unrelated Bill translating into law the content of the 2002 direction through an amendment to the *Criminal Justice (Terrorist Offences) Act* 2005, was surreptitiously introduced at the Irish Parliament, and finally approved in 2005, also as a response to the activism of the Data Protection Commissioner, who had in the meantime at first ordered telecommunication providers to delete any traffic data in their possession that had been stored for longer than six months, and then raised the issue in front of the Irish Courts (See Irish Court of Criminal Appeal, *People (DPP) v. Murphy*, 2005 IE CCA 1). In its Part 7, the so-approved *Criminal Justice (Terrorist Offences) Act* officially established that traffic and location data transmitted through a fixed line or mobile phone had to be retained by the competent providers for a period of three years upon request of the Commissioner of the police force, in order to allow—as stated by Section 63—"(a) the prevention, detection, investigation or prosecution of crime (including but not limited to terrorist offences), or (b) the safeguarding of the security of the State." Such data could, as per the previous legislation, be acceded and disclosed upon authorization (that had to be countersigned by a senior member of the police or military force), the disclosure being mandatory for the providers once requested (*see* Eleni Kosta & Peggy Valcke, *Retaining the Data Retention Directive*, 22 COMPUTER L. & SECURITY REP. 377 (2006)). Meanwhile, on the EU front, the former Proposal for a Framework Decision, that Ireland wished to be approved within the Third Pillar, had instead been passed as a First Pillar Directive; after its coming into force, the Irish Government challenged its legal basis in front of the CJEU (at the time still named European Court of Justice), under Article 230 Treaty on the European Community (TEC) (now Article 263 TFEU. *See Ireland*, Case C–301/06). Later on in 2009, the CJEU ruled against the Irish Government, confirming that the Directive had been properly approved under Art. 95 TEC (now Art. 117 TFEU). After the entry into force of the Directive, the Irish society witnessed the start of a new and feverish phase of debate that led to the referral of both the Directive and the national legislation in the field of retention of data to the Irish High Court.

[58] That was in fact the predecessor of the Minister for Communication, Marine and Natural Resources.

[59] *See supra* note 57.

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press

communicate. They furthermore were against Articles 6(1), 8, and 10 of the ECHR, insofar as they limited the Plaintiff's right to private life, family life, and privileged communication. For this reason, Digital Rights Ireland claimed that Article 63(1), contained in Section 7 of the *Criminal Justice (Terrorist Offences) Act* 2005 and disciplining the retention of data was invalid, and that Directive 2006/24/EC was not consistent with the CFR and the ECHR. In seeking due remedies, the Plaintiff not only asked for declarations to the effect that the Defendants had acted in breach of the domestic and EU laws and that the *Criminal Justice (Terrorist Offences) Act* 2005 was null and void as incompatible with the Constitution, EU law, and Ireland's obligations under the ECHR. More relevantly, in fact, Digital Rights Ireland asked for a Declaration that the EU DRD was null and void for violating the EC Treaty and had been adopted without any legal basis, and sought an Order of the High Court under Article 267 TFEU, referring several questions to the CJEU.

In particular, the CJEU was first of all to be asked to verify the validity of the Directive considering the content of Articles 6(1) and 6(2) TEU (that recognize the CFR as having the same value as the Treaties and prescribe the accession of the EU to the ECHR). Secondly, Articles 3a TEU (now Article 4(3), 1) and 21 TFEU, expressing, respectively, the due commitment of the Member States to absolving the duties and obligations set on them by the Treaties, and recognizing the right to free movement, were raised as parameters, as also was Article 5 TEU (with explicit reference to the principle of proportionality). Finally, and perhaps most significantly, there was a request regarding the compatibility of the Directive with the CFR, with special reference to Article 7 (the right to private and family life, home, and communications), Article 8 (the right to the protection of personal data and establishing *inter alia* they "must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law"), Article 11 (protecting freedom of expression, information and communication from the interference of public authorities), and Article 41 (the right to good administration).[60]

In May 2010, the Irish High Court, having recognized that it lacked the legal capacity to rule on the validity of EU law, that the case raised "important constitutional questions," and that it was furthermore relevant for almost the whole Irish population, ruled in favor of the appellant, granting it also the application for a preliminary reference to the CJEU.[61] The questions to be submitted, the Court decided, were to be defined at a later stage, through further consultations in which the parties were invited to participate in presenting any suggestions and opinion they deemed to be relevant.[62]

[60] Originally, the Plaintiff also asked for the CJEU to specify whether the Directive was lacking the correct legal basis in EU law, but the question was dismissed during the proceedings after the delivery of the recalled *Ireland*, Case C–301/06.

[61] Irish High Court, *Digital Rights Ireland Ltd.* at para. 109.

[62] It must not be forgotten that, notwithstanding the judicial proceedings, the Irish Government still had to fulfill its duty to enact Directive 2006/24/EC, whose content was transfused in the *Communication (Retention of Data) Act* 2011 introducing the necessary modifications to the recalled national pre-existing legal framework on the

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press

The reference was finally filed in June 2012, asking the CJEU to verify the conformity of Articles 3, 4, and 6 of the Directive first of all with Article 5(4) TEU, in their imposing of disproportionate and unnecessary or inappropriate restrictions on the Plaintiff's rights in order to achieve the legitimate aims of ensuring the access to certain data for the purposes of investigation, detection, and prosecution of serious crime and/or ensuring the proper functioning of the internal market of the EU. The CJEU was then called on to ascertain whether the Directive was compatible with the right to free movement (protected by Article 21 TFEU), to privacy (Article 7 CFR and Article 8 ECHR), to protection of personal data (Article 8 CFR), to freedom of expression (Article 11 CFR and Article 10 ECHR), and to good administration (Article 41 CFR). As a last—and somehow revealing—question, the Irish High Court asked to be indicated to what extent the principle of loyal cooperation (Article 4(3) TEU) sets on national courts the duty to make sure that the internal legislation transposing the DRD is consistent with the guarantees set by the CFR.

In that same period of time, between April and June 2012, the Austrian Constitutional Court received three major applications questioning the validity of the newly approved legislative measures implementing the DRD.[63] The first of the appellants was the

matter; the intervention was quite limited, basically consisting in the establishment of a new mandatory retention period, that was set to two years for the telephonic traffic data and one year for the internet ones. The implementation of the new provisions was characterized by a peculiar attention to the judicial evolutions of the case in front of the EU Court.

[63] After the entry into force of the Directive, Austria was among the most reluctant Member States in transposing its content. Once implemented, in fact, the DRD would have significantly overturned the Austrian internal legislation in this matter (contained in the Austrian Code of Criminal Procedure, in the *Telekommunikationsgesetz* (Telecommunication Act, hereinafter TKG) 2003—Federal Law Gazette I No. 70/2003 and in the *Datenschutzgesetz* (Data Protection Act) 2000, DSG, BGBl. I 165/1999, as amended by BGBl. I 112/2011), originally extremely cautious in allowing the retention and processing of communication data, establishing the requisite of the users' consent as unavoidable in order to store any data relating to them, and imposing the shortest possible retention period. This explains the fierce opposition showed by the Austrian society at the entry into force of Directive 2006/24/EC that was the main cause of the delay in transposing the Directive into this legal order. Such an opposition had evidently been foreseen by the Austrian Government (on its side skeptical about the DRD's content), that had in fact declared, pursuant to Art. 15(3) of the Directive, that it was going to postpone its application for 18 months after the deadline of September 2007. The very first transposition bill, introduced to the Austrian Parliament in 2007, was repeatedly put off due to the massive public resistance, causing the missing of the prescribed March 2009 deadline. The European Commission consequently brought an action against Austria before the CJEU for an infringement of the EC Treaty (Case C-189/09, Commission v. Austria, 2010 E.C.R. I-00099), and on 29 July 2010, the CJEU predictably ruled against the Austrian State. Urged to remediate, the Federal Ministry for Transport, Innovation and Technology hence published a new Bill for transposition, consisting in a series of cautious amendments to the TKG, aimed at limiting any interference with fundamental rights as much as possible. In order to appease the internal climate of criticism, the public was involved in the Bill's drafting before its presentation to the Parliament, through the possibility to submit any observations on its content by February 2010. The amended TKG released by the Austrian Legislature on 18 May 2011 therefore aimed at complying with the minimum requirements of the Directive: the maximum data retention period for telecommunication services providers was set to six months after the termination of a communication, admitting it "solely for the purpose of investigating, identifying and prosecuting criminal acts whose severity justifies an order pursuant to art 135 par. 2a Code of Criminal Procedure." This latter provision introduced the admissibility of

Government of the *Land* of Carinthia that, with an appropriate decision, resolved itself to apply to the Constitutional Court,[64] alleging that the amendments to the national law (the *Telekommunikationsgesetz* of 2003, TKG) adopted in order to comply with the DRD, in their disposing the storage of communication data with no need of any prior suspicion, were determining a "massive interference with explicitly stated fundamental rights". In particular, the Appellant made several criticisms. First, it noted that even though the storage of the content of communications was expressly forbidden by the law, the content itself could in some cases be easily inferred by examining the other lawfully stored data. This, together with the awareness on the part of users that a system of data retention was in place, was likely to alter the communication behavior. Second, it noted that, on the one

