The Court of Justice and the Data Retention Directive in *Digital Rights Ireland*: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection

By

Marie-Pierre Granger* and *Kristina Irion

***Reprinted from* European Law Review**
Issue 6, 2014

Sweet & Maxwell
100 Avenue Road
Swiss Cottage
London
NW3 3PF
(Law Publishers)

SWEET & MAXWELL

Analysis and Reflections

The Court of Justice and the Data Retention Directive in *Digital Rights Ireland*: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection

Marie-Pierre Granger[*]

Central European University, Budapest

Kristina Irion[**]

Central European University, Budapest; University of Amsterdam

Data protection; Data retention; Electronic communications; EU law; Fundamental rights; Ireland; Personal data; Privacy; Proportionality

Abstract

In Digital Rights Ireland*, the Court of Justice invalidated the 2006 Data Retention Directive, which required private providers to retain for a considerable period electronic communication metadata for law enforcement purposes. In this landmark ruling, the EU judiciary introduced a strict scrutiny test for EU legislative acts that interfere seriously with important rights protected by the Charter of Fundamental Rights and the European Convention on Human Rights—in this case, the rights to privacy and data protection—and applied a rigorous assessment of the proportionality of the measure under the Charter, criticising numerous aspects of the Directive. This article presents and analyses the judgment, discussing its implications for constitutional review and constitutionalism in the European Union, and the substantive and procedural constraints that it imposes on EU and national data retention schemes. It concludes by reflecting on the ruling's impact on European integration and data related policies.*

Introduction

Fast-developing information and communication technology (ICT) is radically transforming our social and professional lives. We increasingly communicate and interact with others through electronic services (mobile phones, tablets, laptops) and online social media. Furthermore, many of us are connected quasi-permanently to the World Wide Web, accessing and receiving information and services through mobile communication technology (e.g. mobile broadband). The data trail left behind is a boon for law enforcement agencies, but it may also lead to abusive interference with people's private lives. Laws and policies that tap into communication data must therefore balance security benefits with respect for fundamental rights. In *Digital Rights Ireland*,[1] the Court of Justice found that the EU legislator got this

[*] Associate Professor.

[**] Assistant Professor (on leave) and Marie Curie fellow, Institute for Information Law (IViR), respectively.

[1] *Digital Rights Ireland and Seitlinger v Minister for Communications, Marine and Natural Resources* (C-293/12 and C-594/12) [2014] E.C.R. I-238; [2014] 2 All E.R. (Comm) 1.

balance wrong when it adopted the Data Retention Directive.[2] That measure imposed intrusive mandatory data retention schemes without affording sufficient protection to the rights to privacy and data protection, protected under both the EU Charter on Fundamental Rights and the European Convention on Human Rights (ECHR).

Published commentaries on the *Digital Rights Ireland* case to date, mostly written in German by communications and data protection law specialists, are generally focused on its policy and legal implications for (domestic) data retention and other data-related schemes.[3] In this article, we take a more comprehensive approach: we comment on the development in the ruling of EU standards related to the rights to privacy and data protection, and their consequences for data retention and other data-related schemes at EU and national level; but we also reflect on the judgment's impact on inter-institutional relations and constitutional review in the European Union, and its potential bearing on the dynamics of European integration. We begin with a brief presentation of the context surrounding the adoption and implementation of the Directive, and then present the Advocate General's Opinion and the judgment of the Court. In the discussion that follows, we first comment on the EU responsibility to protect human rights, and the modalities and scope of the new strict judicial scrutiny test applicable to EU legislative measures that interfere seriously with important Charter rights. We then assess the privacy and data protection standards that the judgment established, and draw lessons for future data retention schemes and other data-related policies at both EU and national level. In conclusion, we claim, first, that the ruling has the potential to transform interactions between the EU institutions, and to contribute to a redefinition of the basis of European integration in favour of constitutionalism and human rights; and, secondly, that it contributes significantly to a global reflection on how to protect privacy in the Big Data era.

[2] Directive 2006/24 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive (Data Retention Directive) [2006] OJ L105/54.