---

the transmission of information on retained communication data, in case the same was deemed to be useful in order to investigate on the commission of serious criminal acts carrying a sentence of more than one year (or in some listed cases six months) imprisonment, acts among which a specific mention was made for "committed or planned" crimes related to terrorism. The data to be retained consisted, as required by the Directive, in phone, internet and email traffic data (with the exclusion, of the content of such a kind of communications); in particular, as to telephone traffic the providers had to retain, *inter alia*, the phone numbers of the caller and called person (including call-forwarding related data), the names and addresses of both the caller and the called, the start date and time and the duration of the communication, the type of service used (whether call or message), and in case of use mobile phones the location in which the caller and called were at the start of the communication; as to internet traffic, the relevant data were name, address, and identifier of the subscriber to whom a public IP address was assigned, the date and time of the assignment and revocation of a public IP address for an Internet access service, the calling telephone number for dial-up access and the identifier of the line over which Internet access was established; finally, for e-mail communications, the providers were to store the identifier assigned to a subscriber, the IP address of the sender and of each recipient of the e-mail, and the time of each login and logout of an user to an e-mail service, the date, time, identifier and public IP address of the subscriber. In order to do so, the providers of telecommunication services were obliged to "make available all facilities necessary for monitoring communications and for providing information on data in communications"; due to the cost of such an undertaking, the obligation to retain data was restricted to the operators of public communication networks, the private (and therefore generally smaller) ones being left out in order to keep them from being forced to bear disproportionate cost. Public security Authorities and Tribunals could access the stored data upon a court-approved order, issued by the public prosecutor's office pursuant to Article 135.2a of the Code of Criminal Procedure. Upon receiving the access request from the Court and having checked its validity, the providers had to extract the indicated data without delay, encrypt them, and transmit them to the requesting authority, making sure at the same time to store the request's log data (that is to say, to keep trace of the received request and of the actions that followed it) for a period of three years and to transmit them to the Federal Minister of Justice (that in its turn has the duty to report them to the EU Commission and the Austrian National Council), and to the Austrian Data Protection Commission and Data Protection Council (established and disciplined by Sect. 7 of the cited *Datenschutzgesetz* 2000), charged with supervising the protection of data, granting their security and monitoring the compliance to the cited provisions. To guarantee the security of the stored data, the providers had to take the appropriate technical measures to ensure that they could "be accessed only by authorized persons with due adherence to the principle of dual control"; moreover, the storage had to be performed in such a way that a distinction could in any moment be made among the different data, and that the "unlawful destruction, accidental loss or unlawful storage, processing, access and disclosure" of the same were prevented. Albeit carefully formulated, and involving society and the interested organization to construct a comprehensive system of guarantees and control over the retention of communication data, and declaredly adopting the lightest of the measures prescribed by the Directive, it nevertheless led to profound public criticism after its coming into force in April 2012.

[64] Application G 47/12.

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press

hand, the normative provisions were deprived of part of their effectiveness by the fact that they were actually easy to circumvent, through the simple use of prepaid mobile phone cards; and, on the other hand that, as a consequence, the information extrapolated from the retained data was not to be considered fully reliable. The scope of the DRD was hence not correctly fulfilled by the Austrian law, and a disproportionate sacrifice of and interference with fundamental rights was imposed. This sacrifice, the Appellant further alleged, was imposed with no certainty of a practical return, since no evaluation of the objective need (or the possible success) of the system of data retention for criminal investigations had ever been carried out. Last but not least, from an EU law perspective, the Government of Carinthia sustained that an individual right to data protection, of which the Directive and its transposition laws were clearly in breach, was to be acknowledged by the EU. For this reason, the Appellant was asking for the annulment of a list of provisions of the TKG 2003.

The second Appellant was Mr. Michael Seitlinger, an employee who had filed an individual complaint[65] under Article 140(1) of the Austrian Constitution, arguing that the unconstitutional dispositions contained in the TKG had brought about the infringement of his rights (namely Article 8 of the CFR), since the storage of his traffic data not only lacked a reasonable cause and exceeded the billing necessities, but was also against his personal will. Similarly to what was alleged by the Government of Carinthia, Mr. Seitlinger lamented that the analysis of the stored data enabled the deduction of information on "the behavior, habits and whereabouts of the users of communications services and therefore to draw up 'movement profiles.'"[66] Furthermore, since operators of non-public communications services and networks (such as corporate networks) were not subject to the obligation of storing data, there was still a chance for operators of public internet access services to allow for an anonymous use of their services; likewise, operators of public telephone services were able to offer prepaid cards without having to record user data. Therefore, the Applicant claimed the Directive was in breach of Articles 7, 8, 11, and 20 of the CFR; furthermore, he argued, the Austrian legislator was not under an obligation to implement the Directive, since the latter lacked any direct legal effects, and a primacy of application of these rules over Austrian constitutional law was not to be assumed. For these reasons, Mr. Seitlinger asked the *Verfassungsgerichtshof* to bring the issue before the CJEU, seeking a preliminary ruling according to Article 267 TFEU, in order to ascertain the validity of the Directive.

The last claim[67] was filed via a series of petitions, through which over 11,000 applicants, as subscribers of the telecommunication services interested by the data retention provisions,

[65] Application G 59/12.

[66] *Id*.

[67] Applications G 62,70, 71/12.

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press

lamented that the preventive blanket data storage, in absence of any concrete suspicion, was to be considered disproportionate (also in consideration of the lack of due remedies), and determined a violation of their rights under Articles 7 and 8 CFR and Article 1 of the *Data Protection Act*, 2000. The Applicants consequently asked for the annulment of Article 102a of the TKG 2003.

In expressing its concerns over the validity of the DRD, recognizing its doubts on the interpretation of the provisions of the CFR recalled by the Appellants, and considering the two issues of fundamental relevance for its decision on the complaints, with its sentence of 28 November 2012 the Austrian Constitutional Court decided to suspend its proceedings and submit a request for a preliminary ruling to the CJEU.[68]

The fall of the third "tile" of this complex judicial domino was determined by the initiation before the Constitutional Court of Slovenia,[69] on 5 March 2013, of a constitutionality review proceeding on the national law provisions implementing the DRD,[70] promoted by

[68] *Request of a preliminary ruling from the* Verfassungsgerichtshof *(Austria)*, Case C–594/12 of 19 December 2012.

[69] As is known, Slovenia is a parliamentary democratic republic; it became an independent State after the disintegration of Yugoslavia in 1991; on 23 December 1991, after the plebiscite on the sovereignty and independence of Slovenia of 23 December 1990, the Constitution of the Republic was adopted. Slovenia has a bicameral Parliament, composed of the National Assembly and the National Council. The Slovenian Parliament is characterized by an asymmetric duality, because the Chambers do not have equal powers. The National Assembly (*Državni zbor*) is comprised of ninety deputies, elected for a four-year term, with one representative of each of the Hungarian and Italian minorities. The National Assembly exercises legislative power, voting, and monitoring functions. The National Council (*Državni svet*) is the upper house of the Slovenian Parliament and represents social, economic, professional, and local interests. The President of the Republic is the head of State and is elected by the people for a five year term. It represents the unity of the nation and is the head of the armed forces. It is the head of government and holds the executive power with the latter. The Government consists of the President and the Ministers. As regards their responsibilities, the Government and individual Ministers are autonomous and responsible to the National Assembly. As regards the Slovenian judicial system, the unified system of courts consists of courts with general jurisdiction and courts with specialized jurisdiction; they all act in accordance with the principles of constitutionality, independence and the rule of law. Courts with general jurisdiction include forty-four district, eleven regional, four higher courts, and the Supreme Court; four labor courts and social court- that rule on labor-related and social insurance disputes- and the Administrative Court, which provides legal protection in administrative affairs and has the status of a higher court, composed the specialized courts. A special place in the justice system is held by State prosecution, as it is an independent authority, but also part of the executive branch of power. The National Assembly appoints the General State Prosecutor. The Constitutional Court represents the highest authority with regard to the protection of constitutionality, legality, human rights, and basic freedoms. The National Assembly, following nominations from the President of the Republic, appoints the judges. Nine judges are elected for a period of nine years, with no possibility of a further term. The offices of constitutional judge and judges of specialized and general courts are incompatible with other offices in state bodies. The Court judges the conformity of laws with respect to the Constitution and the conformity of laws and regulations with respect to international treaties ratified and to the principles of international law.

[70] Slovenia implemented the DRD in 2007 with regard to telephony data and in 2009 with regard to data relating to the Internet, transposing the provisions in its Act on Electronic Communications that was amended in 2012, with the new provisions entering into force in January 2013. Such a new set of norms imposed on operators the obligation to preventively retain the traffic and location data of all users (having no regard to whether the users

Slovenian Information Commissioner.[71] In his application,[72] the Commissioner requested the Court to verify the constitutionality of Articles 162 to 169 of the *Electronic Communications Act*, claiming that, besides being in breach of the principle of proportionality, their disposing the preventive retention of data evidently entailed interferences with the rights to the protection of personal data (Article 38 of the Slovenian Constitution) and communication privacy (Article 37), and consequently also with the right to freedom of movement (Article 32), the right to freedom of expression (Article 39), and with the principle of the presumption of innocence (Article 27).

Although not excluding its competence to rule on the constitutionality of laws implementing EU sources,[73] in its ordinance of 26 September 2013 the Court stated that the question of the constitutionality of the Slovenian law depended directly on the compatibility of the DRD with Articles 7 and 8 of the CFR, corresponding to Articles 37 and 38 of the Slovenian Constitution. However, as stated by the same Court of Slovenia, "on the basis of point b) of the first paragraph of Article 267 TFEU), the Court of Justice of the European Union has exclusive competence to review the validity of the Directive."[74]

The conditions to make a preliminary reference to the CJEU were therefore all recurring; however, considering that the appeals for the preliminary references raised by the Irish and Austrian Courts in relation to the Directive were already pending before it, the Slovenian Court decided to simply suspend its proceedings and await the decision of the CJEU.[75]

In this sense, the Court of Slovenia took a particularly relevant further step which was important not only in terms of the evolution of the relations between EU law and domestic

---

themselves gave the impetus for this interference with their rights) for a duration of fourteen months for data regarding publicly available telephone services and of 8 months for other kinds of data.

[71] An autonomous and independent body, instituted on 31 December 2005 on the basis of the *Information Commissioner Act* (ZInfP), entitled of the supervision over the protection of personal data and the access to public information. The Commissioner is appointed by the National Assembly at the proposal of the President of the Republic. For more references on the point, see the Commissioner's institutional website, www.ip-rs.si/?id=195.

[72] The text of the complaint can be found in Slovenian at www.ip-rs.si/fileadmin/user_upload/Pdf/ocene_ustavnosti/ZEKom__Zahteva_za_oceno_ustavnosti__data_retention_.pdf

[73] Slovenian Constitutional Court, No. U–I–113/04, Judgment of 7 February 2007, Official Gazette RS No. 16/07 and OdlUS XVI, 16; No. U–I–37/10, Judgment of 18 April 2013, Official Gazette RS No. 39/13.

[74] Full text of the ordinance available at www.us-rs.si/media/u-i-65-13.-.order.pdf.

[75] "The Constitutional Court cannot adopt a decision on the matter at issue until the CJEU, which has exclusive competence to assess the validity of the above-mentioned Directive, decides on its validity. Consequently, the Constitutional Court stayed the proceedings for the assessment of the constitutionality of the challenged provisions of the ECA-1 until the CJEU adopts a decision in the above-mentioned cases." Slovenian Constitutional Court, No. U-I-37/10.

law, but also in terms of the dialogue between Courts, both on a vertical base (CJEU—national Supreme Courts) and horizontally (as for the dialogue between Member States' Courts). This is one of the issues of greatest relevance in the context of EU law, and it is perfectly mirrored by—and also has to be connected to—another aspect. It must be underlined that the remaining two of the three recalled national Courts (the Irish and Austrian ones) not only submitted their preliminary reference requests to the CJEU in order to obtain clarification on the compatibility of the Directive with the European system of protection of rights, but also manifested their need for some guidance about the interpretation of the Treaties, in order to properly adjudicate the cases brought to their attention. The range of the interpretative questions addressed by the CJEU on this occasion encompasses several areas of EU law—but unfortunately, as it is clarified in the following, it was largely left unanswered by the CJEU—showing another shade of the dialogic approach that characterized the national courts involved in the Data Retention case.

Furthermore, the questioning of the DRD has opened an interesting confrontation on another major front. The three cases presented before the Irish, Austrian, and Slovenian Courts cast a light on the likely infringement of a wide set of fundamental rights protected both at the national and the EU level. Among them, it is possible to discern a common core of rights that have a parametrical value, and a series of "ancillary" rights that not all the Applicants and the Courts decided to call into question.

The Irish High Court was the one claiming the violation of the most rights, namely, as recalled, the right to privacy (Articles 7 CFR, 8 ECHR), to protection of personal data (Article 8 CFR), to freedom of expression (Articles 11 CFR, 10 ECHR), to free movement (enshrined in Article 21 TFEU), and to good administration (Article 41 CFR). It also questioned the infringement of the proportionality principle (Article 5(4) TEU) and referred one question about the interpretation of the Treaties.

The *Verfassungsgerichtshof*'s submission to the CJEU meanwhile showed a more "essential" approach. This Court limited its request to checking the compliance of the Directive with the rights to privacy, protection of personal data, and freedom of expression, deciding in parallel to address to the CJEU a detailed series of questions of interpretative nature.

A hybrid stance was finally that of the Slovenian Court, which, while refraining from issuing a preliminary reference to the CJEU, basically limited its interest to privacy and protection of personal data, asserting that they represented the actual core of the Data Retention case, even though it had received complaints lamenting the infringement of a wider set of rights (including those to freedom of expression, freedom of movement, and presumption of innocence).

Notwithstanding these different approaches, the three courts, in their reasoning, adopted a similar position in recognizing a predominant importance to the infringement of the rights to privacy and protection of personal data. The courts concentrated their focus and concerns on these two rights, using the alleged violation of the others as an ancillary argumentation aimed at confirming the thesis of a disproportionate sacrifice imposed by the Directive's dispositions on the exercise of fundamental rights. In other words, the three Courts highlighted how the need to balance such rights with the collective right to security (in the framework of countering terrorism) had brought about a debatable normative solution, including in terms of the application of the principle of proportionality.

The following parts of the article will therefore be devoted to an analysis of the Courts' positions on two key issues: the Directive's impact on privacy and protection of personal data (with its supposed overstretching of the contents of the principle of proportionality), and the interpretation of the Treaties.

I. Endangered Rights? The Rights to Privacy and to Protection of Personal Data as Alleged Standards for Review of the Data Retention Directive

The recent judgment of the CJEU on data retention is of crucial importance, as it recognizes that the protection of privacy plays a strategic role with respect to any other right or freedom of the person.[76]

As has already been said, the Irish High Court decided to make a reference for a preliminary ruling to the CJEU on the compatibility of the DRD with fundamental rights. The CJEU was asked to decide on the compatibility of the Directive with the right to privacy, as protected in the EU Charter and in the ECHR, and with the right to the protection of personal data, as enshrined in the EU Charter. A few months later, a similar decision was issued by the Austrian Constitutional Court, which sought a preliminary ruling on the compatibility of data retention with, among other rights, the right to privacy and the right to data protection.

With respect to the fundamental right to privacy, it is at the center of the arguments presented in the orders for a preliminary reference by the Irish High Court and the Austrian Constitutional Court. Furthermore, it can also be found in the order of the Slovenian Constitutional Court, in the more specific form of the right to privacy of communication and information.

[76] Oscar Prevosti, *Tutela della privacy come presupposto della libertà: due recenti sentenze della Corte di Giustizia dell'Unione Europea a difesa della riservatezza individuale*, 3 OSSERVATORIO COSTITUZIONALE (2014), http://www.osservatorioaic.it/.

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press

As was noted earlier, in the immediate aftermath of the entry into force of the DRD into the Austrian legal order, several complaints were filed before the *Verfassungsgerichtshof*, asking the Court to verify the constitutionality of certain provisions of the law transposing the DRD. The Court, in recognition of the similarity of the three complaints that were filed before it, decided to join the three applications together.

Before pronouncing on the complaints, and in the light of the importance of the issues raised, the Constitutional Court decided to suspend its proceedings and to submit a request for a preliminary ruling to the CJEU. It asked whether Articles 3 to 9 of the Directive were to be considered compatible with the rights to respect for private and family life (Article 7 CFR), to protection of personal data (Article 8 CFR), and to freedom of expression (Article 11 CFR). The importance of the right to protection of personal data in the Austrian legal order is strongly emphasized by the Constitutional Court in its reasoning.[77] The Federal Act on the Protection of Personal Data, in fact, establishes in Article 1 that "restrictions to the right to secrecy are admissible only to safeguard an overwhelmingly justified interest of another person, and in the case of interventions of state authorities only on the basis of the law, if necessary for the reasons set out in Art. 8 para. 2 ECHR."[78] The provision stipulates that "even in the case of permitted restrictions, any intervention with the fundamental right shall be carried out using the least intrusive of all effective methods."[79]

The Austrian Constitutional Court also underlined that the main concerns about the Directive concerned the lack of an objective cause prescribed for the retention period and the fact that the decision about the length of this period remained at the discretion of Member States.[80]

Following the Court's reasoning, concerns also derived from the scope of the retention activity "as to its conformity with the Charter of Fundamental Rights." In particular, the retention of communication data:

---

[77] The Court refers to Art. 1 of the *Datenschutzgesetz*.

[78] See the English translation of the *Verfassungsgerichtshof*'s decision at https://www.vfgh.gv.at/cms/vfghsite/attachments/1/4/5/CH0007/CMS1363699922389/vorlage_vorratsdatenspeicherung_english.pdf

[79] *Id.*

[80] "[...] concerns prevail regarding the retention of data without cause as such and the related consequences. The applicants' concerns are largely based on the high degree of intervention of data retention, and that for several reasons. First, the directive sets out a retention period ranging from six months to two years. This timeframe is to be assessed in consideration of the data volume to be stored. It is the preliminary view of the Constitutional Court that this retention period gives rise to serious concerns." *Id.* at 26.

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press

> almost exclusively affects persons who do not give cause for their data being stored. At the same time they will necessarily be subject to a higher risk, regardless of any concrete modalities of data use defined in national law, namely that the authorities will record their data, become aware of their content, inform themselves of the private behavior of such persons and then further use this data for other purposes.[81]

Furthermore, the Court emphasized the high risk of abuse that could arise from the huge number of people that could have access to the stored data, "given the multitude of telecommunication service providers which exists." These are the reasons why the Austrian Constitutional Court considered the intervention to be disproportionate, underlining the importance of the right to the protection of personal data in the Austrian legal order.