[3] E.g in chronological order, E. Puck, "Nach dem Ungültigkeitsurteil des EuGH zur Vorratsdatenspeicherungs-Richtlinie: Wahrnehmung des Anwendungsvorranges der bereinigten Unionsrechtslage durch die Gerichte und den Rechtsschutzbeauftragten nach der stop" (2014) 2 *Zeitschrift für Verwaltung* 297; R. Busch, "Vorratsdatenspeicherung—noch nicht am Ende!" (2014) 47 *Zeitschrift für Rechtspolitik* 41; S. Simitis "Die Vorratsspeicherung—ein unverändert zweifelhaftes Privileg" (2014) 67 *Neue juristische Wochenschrift* 2158; A. Roßnagel, "Neue Maßstäbe für den Datenschutz in Europa—Folgerungen aus dem EuGH-Urteil zur Vorratsdatenspeicherung," (2014) 17 *Multimedia und Recht* 372; R. Priebe "Reform der Vorratsdatenspeicherung—strenge Maßstäbe des EuGH" (2014) 12 *Europäische Zeitschrift für Wirtschaftsrecht* 456; C.-D. Classen "Datenschutz ja—aber wie?" (2014) 4 *Europarecht* 441; W. Zankl, "EuGH für Datenzugangssperre und gegen Datenvorratsspeicherung" (2014) 2 *Ecolex* 576; P. Schmuck, "Meilenstein für die Freiheit—Aufstieg und Fall der Vorratsdatenspeicherung" (2014) 2 *Juridikum: Zeitschrift im Rechtsstaat* 148; G. Vaciago, "The Invalidation of the Data Retention Directive" (2014) 3 *Computer und Recht* 65; H. Wolff, "Anmerkung zum Urteil des Europäischen Gerichtshofs vom 8.4.2014 zur Vorratsdatenspeicherung" (2014) 14 *Die öffentliche Verwaltung* 608; J. Kühling, "Der Fall der Vorratsdatenspeicherungsrichtlinie und der Aufstieg des EuGH zum Grundrechtsgericht" (2014) 33 *Neue Zeitschrift für Verwaltungsrecht* 681; A. Spina, "Risk Regulation of Big Data: Has the Time Arrived for a Paradigm Shift in EU Data Protection Law?" (2014) 5 *European Journal of Risk Regulation* 248; W. Durner, "Nichtigkeit der RL über die Vorratsdatenspeicherung" (2014) 21 *Deutsches Verwaltungsblatt* 712; A. Cassart and J.-F. Henrotte "L'invalidation de la directive 2006/24 sur la conservation des données de communication électronique ou la chronique d'une mort annoncée" (2014) 20 *Revue de jurisprudence de Liège, Mons et Bruxelles* 954; F. Fabbrini, "Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S." (2015) 8 *Harvard Human Rights Journal* (forthcoming). Some blog posts did nonetheless address the more constitutional aspects of the ruling. See notably, S. Peers, "The Data Retention Judgment: The CJEU Prohibits Mass Surveillance" (April 8, 2014), *http://eulawanalysis.blogspot.hu/2014/04/the-data-retention-judgment-cjeu.html*; O. Linskey, "Joined cases C-293/12 and 594/12 Digital Rights Ireland: The Good, the Bad and the Ugly" (April 8, 2014), *http://europeanlawblog.eu/?p=2289#sthash.Ju0PiCyJ.dpufhttp://europeanlawblog.eu/?s=digital* [Both accessed October 20, 2014].

Data protection and data retention in the European Union—controversies around "Big Brother" policies

Data retention consists in the collection of traffic and location data (metadata), initially without the need for suspicion of crime or judicial intervention, for subsequent use for law enforcement purposes. It differs from the interception of communications content (eavesdropping) or data preservation, whereby authorities request operators to keep the data of specific individuals suspected of crime ("quick freeze").[4] Technical and economic constraints that previously restricted the collection and processing of information have almost disappeared, and data retention is increasingly used in the fight against crime. However, these practices can impinge on fundamental rights. In this first part of our case comment, we introduce the relevant rights framework and its confrontation with the rise of data retention, which led to the adoption and implementation of the Data Retention Directive and its challenge before the Court of Justice.

The Court has long recognised the existence of general principles of Union law protecting fundamental rights, inspired by the common constitutional traditions of the Member States and by the ECHR.[5] These general principles are now consolidated in the Charter of Fundamental Rights, which became legally binding with the coming into force of the Lisbon Treaty in 2009 (art.6(1) TEU) and is applicable to all measures adopted by EU institutions and to Member States when they implement EU law (art.51(1) CFR). Charter rights that correspond to those guaranteed by the ECHR must be interpreted in conformity with the meaning and scope of the rights laid down by the Convention (art.52(3) CFR); this requirement is reinforced by the prospect of EU accession to the ECHR (art.6(2) TEU). Article 8 ECHR protects the right to private and family life, which the European Court of Human Rights (ECtHR) has interpreted as including the right to data protection, and has already applied to national data retention schemes.[6]Article 7 CFR, on the right to respect for private and family life, home and communication, mirrors art.8 ECHR, with the result that the ECtHR case law provides guidance for the development of the EU rights of privacy and data protection. In addition, art.8(1) CFR recognises explicitly an autonomous and specific right to the protection of personal data, which requires that personal data "[m]ust be processed fairly for specified purposes and on the basis of the consent of the person concerned or other legitimate basis laid down by law …" and that compliance should be monitored by an "independent authority".

These constitutional principles are substantiated by EU legislative instruments, adopted to facilitate the cross-border flow of personal data and to protect the rights to privacy and personal data. In 1995, the Data Protection Directive established a protective framework, while nonetheless allowing Member States to adopt derogating measures necessary to safeguard fundamental interests such as national security, defence, public security or law enforcement (art.13(1) of the Data Protection Directive).[7] In 2002, the ePrivacy Directive was introduced as *lex specialis* in the electronic communications sector.[8] It required the

[4] See E. Guild and S. Carrera, "The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive", CEPS Liberty and Security in Europe Papers No.65 (May 29, 2014), *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2445901* [Accessed October 20, 2014].

[5] See *Stauder v City of Ulm* (29/69) [1969] E.C.R. 419; [1970] C.M.L.R. 112; *J. Nold, Kohlen- und Baustoffgroßhandlung v Commission of the European Communities* (4/73) [1974] E.C.R. 491; [1974] 2 C.M.L.R. 338; and *Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel* (11/70) [1970] E.C.R. 1125; [1972] C.M.L.R. 255.

[6] See, in particular, *S and Marper* (2009) 48 E.H.R.R. 50 ECtHR; and *M.K. v France* (2013) ECHR 341. For a discussion of relevant ECtHR cases, see the study by F. Boehm, and M. Cole, "Data Retention after the Judgement of the Court of Justice of the European Union" (Munster/Luxembourg: June 30, 2014), *http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf* [Accessed October 20, 2014].

[7] Directive 95/46 on the protection of individuals with regard to processing of personal data and on the free movement of such data (Data Protection Directive) [1995] OJ L281/31.