In the Irish case too, as has already been noted, the request to the Court regarded the compatibility of the DRD with the CFR, with special reference to Articles 7, 8, and 11, and also with Article 41, concerning the right to good administration. The text of the judgment contains a detailed analysis of the nature of the rights claimed by the Plaintiff. More specifically, the Plaintiff argued that the retention of data conflicted with the right to privacy, the right to family life, the right to communicate (and the right to privileged communication), and the right to travel (and the right to travel confidentially).

In its reasoning on the fundamental right to privacy, the Irish High Court showed firstly that the right to privacy can result from a number of sources; in the Irish context, as underlined in the *Kennedy v. Ireland* case,[82] "it is well established that a person has a constitutional right to privacy."[83] Given the Irish context, in which the sequence of events that led to the preliminary reference to the CJEU was developed and on which we focused earlier in this text, the Irish judge, in its reasoning, put more emphasis on the right to privacy as regards the business transactions. After stating the existence of the right to privacy in business transactions, the Court affirmed that "it is therefore clear that even though it may be accepted that there is a right to privacy in business transactions, that right may be limited by the exigencies of the common good, with the threshold for such interference being relative and being case or circumstance specific."[84] However, as pointed out in the text,

[81] *Id.* at 27.

[82] Irish High Court, *Kennedy v. Ireland* [1987] I.R. 587; [1988] I.L.R.M. 472.

[83] Irish High Court, *Digital Rights Ireland Ltd*.

[84] *Id.*

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press

given the actual nature of the corporate bodies, the mentioned right to privacy is necessarily narrower than that applicable to natural persons. The court anyway highlights that, even though companies as legal entities are to be considered as separated from their members as individuals, the interests of legal persons must as well find forms of protection by courts.

Coming to EU law, the High Court referred to Articles 7 and 8 CFR and Article 8 ECHR, along with some of the cases[85] in which the CJEU had already defined corporate privacy protection as a fundamental principle for the Community. By grounding its reasoning also on the case law of the ECtHR,[86] the Irish judge highlighted the importance of the recognition of the right to privacy in business by both Irish law and EU law, and placed privacy with regards to personal data inside the cases provided for in Article 8 CFR. This led the Court to admit the *locus standi* of the Plaintiff, alleging the interference with its right to privacy. Still arguing on the right to communicate, and recalling the *Copland v. UK*[87] case, in which "[…] the Court considers that the collection and storage of personal information relating to the applicant's telephone, as well as her e-mail and internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8",[88] the Irish judge reaffirmed that the storage of communication data, even without these being used in any way, constitutes an important interference with Article 8 ECHR, and that the retention of the data violates the right to privacy as set out in Article 8 CFR. The Judge therefore welcomed again the Plaintiff's *locus standi*, although "[…] that is not to say that such interference is not legitimately justified or that the Plaintiff would be ultimately successful in its action."[89]

As stated in the judgment, the rights whose violation was claimed and the legislation consequently called into question were to be considered "of great importance to the public at large," demonstrating the existence of a "significant element of public interest concern with regards to the retention of personal telecommunication data, and how this could affect persons' right of privacy and communication."[90]

---

[85] Joined Cases C–46/87 and C–227/88, Hoechst AG v. Commission of the European Communities, 1989 E.C.R.2859; Case 85/87 Dow Benelux NV v. Commission, 1989 E.C.R. 3137; Joined cases 97/87, 98/87 and 99/87, Dow Chemical Iberica SA v. Commission of the European Communities, 1989 E.C.R. 3165.

[86] The judge refers to Eur. Court H.R., *Niemietz v. Germany*, Judgment of 16 December 1992, Series A, No. 251–B, and Eur. Court H.R., *Société Colas Est and Others v. France*, Judgment of 16 April 2002, Reports of Judgments and Decisions, 2002–III.

[87] Eur. Court H.R., *Copland v. the United Kingdom*, Judgment of 3 April 2007, Reports of Judgments and Decisions, 2007–I.

[88] Irish High Court, *Digital Rights Ireland Ltd*.

[89] *Id.*

[90] *Id.*

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press

Finally, the importance and relevance of the right to privacy and protection of personal data also emerges in the aforementioned Slovenian case, although the Constitutional Court did not engage in an open dialogue with the CJEU. According to the Slovenian Court, the alleged unconstitutionality referred above all to the rights to communication (Article 37 of the Constitution) and information privacy (Article 38). The interference with the right to privacy was also underlined, in the opinion of the Court, by the argument that due to the interference with the recalled rights to communication and information privacy, other important rights, like the right to freedom of expression, the right to freedom of movement, and the presumption of innocence, were jeopardized. The Court stated that the protection of fundamental rights enshrined in Articles 37 and 38 of the Slovenian Constitution is equivalent to that of Articles 7 and 8 CFR and that, by consequence, it must be established whether the provisions of the DRD are consistent with these two articles of the Charter.

Pending the case before the CJEU, the position taken by the Slovenian Constitutional Court to suspend the national proceeding shows deference towards the CJEU and an explicit acknowledgment of its jurisdiction. It can also be seen as a first step towards, or a conduct anticipating, the real dialogue eventually established with the CJEU[91] on the occasion of the first preliminary reference ever sent by the Slovenian Constitutional Court on November 2014, in the case of the Commission's Banking Communication.[92]

The decision therefore shows how, within national frameworks, there is a growing awareness among judges of the necessity and importance of collaboration both among themselves and with the CJEU. This collaboration is important in ensuring the more effective functioning of the EU, especially in very sensitive subjects, such as that governed by the DRD.

The analysis thus far conducted of the Austrian, Irish, and Slovenian cases highlights how deeply the measures provided for in the DRD affect the privacy of individuals, thus in part anticipating some of the contents of the important decision of the CJEU in April 2014.

---

[91] On the theme of the deferential dialogue between Courts in the EU, see Ioana Pelin-Raducu, *Deferential dialogues between the Court of Justice and domestic courts regarding the compatibility of the EU Data Retention Directive with (higher?) national fundamental rights standards*, *available at* http://www.on-federalism.eu/index.php/component/content/article/166-deferential-dialogues-between-the-court-of-justice-and-domestic-courts-regarding-the-compatibility-of-the-eu-data-retention-directive-with-higher-national-fundamental-rights-standards (2014).

[92] Slovenian Constitutional Court, No. U–I–295/13, Judgment of 6 November 2014, Official Gazette RS No. 82/2014.

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press

II. Issues About the Interpretation of the EU Treaties

As to the interpretation of the Treaties, the requests submitted by the Irish and Austrian Courts significantly differ one from the other in terms of their nature and legal basis, but are similar in that both recall landmark principles in the evolution of EU law.

The Irish High Court focused on the role accorded by the Treaties to national courts, asking "to what extent," in the light of the principle of loyal cooperation stated in Article 4(3) TEU, such courts can be considered to be compelled to "inquire into, and assess, the compatibility of the national implementing measures for Directive 2006/24 with the protections afforded by the Charter, including Article 7 thereof (as informed by art. 8 of the ECHR)." As said, because of the entry into force of the CFR in 2009, the Charter now has a fully prescriptive nature and falls within the jurisdiction of the CJEU. Hence, from any legal point of view, the CJEU is now formally the "natural" judge entitled to watch over the respect of the EU's normative framework also when it comes to the rights protected by the CFR. At the same time, and notwithstanding this, the principle of loyal cooperation imposes on Member States the duty to "take any appropriate measure, general or particular, to ensure fulfilment of the obligations arising out of the Treaties or resulting from the acts of the institutions of the Union," facilitating "the achievement of the Union's tasks and refrain[ing] from any measure which could jeopardize the attainment of the Union's objectives." This leaves room for an ambiguous situation in which national courts seem to be bound by the Treaties to exercise a competence the Treaties themselves have (from 2009, for what concerns rights) conferred upon the CJEU. A solution to such ambiguity has been provided by the consolidation of the use of the preliminary reference procedure by national courts, which has started to establish a concrete mechanism of coordination and mutual support between national courts and the CJEU. As the latter itself has made clear in well-established case law,[93] in fact, "when requested to give a preliminary ruling, [the CJEU] must provide all the guidance as to interpretation needed in order for the national court to determine whether that legislation is compatible with the fundamental rights the observance of which the court ensures."

It is in this context that the Irish Court's reference must be considered.[94] The interpretative issue submitted to the CJEU appears to us not to be particularly significant. Although it was

[93] *See* Case C–260/89, ERT v. DEP, 1991 E.C.R. I–2925; Case C–299/95, Friedrich Kremzow v. Republik Österreich, 1997 E.C.R. I–2629; Case C–309/96, Annibaldi v. Sindaco del Comune di Guidonia and Presidente Regione Lazio, 1997 E.C.R. I–7493; Case C–94/00, Roquette Frères SA v. Directeur general de la concurrence, de la consummation et de la repression des frauds, and Commission of the European Communities, 2002 E.C.R. I–9011; Case C–349/07, Sopropé - Organizações de Calçado Lda v Fazenda Pública, 2008 E.C.R. I–10369; Case C–256/11, Murat Dereci and Others v Bundesministerium für Inneres, 2011 E.C.R. I–11315; Case C–27/11, Anton Vinkov v. Nachalnik Administrativno-nakazatelna deynost, 2012 E.C.R. 0000; and Case C–617/10, Åklagaren v. Åkerberg Fransson, 2013 E.C.R. 0000.