[8] Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive) [2002] OJ L201/37.

confidentiality of electronic communications and related traffic data, but allowed Member States to adopt data retention measures for a limited period if these were "necessary, appropriate and proportionate measures within a democratic society" (art.15(1)).

At the time, Member States had divergent norms and practices related to data retention, and could not agree on a common data retention framework.[9] After the terrorist attacks in Madrid (2004) and London (2005), however, European governments became eager to step up their surveillance mechanisms, including data retention, in order to fight more effectively against terrorism and organised crime.[10] In April 2004, a group of Member States—France, the United Kingdom, Sweden and Ireland—called for the adoption of a wide-ranging Framework Decision under the intergovernmental Third Pillar. It would have harmonised rules concerning the retention of, access to, and exchange of communications data for law enforcement purposes. Following advice from the Legal Services of the Council and the Commission that the measure could not be validly adopted under the Third Pillar,[11] the Commission prepared an alternative proposal for a Directive, which *only* sought to harmonise rules imposing data retention obligations on private providers. This way, it could be based on the Treaty provisions related to the internal market (ex art.95 EC, now art.114 TFEU).[12] The European Parliament, which had opposed the Framework Decision on human rights grounds, nonetheless backed the proposal for a Directive.[13]

In 2006, in record time, the Council and Parliament adopted the Data Retention Directive under the Community co-decision procedure and by qualified majority. The Directive created an extensive derogation scheme to the pre-existing EU data protection framework. It required Member States to adopt measures obliging electronic communications providers to retain all traffic and location data from landline, mobile and internet communications, for a period of not less than six months and up to two years. It thus replaced the prior *option* with an *obligation* to set up mandatory data retention schemes, for the data to be accessed later and used by law enforcement agencies (and possibly intelligence services) for the detection, investigation and prosecution of serious crime.[14] The Directive did not, however, regulate the use, access and exchange of the retained data.

Ireland, which had voted against the Directive, brought an action for the measure's annulment, arguing that it had been adopted on the wrong legal basis (*Ireland v Parliament and Council*).[15] The Court of Justice disagreed. Since the Directive only regulated the activities of electronic communications providers, and did not deal with access or exchange of data by State authorities, it did not affect matters related to

[9] In 2004, 15 Member States did not have laws requiring data retention. Where such laws existed, in half of the cases, there were no implementing measures. In the other half, the scope and periods of retention were highly disparate. See European Commission, Data Retention Directive, MEMO/05/328.

[10] See The Hague Programme on strengthening freedom, security and justice in the European Union [2005] OJ C53/1; European Council Declaration on combating terrorism, 7906/04 JAI, 100; European Council Presidency Conclusions of June 16 and 17, 10255/1/05 REV 1, 5, etc.

[11] "EU: Data Retention proposal partly illegal, say Council and Commission lawyers" (April 2005), Statewatch News Online, *http://www.statewatch.org/news/2005/apr/02eu-data-retention.htm* [Accessed October 21, 2014].

[12] See Commission Staff Working Paper, "Projet de décision-cadre sur la conservation des données—Analyse juridique" SEC(2005) 420, p.2.

[13] See European Parliament Legislative Resolution on the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism (8958/2004 — C6-0198/2004–2004/0813(CNS); European Parliament Legislative Resolution on the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (C6-0293/2005 — 2005/0182(COD)).

[14] See Guild and Carrera, "The Political and Judicial Life of Metadata" (May 29, 2014), *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2445901* [Accessed October 20, 2014].

[15] *Ireland v Parliament and Council* (C-301/06) [2009] E.C.R. I-593; [2009] 2 C.M.L.R. 37.

policy and judicial co-operation in criminal matters, and had thus been validly adopted on the internal market legal basis.

Four years after the transposition deadline had passed, three of the Member States (Sweden, Austria, Belgium) still had not fully transposed the Directive.[16] Moreover, 16 of them had relied on art.15(3) of the Directive to postpone the retention of data related to internet access, telephony and email.[17] Legal challenges poured into national courts, and led throughout the Union to a series of judgments by Member States' highest administrative and constitutional courts annulling provisions from national transposition acts.[18] The European Commission nonetheless pursued infringement proceedings (art.258 TFEU) against Member States that had failed to transpose the Directive properly.[19] Eventually, citizens, civil society organisations and national courts resorted to the indirect preliminary reference route (art.267 TFEU) to seek the invalidation of the "mother" instrument on human rights grounds.

Digital Rights Ireland—facts and procedure

Digital Rights Ireland, a private organisation dedicated to the protection of human rights in a digital age (C-293/12), and an Austrian regional government (Carinthia), together with more than 11,000 other applicants (C-594/12) had challenged national transposition measures on the grounds of constitutional incompatibility and violation of EU law before, respectively, the High Court of Ireland and the Austrian Constitutional Court. These courts referred to the Court of Justice questions essentially concerning the validity of the Data Retention Directive, in light of the EU proportionality requirement, the Charter, and existing EU legislation on data protection.[20]

The process leading to the final judicial decision was unusually participatory.[21] The Commission, Council, European Parliament, eight Member State governments, and the Irish Human Rights Commissioner submitted written observations,[22] and most also participated in the joint hearing. The Court of Justice requested the opinion of the European Data Protection Supervisor (EDPS) and addressed written questions to intervening parties.

The Advocate General's Opinion

Advocate General Cruz Villalón called for the invalidation of the Directive on the grounds of its incompatibility with art.7 CFR (right to privacy).[23] Approaching the case from a "constitutional"

[16] See European Commission, *Evaluation Report on the Data Retention Directive ((Directive 2006/24)* COM(2011) 225.