[94] The fact that, as said, the questions to be addressed to the CJEU were by will of the Irish High Court not defined in its May 2010 decision, but entrusted to a subsequent public consultation "deprives" us of a powerful

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press

specifically framed in the scope of the principle of loyal cooperation, apparently aiming at receiving clarifications on the implication of it on the national courts' activity, the question had substantially already been answered in general terms by the European case law. This case law confirmed over time the role of national jurisdictions in granting the respect—and, ultimately, the unity and supremacy—of EU law, and set out a series of operative reference principles for performing such an activity in the rights domain.

As to the interpretative questions submitted by the Austrian Constitutional Court, instead, it was first of all asked whether, in order to assess the permissibility of interferences, Directive 95/46/EC (on the protection of individuals with regard to the processing of personal data and on the free movement of such data)[95] and Regulation (EC) 45/2001 (on the protection of individuals with regard to the processing of personal data by the Community Institutions and bodies and on the free movement of such data)[96] were to be considered on an equal footing with the provisions of Article 8(2) and Article 52(1) of the Charter, in the light of the explanations on Article 8 CFR.

It furthermore asked what is the relation between "Union law" referred to in Article 52(3) last sentence of the Charter and the Data Protection Directive, and—given that Directive 95/46/EC and Regulation (EC) 45/2001 lay down conditions and limitations on exercising the right to data protection set out in the Charter—whether changes arising from later secondary law should be considered when interpreting Article 8 of the Charter.

In the Austrian legal order, besides, a secondary law provision (that is to say, Article 1 DSG 2000) actually guarantees the fundamental right to data protection to a wider extent than the wording of Article 8 CFR, also drawing narrower conditions for the limitation of such right. Consequently, the *Verfassungsgerichtshof* asked the CJEU to clarify whether, in consideration of Article 52(4) of the Charter, the principle of providing more extensive protection laid down in Article 53 of the Charter meant that the relevant limits for permissible restrictions by secondary law should be drawn more narrowly. In other words, it asked whether the rights recognized by national secondary legislation can take precedence over the limitations that result from the CFR when they afford a wider kind of protection than that which is granted in the CFR. In particular, the Austrian Constitutional Court observed that:

> while no one single fundamental right in the constitution of one individual Member State can set the

instrument for understanding the Court's intentions, as basically no reasoning of it is provided in the order of referral.

[95] EC Directive 95/46 of 24 October 1995, O.J. 1995 L 281/31.

[96] EC Regulation 45/2001 of 18 December 2000, O.J. 2001 L 8/1.

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press

> standard and remove the unlimited applicability of the fundamental right enshrined in the Charter (cf. SA Bot, 02/10/2012, case C-399/11, *Melloni*, para. 96 et. sequ.), if a comparative legal study of the constitutions of the Member States revealed that they provided a more extensive protection than that of the Charter of Fundamental Rights, such fact may well be relevant and compel Union courts to interpret the said guarantee as laid down in the Charter of Fundamental Rights in such a way that the fundamental rights standard of the Charter will in no case be lower than that afforded by the constitutions of the Member States.[97]

This assumption found a confirmation in Article 52(4) of the CFR, which explicitly declares that "the fundamental rights which are recognized in the Charter as they result from the constitutional traditions common to the Member States shall be interpreted in harmony with these traditions (compare also Art[icle] 6, para[graph] 3 TEU)." Not every Member State's constitution contains a separate right to data protection, the Court observed. Yet a general assumption could be made—and relying also on the case law of the Constitutional and Supreme Courts of the Member States—that there was actually room to affirm that a fundamental right to data protection was in effect a part of the constitutional traditions of the Member States, but also of human rights and fundamental freedoms within the meaning of Article 53 of the CFR, recognized by the Constitutions of the Member States.

The last question submitted by the Austrian Court was whether, considering Article 52(3) of the Charter, paragraph 5 of the Preamble, and the explanations on Article 7 of the Charter (according to which the rights guaranteed therein are the same as those laid down in Article 8 ECHR), it was possible that the case law of the ECtHR on Article 8 ECHR may influence the interpretation of Article 8 CFR. This question was aimed at clearing any doubt over the role of the jurisprudence of the ECtHR on Article 8 ECHR (that entails several rulings on data protection), and stemmed from the ambiguity in the explanations of Article 7 CFR that left some perplexities as to whether the case law on Article 8 ECHR could be referred to in interpreting Article 8 CFR.

It is evident how the issues raised by the *Verfassungsgerichtshof* touch upon a series of sensitive themes, not yet stabilized following the entry into force of the Lisbon Treaty. Also in this case, as anticipated, the CJEU did not provide an explicit answer to the complex questions raised. Nevertheless, its reasoning, in solving the doubts over the compatibility of the DRD with the CFR, provided some useful tools for addressing the issues.

---

[97] Austrian Constitutional Court (*Verfassungsgerichtshof*), Joined Cases G 47/12–11, G 59/12–10, G 62, 70, 71/12–11, Judgment of 28 November 2012, para. 50.

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press

D. The Data Retention Directive Before the Court of Justice of the European Union

It took almost two years for the CJEU to come to what has immediately been recognized as a landmark decision for the EU. Before the Grand Chamber delivered its judgment (on 8 April 2014), in December 2013 Advocate General Pedro Cruz Villalón had issued his Opinion on the joint preliminary reference requests. Notwithstanding the legitimacy of its final objective of making certain data available for the activities related to the countering of serious crime, the Advocate General affirmed that the whole DRD was to be considered incompatible with the conditions set forth by Article 52(1) CFR for the limitations to the exercise of rights and freedoms recognized by the Charter. This was mainly for three reasons.

First, in prescribing providers to collect and retain data, the Directive's content determined a serious interference with the fundamental right to privacy, since from the said data and their use one could easily reconstruct a detailed profile of each individual's private life and identity. Moreover, the risk of unlawful and privacy-detrimental abuse of such data was enhanced by the circumstances that they were not to be retained by public authorities (nor under the control of them), but by private entities, that in addition had no obligation to store them within the territory of the EU, with the consequential possibility of their subjection to different legal regimes than those set by the EU. Besides, considering the described serious interference with a fundamental right, in assigning the task of regulating access to – and use of – the collected and stored data to the Member States, the Directive failed to respect the condition that any limitation to the rights enshrined in the Charter must be provided for by law. Furthermore, the limitations to fundamental rights that were prescribed in the Directive (namely, as an effect of its imposing the storage of personal data) were not backed up by the enunciation of the fundamental principles under which the minimum guarantees for the access to data and their use should have been set. An explicit definition of those principles, the Advocate General argued, would have represented a necessary assumption by the EU of its "share of responsibility" in the regulation of such a delicate matter, as it would at least have contributed to the "definition, establishment, application and review of observance of the necessary guarantees," permitting to "assess the scope of what the interference with the fundamental rights entails in practical terms and which may, therefore, determine whether or not the interference is constitutionally acceptable."

A second main point in the Advocate General's opinion was that the Directive did not fulfill the requirements set by the principle of proportionality (as set out in both the CFR and the TEU). There was in fact no sufficient justification, Cruz Villalón declared, for the maximum data storage period being set at two years, a shorter period of one year or less being perfectly capable of guaranteeing the same results. Article 12 of the Directive, in fact, offers Member States the safeguard-possibility of extending the prescribed term in case of particular circumstances, submitting a related request to the European Commission.

Finally, and considering the complex consequences of a declaration of invalidity in the EU legislation field and, in parallel, the generally moderate approach of the Member States in implementing the Directive, that partly mitigated the serious interference of the latter with fundamental rights, the Advocate General recommended the effects of the declaration of invalidity to be suspended until the approval by the EU legislature—"within a reasonable period"—of new legislative measures aimed at addressing the identified flaws of the DRD.

Absolutely in line with the Opinion of the Advocate General was the judgment of the CJEU declaring the DRD invalid. The Court's reasoning starts with an assessment of the Directive's concrete degree of interference with Articles 7 and 8 CFR. The Court then made use of the proportionality test aimed at verifying whether any justification could be validly recognized for the derogations disposed by the Directive to the system of protection of the rights to privacy and protection of data established by the measures contained in both the CFR and the relevant EU legislation (namely, the recalled Directives 95/46 and 2002/58).[98]

As to the first of these aspects, the Court preliminarily underlined that as a general rule, and according to its own case law on the matter,[99] in order to evaluate whether the right to privacy could suffer limitations or infringements, the "sensitiveness" of the private information involved is not relevant, nor is the material occurrence of a damage or inconvenience. The threshold for the assessment of a legitimate interference is therefore relatively low, since it is sufficient to prove that a normative measure is potentially detrimental in terms of rights protection.[100] Under this preliminary condition, the CJEU considered that the Directive determines a "wide-ranging" and "particularly serious"[101] interference with the rights to privacy and protection of personal data. On the one hand, in fact, the provisions of Articles 3 and 6 of the DRD, by imposing over the providers of communication services the obligation to retain data regarding an individual's private life and communications, are so to put a limit to a person's right to private life as established by Article 7 of the Charter. Likewise the same must be said for the access of the competent national authorities to the stored data, according to Articles 4 and 8 of the Directive. Such an activity, the Court argues, has already been established as being detrimental for the right to privacy by a vast case law of the ECtHR (based on Article 8 of the Convention).[102]

---

[98] As recalled, the two Directives entailed the confidentiality of communication of traffic data and prescribed upon service providers the duty to store such data as long as they are necessary for billing purposes, and to cancel them, or at least make them anonymous, when they are no longer needed for the communication transmission.