[17] See related declarations annexed to the publication of Directive 2006/24 in OJ [2006] L105/61.

[18] E.g. in Bulgaria, Germany, Czech Republic, Cyprus, and Romania. For references and details, see C. Jones and B. Hayes (Statewatch), "The EU Data Retention Directive: A Case Study in the Legitimacy and Effectiveness of EU Counter-terrorism Policy" (2013), *http://www.statewatch.org/news/2013/dec/secile-data-retention-directive-in-europe-a-case-study.pdf* [Accessed October 21, 2014]; E. Kosta, "The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection", (2013) 10 *SCRIPTed* 339, *http://script-ed.org/?p=1163* [Accessed October 21, 2014].

[19] Germany and Romania were criticised for their failure to replace laws after their respective national constitutional courts invalidated the first national implementation laws. As for Sweden, it was fined €3 million. See European Commission, "Data retention: Commission requests Germany and Romania fully transpose EU rules" (2001) IP/11/1248.

[20] The Irish High Court also asked whether the principle of loyal co-operation (art.4(3) TEU) required national courts to assess the compatibility of the Directive's national transposition measures with the Charter.

[21] "'As large a charter as the wind'? ECJ to hold hearing in data retention cases, focusing on Charter of Fundamental Rights", Content and Carrier (2013), *http://www.contentandcarrier.eu/?p=435* [Accessed October 21, 2014].

[22] The Governments of Ireland, Austria, Spain, France, Italy, Poland, Portugal and the United Kingdom.

[23] Opinion of A.G. Cruz Villalón in *Digital Rights Ireland* (C-293/12) [2013] E.C.R. I-845.

perspective,[24] he proposed to examine, first, the *general proportionality* of the Directive in terms of the overall appropriateness of the means deployed by the measure to achieve its stated objectives (art.5(4) TEU); and, secondly, its *compatibility with the Charter*, and, in particular, that instrument's proportionality clause (art.52(1) CFR).

At pains to reconcile the Court's prior legal basis ruling with his own conclusion, the Advocate General emphasised the "functional duality" of the Directive, as both an internal market harmonisation directive and an instrument imposing data collection and retention for law enforcement purposes.[25] This second effect triggered, in his view, a corresponding responsibility of the EU legislator to adopt effective guarantees to protect fundamental rights.[26] For the Advocate General, what "required the utmost vigilance" was not the processing of the data retained, but the collection and retention of the data, and their impact on the right to privacy.[27] Even though he agreed that arts 7 (privacy) and 8 (data protection) of the Charter were undeniably closely linked, he called for a *differentiated treatment*,[28] as also advocated by the EDPS.[29] The Advocate General then focused his analysis on the Directive's interference with the right to privacy.

He started by referring to ECtHR case law,[30] which treated the mere storing by a public authority of data relating to the private life of an individual as an interference with art.8 ECHR (respect for his private life). He considered that the Directive's interference with the right to privacy of EU citizens was a "particularly serious" one,[31] because of the length and scale of data collection, the mapping and profiling potentials of metadata, and the risk of unlawful use of the data.[32] The Advocate General then evaluated the Directive's proportionality under, first, art.5(4) TEU and, secondly, art.52(1) CFR, as both tests were, in his view, of a "different nature".[33]

Under the general proportionality test (art.5(4) TEU), A.G. Cruz Villalón took the view that the "intensity of judicial review" must be commensurate with the discretion available to the EU legislator. He found that, in the case at hand, "the intensity of the intervention in the area of regulation of fundamental rights" was "manifestly disproportionate" to the internal market objective.[34] Highlighting the paradox according to which "the reason for [the Directive's] legitimacy in terms of legal basis would … be the reasons for its illegitimacy in terms of proportionality",[35] he refrained from testing it against the "real" security objective, and proceeded, instead, to examine its compatibility with the Charter.

Applying traditional human rights reasoning reproduced in art.52(1) of the Charter, the Advocate General verified whether the interference was *provided by law*, *respected the essence* of the right to privacy, and *was proportionate*, that is, *necessary* and *genuinely* meeting *legitimate general interests objectives* or the *rights of others*. On the first element, the "quality of law" dimension, he harshly criticised the irresponsible behaviour of the EU legislator:

> "The EU legislature [could] not when adopting an act imposing obligations which constitutes serious interference with the fundamental rights of citizens of the Union, entirely leave to the Member States

[24] Opinion of A.G. Cruz Villalón in *Digital Rights Ireland* (C-293/12) [2013] E.C.R. I-845 at [1].
[25] Opinion in *Digital Rights Ireland* (C-293/12) at [46].
[26] Opinion in *Digital Rights Ireland* (C-293/12) at [117], [123].
[27] Opinion in *Digital Rights Ireland* (C-293/12) at [59].
[28] Opinion in *Digital Rights Ireland* (C-293/12) at [61].
[29] EDPS, *Public hearing in Joint Cases C-239/12 and C-594/12 (9 July 2013): Pleading of the EDPS*, *https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Court/2013/13-07-09_Pleading_notes_Joint_Cases_C-23912_and_C-59412_EN.pdf* [Accessed October 21, 2014].
[30] *Amann v Switzerland* (2000) 30 E.H.R.R. 843 ECtHR.
[31] Opinion in *Digital Rights Ireland* (C-293/12) at [70].
[32] Opinion in *Digital Rights Ireland* (C-293/12) at [71]–[76].
[33] Opinion in *Digital Rights Ireland* (C-293/12) at [89].
[34] Opinion in *Digital Rights Ireland* (C-293/12) at [102].
[35] Opinion in *Digital Rights Ireland* (C-293/12) at [102].

> the task of defining the guarantees capable of justifying that interference … It must … fully assume its share of responsibility … .”[36]

In his view, neither competence limitations nor the fact that many Member States had provided suitable safeguards[37] could absolve the EU legislator from its responsibility to secure guarantees “at least in the form of principles”.[38] This deficiency would already justify the annulment of the Directive.[39]

The Advocate General nonetheless also examined the proportionality of the interference with the right to privacy under art.52(1) CFR. While he found that the Directive pursued a legitimate objective (the fight against crime), and that data retention was generally appropriate for that purpose, he was clearly sceptical about the suitability of the indiscriminate and long data retention period. He felt that retention periods that were “measured in years” rather than months belonged to “historical time” and “memory life”[40] and were unnecessary “in the absence of exceptional circumstances”.[41]

He consequently proposed that the Directive be declared invalid, but recommended limiting the temporal effect of the ruling. He believed that such a compromise was appropriate since most Member States had offered appropriate guarantees and imposed moderate data retention periods.

Ruling of the Court

The Court of Justice, sitting as the Grand Chamber, also concluded that the Directive was invalid. It took cues from the Advocate General as to the delicate nature of assessing the general proportionality of the measure in light of its contested real purpose. At odds with the judgment in *Ireland v Council and Parliament*, the Court declared without further explanation that the “main objective” of the Directive was to harmonise data retention regimes “in order to ensure that the data [was] available for the purpose of the prevention, investigation, detection and prosecution of serious crime”.[42]

The Court of Justice agreed that the Directive “allow[ed] very precise conclusions to be drawn concerning the private lives of the persons whose data had been retained”,[43] which could impact on freedom of expression,[44] but considered that the measure “directly and specifically” affected the right to private life (art.7 CFR) *and* the protection of personal data (art.8 CFR). In tune with their Strasbourg colleagues, the Luxembourg judges established that the Directive’s data retention obligation (arts 3 and 6) constituted “in itself an interference” with the right to privacy, and that its rules related to access to the data (arts 4 and 8) represented a “further” interference with this right.[45] Furthermore, the Court took as given that the Directive, in that it provided for the processing of personal data, interfered with the right to the protection of personal data.[46] Without detailed reasoning, it qualified these interferences as “wide-ranging” and “particularly serious”, and “likely to generate in the minds of the persons concerned [everyone] the feeling that their private lives are the subject of constant surveillance”.[47]

[36] Opinion in *Digital Rights Ireland* (C-293/12) at [120].
[37] Opinion in *Digital Rights Ireland* (C-293/12) at [132].
[38] Opinion in *Digital Rights Ireland* (C-293/12) at [124].
[39] Opinion in *Digital Rights Ireland* (C-293/12) at [131].
[40] Opinion in *Digital Rights Ireland* (C-293/12) at [148].
[41] Opinion in *Digital Rights Ireland* (C-293/12) at [151].
[42] *Digital Rights Ireland* (C-293/12) at [24]. Only later in its reasoning (at [41]) did the Court acknowledge the Directive’s functional duality.
[43] *Digital Rights Ireland* (C-293/12) at [27].
[44] *Digital Rights Ireland* (C-293/12) at [28].
[45] *Digital Rights Ireland* (C-293/12) at [34], [35].
[46] *Digital Rights Ireland* (C-293/12) at [36].
[47] *Digital Rights Ireland* (C-293/12) at [37].

The Court then analysed the legality of the Directive's interference with the rights to privacy and data protection under art.52(1) CFR (at [38]). It entirely skipped the first leg of the test ("quality of law") on which the Advocate General had elaborated at length. The Court also quickly resolved that the Directive respected the "*essence*" of the right to privacy, since it did not concern the content of communications,[48] and that of the right to the protection of personal data, since it imposed respect for certain principles of data protection and data security (at [40]). The Court recognised that the fight against terrorism and serious crime, in that it contributed to security, was a legitimate objective of general interest (at [41], [42]) and thus that data retention "genuinely satisfie[d] an objective of general interest" (at [44]).

The Court then carried out a thorough proportionality analysis, based on information it gleaned from the answers of intervening parties to its questions. Starting with references to its own previous case law, in which it had examined whether measures "d[id] not exceed the limits of what is appropriate and necessary in order to achieve those objectives",[49] it then turned to Strasbourg for inspiration in determining the scope of discretion enjoyed by the EU legislator when fundamental rights are at stake. In a strong statement of principle, it declared that:

> "When *interferences with fundamental rights* are at issue, *the extent of the EU legislature's discretion may prove to be limited*, depending on a number of *factors*, including, in particular the *area* concerned, the *nature of the right* at issue guaranteed by the Charter, the *nature and seriousness of the interference* and the *object* pursued by the interference."[50]

Following closely the reasoning of the ECtHR in *S and Marper*, the Court considered that, in the case at hand,

> "in view of the *important role* played by the protection of personal data in the light of the fundamental right to respect for private life and *the extent and seriousness of the interference* with that right caused by the [Directive], *the EU legislature's discretion* [was] *reduced*, with the result that *review* of that discretion should be *strict*."[51]

The Court then tiptoed carefully around the questions of the actual effectiveness and purpose of data retention. It repeated that data retention was a "valuable tool", "appropriate" to achieve the security objective,[52] even if the Directive did not cover every possible means of electronic communication.[53] It also agreed that the fight against organised crime and terrorism was "of the utmost importance in order to ensure public security" and that it needed to rely on "modern investigation techniques".[54] However, the Court, like the Advocate General, took issue with the particular restrictions imposed by the Directive,[55] which were not limited to what was "strictly necessary".[56]