[99] Joined Cases C–465/00, C–138/01 and C–139/01 Rechnungshof v. Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v. Österreichischer Rundfunk, 2003 E.C.R. I–4989.

[100] On the point, see also Boehm & Cole, *supra* note 5, at 30.

[101] Joined Cases C–293/12 and C–594/12, Digital Rights Ireland, Seitlinger and Others, para. 37 (Apr. 8, 2014), http://curia.europa.eu/.

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press

Furthermore, the interference of the Directive with the right to protection of personal data (Article 8 CFR) is confirmed by the Directive's rule on processing personal data.

The width and seriousness of such a twofold interference are for the Court determined by the circumstance that, knowing their data were stored and processed without their prior information and consent, individuals are likely to experience the unpleasant feeling of being subject to forms of pervasive and constant surveillance, which may adversely affect their private lives. The CJEU recalled the Advocate General's analysis on the point, based on the assumption that the huge amount of retained data, their long-term preemptive storage, and the exponential growth and diffusion of electronic communication acted altogether as potential amplifiers of the threat of profiling and scrutiny over private lives that individuals could feel.

Once it had assessed the interference with the recalled rights, the Court considered whether it could be justified in the light of two prescriptions contained in Article 52(1) CFR, that, in addition to establishing that any limitation to fundamental rights must be provided for by law, states that those limitations must also respect the essence of rights[103] and the principle of proportionality. As is well known, this principle entails that the limiting measures have to be strictly necessary, and have to genuinely meet objectives of general interest recognized by the EU or the need to protect the rights and freedoms of others.

Under the essence of rights analysis, the CJEU stated that, notwithstanding the deep interference with both the right to privacy and to protection of personal data, the Directive does not adversely affect them, respectively because it prohibits the acquisition of the content of electronic communications (as per Article 1(2)) and puts upon Member States the duty to draw a set of principles of data protection and security that providers must comply with. This allows a proper prevention, with the due technical and organizational precautions, of the accidental or unlawful destruction, loss, or alteration of the stored data. The fact that the essence of the rights at stake is not impaired by the DRD provisions does not restrain the Court from expressing concerns about the extent of their interference. Even though the Directive sets rules in order to guarantee the security of data, whose content cannot in any way be stored by providers, such rules are not able to provide an effective degree of protection against abuse, unlawful access and use, and in-

[102] The reference is to cases Eur. Court H.R., *Leander v. Sweden*, Judgment of 26 March 1987, Series A, No. 116, para. 48; Eur. Court H.R., *Rotaru v. Romania* at para. 46; Eur. Court H.R., *Weber and Saravia v. Germany*, Judgment of 29 June 2006, Reports of Judgments and Decisions 2006-XI, para. 79; *Digital Rights Ireland*, Joined cases C–293/12 and C–594/12 at para. 35.

[103] The aim underlying the "essence of rights" criterion is of preserving the "hard core" (the essence, indeed) of a fundamental right, so as to guarantee that, even when limited by a necessary measure, it is not deprived of its whole content and meaning.

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press

depth information on the content of individuals' communication, and their private lives can in any case be deduced from the lawfully stored data.[104]

The DRD is then tested to verify its pursuit of an objective of general interest. Tracing a distinction already highlighted by the Advocate General, the CJEU affirmed that beyond the formally stated objective of harmonizing Member States' legislation in the field of data retention (stated in its Article 1), the Directive is conceived to attain the broader purpose (its "material objective," in the Court's wording) of combating terrorism, since its measures are aimed at making data available for the necessary investigation, detection, and prosecution of serious crimes.[105] What is more, since the Directive aims at preventing and fighting a threatening criminal phenomenon, it is of valuable importance for the guarantee of the fundamental right to public security (Article 6 CFR). Therefore, as already confirmed by a consistent jurisprudence,[106] it basically complies with both the alternative conditions set out by the last line of Article 52, genuinely satisfying an objective of general interest recognized by the EU and protecting a fundamental right such as the one to security. The limitations imposed by the DRD on the fundamental rights recognized by Articles 7 and 8 CFR must therefore be considered as fully justifiable.

Undoubtedly, the most noteworthy part of the decision delivered by the CJEU is the one devoted to the proportionality test over the measures contained in the DRD. In fact, if the Court's analysis has so far found that such measures can be considered acceptable, completely different results come from the test, displaying the Directive's main flaws and an interesting approach of the CJEU towards the case law of the ECtHR. This is particularly relevant for the solution of the recalled collateral arguments raised by the Austrian preliminary reference request in the field of the interpretation of the Treaties.

In recalling the importance of the rights at stake, the Court reminds that whenever an interference with fundamental rights is provided, in considering factors like the nature of the involved right, the interference and its object, the margin of discretion accorded to the EU legislature may be limited, leading to stricter judicial review of the conditions set by the proportionality principle. In doing so, the Court interestingly recalls a landmark case of the

---

[104] *Digital Rights Ireland*, Joined cases C–293/12 and C–594/12 at para. 66.

[105] The relevance of such data, the Court observes, has been widely recognized as of growing importance for the activities relating to the countering of serious crime and terrorism, due to the increasing diffusion of electronic communication. The reference is to the conclusions of the Justice and Home Affairs Council of 19 December 2002, reported in recital 7 of the DRD's preamble.

[106] Cases C–402/05 P and C–415/05P, Yassin Abdullah Kadi and Al Barakaat International Foundation v. Council of the European Union and Commission of the European Communities, 2008 E.C.R. I–06351, para. 363; Joined Cases C–539/10 P and C–550/10 P, Stichting Al-Aqsa v. Council of the European Union and Kingdom of the Netherlands v. Stichting Al-Aqsa, 2012 E.C.R. 0000, para. 130; C–145/09 Land Baden-Württemberg v Panagiotis Tsakouridis, 2010 E.C.R. I-–1979, paras. 46–47.

ECtHR[107] that first stated the need for more rigid standards for judicial review in case of need to protect the right to privacy from interferences provided for by data retention legislation. As anticipated, the CJEU disregarded all the questions relating to the interpretation of the Treaties contained in the two preliminary referrals by the Irish and Austrian Courts. However, when the CJEU recalled the ECtHR's case law on Article 8 ECHR, while considering the importance of Article 7 CFR, it established an important parallel, connecting the interpretation of the CFR with the ECHR and implicitly responding to some of the interpretative issues posed by the *Verfassungsgerichtshof*.

The first part of the proportionality test is held on the appropriateness of the data retention measures for the attainment of the Directive's objectives. From this point of view, the data stored under the DRD can prove to be a "valuable tool for criminal investigation,"[108] and the fact that several material conditions (such as the existence of a series of means of circumventing the retention of data, leaving some communications systematically unmonitored) could limit the Directive's extent and effectiveness (hence allowing for anonymous communications) is not so to make its measures inappropriate; therefore, they must be considered as compliant with the appropriateness requirement.

There are extremely different considerations in order when it comes to the necessity of the Directive's provisions, which cannot in any way be solely entailed by the "utmost importance" of the purpose of fighting terrorism and preserving the right to security.[109]

This is even more important bearing in mind the particular interconnection highlighted by the CJEU between Articles 7 and 8 CFR. The Court warned that even though for sure "the protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life enshrined in Article 7 of the Charter," the existence of provisions guaranteeing the respect of Article 8

[107] Eur. Court H.R., *S. and Marper v. the United Kingdom*, Judgment of 4 December 2008, Report of Judgments and Decisions 2008-V. The case concerned the conformity of the UK national DNA database with the right to respect for private and family life enshrined in Art. 8 ECHR. The Court was called on to assess whether the retention of fingerprints and DNA data of individuals who had, for a period of their lives, been suspected of criminal offences (but not convicted for having committed the crime) was to be considered compatible with the guarantees offered by Art. 8. In keeping with an already consolidated case law, the Court deemed that the retention of fingerprints and DNA (similarly to those of any kind of data) was not consistent with the right to privacy, interestingly asserting that justifications for the retention of data in light of Art. 8 ECHR should be evaluated considering that, notwithstanding the legitimate aim of preventing crimes, whenever a "right at stake is crucial to the individual's effective enjoyment of intimate or key rights," the margin of appreciation recognized to Member States in enacting data retention legislation must be drawn narrower. On the point, see BOEHM & COLE, *supra* note 5, at 23.

[108] *Digital Rights Ireland*, Joined cases C–293/12 and C–594/12 at para. 49.

[109] The fundamental nature of these rights, and of the rights to privacy and protection of personal data, the Court seems to sustain, cannot in fact automatically lead to the prevalence of the former over the latter, it being crucial to carefully balance the scope and extent of the three rights in such a way that interferences to them are restricted to cases of strict necessity. *Id.* at para. 51.

does not inevitably determine the existence of sufficient measures of protection of Article 7. In order to comply with both, the Directive should have set a clear system of safeguards, so that the limitations to Articles 7 and 8 are balanced by due guarantees against abuse, unlawful access, and use of the stored data, and by rules on the scope and application of the limitations. As testified by the jurisprudence of the ECtHR on Article 8 ECHR that the CJEU, once again, recalls,[110] these limitations are of crucial importance when the data are subjected to automatic processing and may be exposed to the risk of unlawful access.

The review on the necessity requirement (that, as anticipated, gives fully negative results)[111] is led by the CJEU under three main themes: the scope of the interferences determined by the Directive, their limitations, and the definition of the retention period.