Inspired again by ECtHR case law, the Court of Justice stated that EU legislation that imposes serious interference with rights such as the respect for private life,

> "must lay down *clear and precise rules* governing the scope and application of the measure in question and imposing *minimum safeguards* so the person whose data have been retained have *sufficient*

[48] *Digital Rights Ireland* (C-293/12) at [39].
[49] *Digital Rights Ireland* (C-293/12) at [46].
[50] *Digital Rights Ireland* (C-293/12) at [47] (emphasis added).
[51] *Digital Rights Ireland* (C-293/12) at [48] (emphasis added).
[52] *Digital Rights Ireland* (C-293/12) at [43], [49].
[53] *Digital Rights Ireland* (C-293/12) at [50].
[54] *Digital Rights Ireland* (C-293/12) at [51].
[55] *Digital Rights Ireland* (C-293/12) at [61].
[56] *Digital Rights Ireland* (C-293/12) at [52].

> *guarantees* to effectively protect their personal data against the risk of abuse and against unlawful access and use of that data."[57]

The Court found the Directive's "blanket approach", the absence of EU-set limits on access to and use of the data (or of objective criteria to define such limits), and the long and indiscriminate period of retention imposed by the European Union to be particularly problematic. First, given "widespread" and "growing" use of electronic communication, the EU-imposed data retention scheme interfered with the fundamental rights of "practically the entire European population".[58] It applied indiscriminately to "all persons and all means of electronic communications as well as traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime".[59] It did not require any link between the persons whose communications data was retained and specific security threats.[60] It also failed to protect professional secrecy.[61]

Secondly, the Court of Justice found that the Directive failed to set limits and impose objective criteria concerning access to data by competent national authorities and subsequent use for law enforcement. Notably, it lacked "substantive and procedural conditions" concerning access to and use of the data by national authorities, when these should be "strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions".[62] It lacked a definition of "serious crime",[63] and did not set out any "objective criterion" to guarantee that "the number of persons authorised to access and subsequently use the data retained [be] limited to what is strictly necessary".[64] Moreover, it did not subject access to the data to prior review by a court or an independent administrative body.[65] Finally, it imposed long data retention periods without differentiation based on security purpose, and without objective justification.[66]

The Court thus concluded that the Directive,

> "entail[ed] a *wide-ranging and particularly serious interference with the fundamental rights* enshrined in … the Charter, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary."[67]

The Court also found serious problems with the Directive's rules related to security and the protection of data by private operators or providers, which were not "specific and adapted to the vast quantity of data" retained, their "sensitive nature" and "risks of unlawful access".[68] EU legislative instruments did not ensure a high enough level of protection and security, especially as commercial actors could take account of financial considerations in determining the security level.[69] Moreover, the Directive did not require that the data be stored in the European Union, therefore running the risk that no independent authority would have control over the use and access of these data, when "[s]uch a control, to be carried out on the basis

[57] *Digital Rights Ireland* (C-293/12) at [54] (emphasis added).
[58] *Digital Rights Ireland* (C-293/12) at [56].
[59] *Digital Rights Ireland* (C-293/12) at [57].
[60] *Digital Rights Ireland* (C-293/12) at [58]–[59].
[61] *Digital Rights Ireland* (C-293/12) at [58].
[62] *Digital Rights Ireland* (C-293/12) at [61].
[63] *Digital Rights Ireland* (C-293/12) at [60].
[64] *Digital Rights Ireland* (C-293/12) at [62].
[65] *Digital Rights Ireland* (C-293/12) at [62].
[66] *Digital Rights Ireland* (C-293/12) at [65].
[67] *Digital Rights Ireland* (C-293/12) at [65].
[68] *Digital Rights Ireland* (C-293/12) at [66].
[69] *Digital Rights Ireland* (C-293/12) at [67].

of EU law, [was] an essential component of the protection of individuals with regard to the processing of personal data".[70]

The Court logically concluded, therefore, that the EU legislature "exceeded the limit imposed by compliance with the principle of proportionality in light of Article 7, 8 and 52(1) of the Charter"[71] and, without dealing with the other questions raised, declared the Directive to be invalid, without temporal restrictions. The Directive is thus considered as having never existed.

Comment

Digital Rights Ireland is set to become a landmark case. It further develops the parameters of constitutional review when fundamental rights are at stake. In particular, the judgment assigns to the European Union a *new responsibility to protect human rights* and establishes a *strict scrutiny test* applicable to EU legislative measures that interfere seriously with human rights; it also applies *rigorous proportionality testing under the Charter*. Furthermore, the ruling clarifies the contours of *privacy and data protection* in the European Union, and gives instructions to the legislator in the design of data retention schemes that are respectful of human rights. These issues will now be explored in more detail in the discussion that follows.

Towards a responsibility to protect human rights

In spite of the European Union's longstanding commitment to the protection of human rights, enshrined in the Treaty since the Single European Act (now arts 2 and 6 TFEU), this pledge did not, until recently, significantly restrain EU activities.[72] The Court of Justice reviewed EU administrative and regulatory measures with increasing vigour in light of their compliance with general principles for the protection of human rights, notably in competition and staff cases,[73] but was reluctant to subject EU legislative acts to strict fundamental rights review and annul them.[74] This is, however, slowly changing since the advent of the Charter as a legally binding document of constitutional status in 2009.

The EU political institutions have developed mechanisms to secure compliance with the Charter in various areas of activities, including in legislative drafting.[75] The Court also stepped up its judicial control over respect for fundamental rights by the EU legislator. For example, in the *Kadi* cases,[76] to which the Court refers in the *Digital Rights Ireland* ruling, and other cases dealing with EU counter-terrorist measures,[77] the Court of Justice reviewed—and, where needed, annulled—EU decisions and regulations

[70] *Digital Rights Ireland* (C-293/12) at [70].

[71] *Digital Rights Ireland* (C-293/12) at [69].

[72] For critical assessment, see A. Williams, *EU Human Rights Policies: A Study in Irony* (Oxford: Oxford University Press, 2004).

[73] For a review of these cases, see P. Craig and G. de Búrca, *EU Law: Texts, Cases and Materials* (Oxford: Oxford University Press, 2011), pp.378–380.

[74] J. Coppell and A. O'Neill, "The European Court of Justice: Taking Rights Seriously" (1992) 29 C.M.L. Rev. 669; M.-P. Granger, "The Court of Justice's Dilemma—between 'More Europe' and 'Constitutional Mediation'" in C. Bickerton, D. Hodson and U. Puetter (eds), *New Intergovernmentalism: States, Supranational Actors, and European Politics in the Post-Maastricht Era* (Oxford: Oxford University Press, forthcoming).

[75] For a critical assessment of these initiatives, see I. de Jesús Butler, "Ensuring Compliance with the Charter of Fundamental Rights in Legislative Drafting: The Practice of the European Commission" (2012) 37 E.L. Rev. 397.

[76] *P and Al Barakaat International Foundation v Council and Commission* (C-402/05 P and C-415/05) [2008] E.C.R. I-6351; [2008] 3 C.M.L.R. 41; *Commission and Council v Kadi* (C-584/10 P, C-593/10 P, and C-595/10 P) [2013] E.C.R. I-518; [2014] 1 C.M.L.R. 24. The Court's scrutiny may, however, have been triggered less by a concern for human rights than for the autonomy of EU law.

[77] For a listing of these cases, see Craig and De Búrca, *EU Law: Texts, Cases and Materials* (2011), p.374.

for violation of fundamental rights protected by EU law, such as due process or the right to property.[78] Still, until *Digital Rights Ireland*, with few exceptions,[79] the Court had been overall deferential towards EU framework laws, even when directives and framework decisions left room for serious interference with human rights.[80] Its usual technique was to "pass" these laws and then to instruct the Member States to use their discretionary powers to implement the measure in a manner compatible with EU human rights standards. In contrast, in *Digital Rights Ireland*, the Court of Justice shifts the responsibility to protect human rights onto the EU legislator. When EU legislative acts themselves impose serious interference with human rights, they must, simultaneously, provide for necessary safeguards, expressed in a clear and precise way, to prevent the interference from going beyond what is strictly necessary. If taken up by the EU legislator, this instruction could result in more human rights-loaded EU legislation, which would, incidentally, increase the scope and legitimacy of the Court of Justice's monitoring of corresponding national measures for human rights violations.

The new legal weight of the Charter and the nearing prospect of accession to the ECHR certainly contributed to the Court's calling on the EU institutions to assume greater responsibility for ensuring compliance with human rights standards. The timing of the shift may, however, be explained by the Snowden revelations, which exposed the scale of electronic surveillance carried out by governmental agencies on both sides of the Atlantic and cast doubts as to the ability of national authorities to afford sufficient guarantees to basic rights.[81] It may also be read as a response to mounting concerns concerning the respect for human rights in some Member States, notably Hungary,[82] and a judicial contribution to the development of mechanisms aimed at better securing respect for the core principles and values on which the European Union is based.[83]

Legislative discretion and judicial control in the European Union—the uncertain scope of the new "strict scrutiny" test

In *Digital Rights Ireland*, the Court of Justice places EU institutions on a shorter leash when they meddle with fundamental rights. The level of discretion accorded to the EU legislator, and the ensuing intensity of judicial control, depend on the area concerned, the nature of the Charter right at issue, the nature and seriousness of the interference, and the objective pursued.[84]

[78] The Court also invalidated provisions of EU regulations that were contrary to the right to data protection and the right to privacy protected under the Charter and the ECHR in *Volker und Markus Schecke GbR v Land Hessen* (C-92 and 93/09) [2010] E.C.R. I-662; [2012] All E.R. (EC) 127.

[79] E.g. *Test-Achats*, in which the Court invalidated a provision of a Directive that enabled Member States to allow insurance companies to derogate from the principle of non-discrimination based on sex. See *Association Belge des Consommateurs Test-Achats ASBL, Yann van Vugt, Charles Basselier v Conseil des ministres* (C-236/09) [2011] E.C.R. I-773; [2011] 2 C.M.L.R. 38.

[80] E.g. inter alia, *Booker v Aquacultur Ltd and Hydro Seafood GSP v The Scottish Ministers (Fish Disease Control Directive)* (C-20 and 64/00) [2003] E.C.R. I-7411; *Netherlands v Council and Parliament (Biotechnology Directive)* (C-377/98) [2001] E.C.R. I-7079; [2001] 3 C.M.L.R. 49; *Advocateen voor de Wereld VZW v Ledeb van Ministeraad (European Arrest Warrant)* (C-303/05) [2007] E.C.R. I-3633; [2007] 3 C.M.L.R. 1; *Parliament v Council (Family Reunification Directive)* (C-540/03) [2006] E.C.R. I-5769; [2006] 3 C.M.L.R. 28.

[81] D. Bigo, S. Carrera, N. Hernanz, J. Jeandesboz, J. Parkin, F. Ragazzi and A. Scherrer, "Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law", Study for the European Parliament (Brussels: 2013).