As to the first of the three, the CJEU points out that the Directive exceeds the principle of proportionality in the scope of its interferences, for two main reasons. On the one hand, it imposes the storage of all traffic data derived from all means of electronic communication, and from all the subscribers and registered users. This means that the interferences with fundamental rights it determines practically affect the entire population of the EU, regardless of the users' effective implication in situations "liable to give rise to criminal prosecutions,"[112] or of their being obliged by relevant national legislation to professional secrecy. It hence requires the storage of data relating to people that are by all means unsuspicious, and it substantially violates the lawfully established domain of professional secrecy, lacking prescribed specific exceptions for the recalled circumstances. Furthermore, in failing to explicitly require a relation between the data to be stored and a threat to public security, the Directive does not draw the necessary restrictions to data retention, in terms of time periods, geographical zone, and the person or group of people likely to be involved in criminal activities or "to contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences."[113]

As to the necessity of purpose limitations, the Court observes that the Directive cannot be considered compliant with EU law standards for three reasons. First of all, it does not directly provide for any limit whatsoever, and nor does it set any criteria for the limitation of access to/use of retained data by public authorities. It only makes general reference to serious crime, but it must be recalled that no definition of this is provided for in EU law, meaning that it is therefore left to Member States' law. This, in the Court's opinion, is insufficient. The lack of homogeneity stemming from the conferral on Member States of the duty to discipline in detail parts of the content of the Directive is also at the core of the

[110] Eur. Court H.R., *S. and Marper*; Eur. Court H.R., *M.K. v. France*, Judgment of 18 April 2013 (not final).

[111] *Digital Rights Ireland*, Joined cases C–293/12 and C–594/12 at para. 65

[112] *Id.* at para. 58.

[113] *Id.* at para. 59.

second argument on the basis of which the Court strikes down the poor limitations system set up by the DRD. In asking the Member States to define the procedures to be followed and the conditions to have access to retained data, the Directive only binds them to do so "in accordance with necessity and proportionality requirements." By contrast, the Directive does not prescribe them to keep the prevention, detection, and investigation of precisely defined crimes as a parameter for the restriction of such access and to use it for what is strictly necessary. This is likely to bring about the establishment of an "unacceptably extensive regime"[114] at the national level, but also entails, in our opinion, another important consequence. This is that it seriously impairs the fulfillment of the stated purpose of the Directive, that is to say the harmonization of national legislation in this matter. Thirdly, the limitations set by the DRD do not meet the necessity requirement in that they lack criteria for limiting the number of subjects having access to/permission to use the data to what is strictly necessary. Furthermore, in the Court's opinion, the Directive should have either prescribed itself or at least demanded the Member States to prescribe the access and use of data to be dependent upon the decision of a judicial organ or an independent authority, so as to have a further form of guarantee.[115]

Additionally, the definition of the retention period, for the Court, fails to meet the necessity requirements. In fact, even in this case, no mention is made in the Directive of any objective criteria to be followed for the limitation of the retention period to what is strictly necessary. The retention period is, furthermore, unlawfully indiscriminate, being generally fixed at six to twenty-four months regardless of the distinction as to the different categories of data contained in Article 5 of the Directive—a distinction that would logically imply that different kinds of data may be used for different kind of purposes, not necessarily requiring the same storage time.[116]

Having assessed the substantial failure of the DRD in the proportionality test—which would, in itself, have been largely sufficient to declare it invalid—the Court decided to address a short series of important technical flaws in the law. The CJEU held that the system set up by the DRD does not comply with the additional requirement of providing for sufficient safeguards under Article 8 CFR. Indeed, it does not put in place specific rules for the huge amount of stored data, their sensitive nature, and the risk of their unlawful seizure. Thus, it does not guarantee the effective protection of the stored data against abuse, unlawful access, and unlawful use.[117]

---

[114] BOEHM & COLE, *supra* note 5, at 38.

[115] *Digital Rights Ireland*, Joined cases C–293/12 and C–594/12 at para. 62.

[116] As said *supra* (note 63), this condition had been foreseen by the Austrian Legislature, that in implementing the Directive had in fact conjugated the retention period along with the different categories of data.

[117] Furthermore, the Court remarks, by permitting the providers to "have regard to economic considerations when determining the level of security which they apply, as regards the costs of implementing security measures" the Directive does not guarantee that the said providers respect sufficient security measures, and particularly the

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press

As a final important remark, the CJEU pointed out that the lack of a provision imposing an obligation for retention servers to be physically located within the territory of the EU substantially subtracts them to the control mechanisms prescribed by Article 8(3) CFR, that states that an independent authority should be established to oversee compliance with the requirements of protection and security of personal data. Such a compliance control, which is evidently essential for the protection of individuals in the matter of their personal data, could obviously only be performed in terms of EU law, which would logically not be applicable to services taking place outside the EU and therefore under foreign legislation.

The CJEU thus stated conclusively that the substantial exceeding of the extent of the proportionality principle, in the light of Articles 7, 8, and 52(1) of the CFR, was such as to make Directive 2006/24/EC invalid *ab initio*.

E. The Impact of the Court of Justice of the European Union's Decision on the National Level

Following the CJEU's judgment on Data Retention and the consequent annulment of the Directive, EU Member States are now facing important consequences. As has been shown in detail above, the immediate result of the Court's judgment is the invalidity of the Directive, for the Court stated that the entire directive violated the Charter and declared it invalid *ab initio*. Consequently, the original obligation to introduce regimes of data retention no longer exists, but national measures adopted to implement the DRD are still in place. As has been pointed out:

> […] the declaration of invalidity of the EU act does not have a direct impact on national law which is why it remains valid - even though possibly under the threat of being declared void on the first opportunity a court can seize - until concrete steps for amendment or revocation by the national legislatures are taken or a court rules on the validity of its applicability.[118]

As a consequence of the CJEU's ruling, Member States are no longer obliged to retain data as mandated by the DRD; they are now free to modify their national legislation on this issue, or even to annul it.[119]

---

one of the permanent erasing of data at the end of the retention period. *Digital Rights Ireland*, Joined cases C–293/12 and C–594/12s at para. 67.

[118] BOEHM & COLE, *supra* note 5, at 49.

[119] "If States do not react and change their data retention regime that were based on the now void DRD, claims before national courts and/or proceedings in front of the ECtHR (after having exhausted domestic remedies)

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press

The immediate consequence of the CJEU's ruling at EU level was the decision of the European Commission to end proceedings against EU Member States which did not transpose the Directive within the given time limits. Recently, the European Parliament legal services presented an opinion on the CJEU's ruling and its consequences, answering specific questions raised by its Committee on Civil Liberties, Justice and Home Affairs.[120]

Shortly after the CJEU's judgment, the Constitutional Courts of several Member States were called to rule on the validity of the national data retention legislation, in the light of the important statements of the CJEU in the DRD ruling. In Austria,[121] Slovenia,[122] and Romania[123] the national legislation was declared invalid by Constitutional Courts. In Poland, too, the Constitutional Court declared various provisions relating to the access and processing of the retained data by police and other authorities to be unconstitutional.[124] Finally, on 23 April 2014, after the CJEU's ruling on the DRD, the Slovak Constitutional Court suspended the effectiveness of the Slovak implementation of the Directive. This means that the Court suspended only the provisions that mandated data retention; other general provisions on access to this information are left intact.[125]

---

remain possible within the constraints of the respective national procedural laws. Individuals, NGOs as well as companies may initiate such proceedings claiming a violation of Arts. 7 and 8 CFR, 8 ECHR and the respective provisions of national constitutions. National courts confronted with such claims would then be obliged to review national data retention measures and take EU law, in particular the respective guarantees stemming from Art. 7 and 8 CFR, into account. Therefore, there is a high chance that courts of Member States will also declare the national transposing act void, as it can be seen in first proceedings (e.g. in Austria and Slovenia) on this issue." BOEHM & COLE, *supra* note 5, at 49, 57.

[120] European Parliament Opinion on the CJEU's ruling on the Data Retention Directive, https://s3.amazonaws.com/access.3cdn.net/27bd1765fade54d896_l2m6i61fe.pdf.

[121] Austrian Constitutional Court (*Verfassungsgerichtshof*), Joined cases G 47/2012–49, G 59/2012–38, G 62/2012–46, G 70/2012–40 and G 71/2012–36, Judgment of 27 June 2014.

[122] The Slovenian Constitutional Court abrogated Arts. 162–169 of the Electronic Communication Act and ordered the deletion of all the retained data. Slovenian Constitutional Court, Case U-I-65/13-19, Judgment of 3 July 2014, Official Gazette RS No. 54/2014.

[123] The Romanian Constitutional Court also declared unconstitutional, in an unanimous decision, the Romanian Data Retention Law which was introduced in 2012, after the declaration of unconstitutionality of an earlier data retention act transposing the Directive, in 2009. Romanian Constitutional Court, Decision No. 440 of 8 July 2014, Romanian Official Gazette no. 653 of 4 September 2014.

[124] Polish Constitutional Tribunal, Case K 23/11, Judgment of 30 July 2014.

[125] *See* Martin Husovec, *First European Constitutional Court suspends data retention after the decision of the Court Of Justice of EU*, *available at* https://cyberlaw.stanford.edu/blog/2014/04/first-european-constitutional-court-suspends-data-retention-after-decision-court.

More specifically, as regards the three countries analyzed in this paper, it should be stressed that, after the CJEU's decision, Ireland has not yet reacted; the Digital Rights Ireland case continues and the Irish legislation of 2011 remains in force. By contrast, Austria and Slovenia promptly reacted to the decision of the CJEU within days of each other.

Austria was the first country to respond, with the first judicial decision on this matter following the CJEU's ruling. On 27 June 2014, the Austrian Constitutional Court declared the Austrian Act implementing the Directive to be disproportionate, unconstitutional, and void. To annul the act, however, the Court referred to the guarantees of Article 8 ECHR. More specifically, the scope of the act was considered as severely interfering with the right to data protection, in particular as regards the possibility of creating profiles of individuals, the low level of control on access to data, and the security requirements. Therefore, the Austrian Court found that "the Austria telecommunications law, the Code of Criminal Procedure and the *Sicherheitspolizeigesetz* ("Security Police Law") did not contain sufficient safeguards for the retention, access, and security of the retained data."[126]

With a reasoning similar to that of the Austrian Constitutional Court, on 3 July 2014, the Slovenian Constitutional Court also abrogated the national legislation on data retention. The Constitutional Court of the Republic of Slovenia abrogated the data retention provisions of the Act on Electronic Communications (ZEKom-1) in its judgment U–I–65/13–19, following the constitutional request of the Information Commissioner, lodged in March 2013.[127]

More specifically, the Slovenian Constitutional Court abrogated ZEKom-1 Articles 162, 163, 164, 165, 166, 167, 168, and 169.[128] It also ordered that operators of electronic communications delete retained data immediately after the judgment's publication in the Official Gazette. When ruling data retention to be unconstitutional, the Slovenian Court declared data retention to be disproportionate on the basis that:

> Unselective retention of data in its major part constitutes a breach into the rights of a large proportion of population that did not provide any reason for such breaches; blanket data retention does

[126] See the openrightsgroup table on "Data retention in the EU following the CJEU ruling," https://www.openrightsgroup.org/assets/files/pdfs/reports/Data_Retention_status_EU_Dec_2014.pdf.

[127] The text of the complaint can be found in Slovenian at www.ip-rs.si/fileadmin/user_upload/Pdf/ocene_ustavnosti/ZEKom__Zahteva_za_oceno_ustavnosti__data_retention_.pdf

[128] For a complete examination of the Slovenian Constitutional Court's decision see Samo Bardutzky, *The Timing of Dialogue: Slovenian Constitutional Court and the Data Retention Directive*, *available at* http://www.verfassungsblog.de.

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press

> not provide for anonymous use of communication which is particularly important in cases where untraceable use is necessary to reach certain purposes (e.g. calling for help in mental distress); arguments for selected retention periods (8 months for internet related and 14 months for telephony related data) were not provided nor elaborated in the legislative materials; the use of retained data was not limited to serious crime.[129]

In addition to the countries mentioned above, which have permanently or partially erased the national laws on data retention as a result of the ruling of the CJEU, there are nevertheless some countries that, on the contrary, have decided to confirm the national rules on data retention. This is the case, for example, of Denmark. In Denmark, the Parliament asked the government about the lawfulness of the Danish data retention law and, on 2 June 2014, the government concluded that the national rules on data retention fully respect the proportionality requirements established in the CJEU's ruling.[130] The Swedish government also ordered a study to be carried out and, in June 2014, a group of experts appointed by the Ministry of Justice came to the conclusion that the national legislation on data retention is lawful and contains clear rules on the conditions of access to retained data. Finally, in the United Kingdom, just a few days after the CJEU's decision, a new data retention law came into force,[131] which re-enacted data retention provisions of the 2009 Data Retention Regulations that were based on the DRD, annulled in April 2014. However, the retention period established by the new Act may change subject to a maximum 12 months, instead of the previously fixed twelve months.

The rapidity and the different ways in which different Member States have reacted to the ruling of the Court highlights the importance and relevance of fundamental rights in the issue of data retention, as well as the central role of this issue in the current historical period that Europe is experiencing.

---

[129] Republic of Slovenia Information Commissioner press release, *available at* https://www.ip-rs.si/index.php?id=272&tx_ttnews[tt_news]=1256&cHash=2885f4a56e6ff9d8abc6f94da098f461.

[130] Legal analysis from the Danish Ministry of Justice, http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2014/Notat%20om%20lognings direktivet.pdf (only in Danish).

[131] *Data Retention and Investigatory Powers Act 2014* (c.27), of 17 July 2014, *available at* http://www.legislation.gov.uk.

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press

F. Conclusions

From the analysis so far conducted, two main general trends may be identified in the judicial reaction that took place in Europe after the enactment of the DRD. Both of them are tightly related, in our opinion, to the fundamental nature of the right to privacy, affected by the Directive and its transposition laws, and the need for national security, with which the first must be balanced.

A first trend regards the protection of rights in itself. Under this perspective, the DRD case has posed a milestone for the future developments of EU legislation in two key areas of recent emergence: EU anti-terrorism and security legislation and fundamental rights in the framework of new technologies. This is both true at the methodological level and at the content level. As to methodology, the CJEU has, with this case, decided a landmark case in the field of rights balancing, asserting that the importance, generality, and width of a collective fundamental right such as the one to security is in no case to be considered as allowing for measures disproportionately detrimental to other fundamental rights, such as the ones to privacy and protection of personal data. The proportionality test led by the Court, together with its findings in terms of the respect for the criterion of sufficient safeguards to ensure effective protections, have set out a relevant core for the judicial balancing of rights. At the content level, the Court's decision has opened the way for a re-discussion of the extent of rights emerging from the use of new technologies and of the potential threats to them. In this sense, some have seen in the Data Retention case the origin of an evolving thread that is leading to the gradual judicial articulation of an individual right to "IT-security."[132]

The second main trend influenced by this complex case is, as already highlighted in the introductory remarks of this article, the trend of both vertical and horizontal trans-judicial dialogue.

From a first point of view, the crucial character of the issues at stake has pushed the national courts to correctly make use of the preliminary reference tool. At the same time, the fact that the majority of national courts that ruled against the constitutionality of the transposition laws did so without making any reference to the compatibility of the Directive itself with their Constitutions shows that the principle of the supremacy of EU law (for which the validity of EU acts with respect to the EU Treaties cannot be questioned by national Courts) is being metabolized by the latter; notwithstanding this, it must be underlined that in principle such Courts, as last instance Courts, should all have exercised their duty to preliminary refer the issue to the CJEU in case of doubts about the validity of provisions mirroring the content of an EU legislative act. A significant exception in this

[132] Oreste Pollicino, *Interpretazione o manipolazione? La Corte di Giustizia definisce un nuovo diritto alla* privacy *digitale*, FEDERALISMI.IT – 3 FOCUS COMUNICAZIONI, MEDIA E NUOVE TECNOLOGIE 2, 24 (2014).

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press

sense is represented by the ruling of the Romanian Constitutional Court, which relied on the ECHR more than on EU law, and could in any case be conditioned by the relatively recent accession of Romania to the EU.

The importance of the rights and interests influenced by the Directive and the fact that those interests are shared by all the EU Member States has further stimulated the dialogue between the courts, as was shown by the choice of the Slovenian Constitutional Court to suspend the proceedings and wait for the CJEU's response to the questions referred by its Irish and Austrian counterparts, instead of joining them with its own preliminary reference.

An intensified dialogue among national Courts could possibly inaugurate a positive and useful trend in the appeal to the EU judiciary. If a constant and careful confrontation between national Courts in the matter of implementing, practicing, and enforcing EU legislation was successfully established, the number of proceedings before the CJEU (and eventually the ECtHR?) would dramatically decrease, mirrored by a more interactive and cooperative attitude of national Courts.

But another aspect in the field of horizontal trans-judicial dialogue must be highlighted, since it has experienced an important step forward from the DRD case. The case, in fact, has consolidated an already "blooming" phenomenon of communication between the CJEU and the ECtHR, with the former openly referring to the latter's case law as a valid reference for the adjudication of fundamental rights contained both in the CFR and the ECHR. The phenomenon, that had its motivation in the entry into force of the Lisbon Treaty in 2009 and in the consequent acquisition of the full legal standing for the CFR, was lately supposed to gradually lead to the EU's accession to the ECHR.[133] Such a hypothesis has been for the moment excluded by the CJEU, which on 18 December 2014 ruled out the draft accession agreement as incompatible with EU law, determining a serious standstill of the issue.[134] Whatever the future and final outcome of this yet uncertain process is, the common content of the CFR and the ECHR stays as a fact, establishing a strong and undeniable link between the two Courts of Luxembourg and Strasbourg and highlighting the need for at least an "operational" solution. It seems to us that such a solution could best be found in judicial cooperation, which appears to be the most reciprocally useful and constructive practice to follow. For the time being, at least on the part of the CJEU and notwithstanding the evolution of the accession proceedings of the EU to the ECHR system, such a practice seems to be strengthening.

[133] On the point, see, in this same issue, Francesco Cherubini, *The Relationship Between the Court of Justice of the European Union and the European Court of Human Rights in the View to the Accession.*

[134] Opinion 2/13, Draft agreement on the accession of the European Union to the European Convention for the Protection of Human Rights and Fundamental Freedoms (Dec. 18, 2014), http://curia.europa.eu/.

https://doi.org/10.1017/S2071832200021325 Published online by Cambridge University Press