[82] On the same day that the judgment in *Digital Rights Ireland* was delivered, the Court also condemned the premature dismissal of the Hungarian Data Protection Officer as a violation of the Data Protection Directive: *Commission v Hungary* (C-288/12) [2014] E.C.R. I-237; [2014] All E.R. (EC) 895.

[83] See European Commission, DG Internal Policy Study, "The Triangular Relationship between fundamental rights, rule of law and democracy in the EU: Towards an EU Copenhagen Mechanism" (2013) PE 493/031.

[84] *Digital Rights Ireland* (C-293/12) [2013] E.C.R. I-845 at [47].

When adopting legislative measures that interfere seriously with important fundamental rights, the EU legislator has reduced discretion, and the Court will exercise strict control over such acts.[85] As noted by the Council's legal advisers, the Luxembourg Court will not "satisfy itself with anything less than a strict assessment of the proportionality and necessity of measures that constitute serious restrictions to fundamental rights, however legitimate the objectives pursued by the EU legislature".[86] In the future, EU institutions will need to evaluate more carefully the means deployed in pursuing EU objectives, provide better supportive evidence as to the necessity of restrictive measures, carry out serious Charter impact assessments, and generally try to minimise interference with human rights in their legislative undertakings. The Court will not take their statements at face value, but will check that this has been done rigorously, as testified by the detailed empirical questions which the Court asked of the parties to the hearing (e.g. information related to the effectiveness and profiling potential of the instrument, and objective criteria and supporting evidence which served as a basis for the adoption of the Directive).[87]

However, the Court leaves many questions open as to the circumstances in which the strict scrutiny test applies. How "serious" must the interference with human rights be, and how should it be assessed? Does the strict scrutiny apply to any of the rights protected by the Charter, or only to certain, more important, rights; and if so, to which ones? Is the pursuit of certain objectives more likely to justify even serious interference with the Charter's rights; and if so, which ones are they and how should they be determined? Are some policy areas subject to closer scrutiny than others; and if so, which ones, and why? These issues are not addressed explicitly in the ruling, but the Court's position and reasoning may indicate some elements of answer.

First, the Court does not explain what makes the interference a serious one,[88] but endorses the Advocate General's reasoning[89] on the scale and duration of the interference, the intrusion into someone's privacy caused by profiling and mapping potential, or the serious risk of abuse, in particular due to the outsourcing of data retention to the private sector and the possibility for this data to be removed outside of the territorial jurisdiction of the Member States.

Secondly, until now, the Court of Justice has adopted a tougher stance on the EU legislator in relation to non-discrimination based on sex, due process rights, the right to property, and the rights to privacy and data protection. We do not suggest that the Court of Justice is purposely establishing a hierarchy of rights in the Charter, going beyond the existing distinction between rights and principles (art.52(5) CFR). Still, it seems to afford certain rights, including the right to privacy, a particular status.[90]

Thirdly, the fact that the Court of Justice assessed the proportionality of the interference with the rights to privacy and data protection under the Charter only by reference to the "unofficial" security objective of the Directive is puzzling. Had it been keen to "save" the Directive once again, choosing the security objective would have served that purpose well; it is, quite obviously, easier to justify serious intrusion into privacy based on security grounds than on market objectives. However, given that the Court was willing to invalidate the Directive, its decision to rely on the security aim makes little sense at first sight. Perhaps the Grand Chamber was trying to absolve the faux pas of the previous legal basis ruling. We offer, however, a second plausible explanation. Under pressure to take fundamental rights seriously, the

[85] *Digital Rights Ireland* (C-293/12) [2013] E.C.R. I-845 at [48].

[86] See Council of the European Union, General Secretariat, "Judgment of the Court of 8 April 2014 in joined Cases C-293/12 and C-594/12" (May 5, 2014) 909/14 JUR.

[87] "As large a charter as the wind?", Content and Carrier (June 15, 2013), *http://www.contentandcarrier.eu/?p=435* [Accessed October 21, 2014].

[88] *Digital Rights Ireland* (C-293/12) [2013] E.C.R. I-845 at [37].

[89] Opinion in *Digital Rights Ireland* (C-293/12) [2013] E.C.R. I-845 at [70]–[80].

[90] C. Kuner, "The Data Retention Judgment, the Irish Facebook Case, and the Future of EU Data Transfer Regulation" (June 19, 2014), *http://www.concurringopinions.com/archives/2014/06/the-data-retention-judgment-the-irish-facebook-case-and-the-future-of-eu-data-transfer-regulation.html* [Accessed October 21, 2014].

Court has been willing overall to submit security measures, such as anti-terrorist policies (incidentally, often initiated under intergovernmental procedures) to human rights checks. The Court's framing of the Directive as a security measure thus situates the case in the line of the *Kadi* jurisprudence and enables the Court to develop a strong precedential basis for stricter human rights scrutiny of security policies, even when adopted under the ordinary (supranational) legislative process. By marginalising the internal market objective, the Court retains the option of applying different standards of review for market-related measures. This suspicion is fuelled by other decisions, such as the *Pringle* case, in which the Court declined to apply the Charter to intergovernmental EU crisis measures, although these could lead to violations of human rights norms.[91]

Metadata—"essential" issues

In a forward-looking and progressive approach, the Luxembourg justices classify electronic communications metadata as personal data, the collection of which triggers the scope of application of arts 7 and 8 CFR.[92] However, when it summarily dismisses any interference with the essence of privacy and data protection rights, the Court unfortunately reverts to an out-dated perspective, according to which the collection of metadata is less sensitive simply because it does not concern the content of communications (at [40]). This hierarchical and formalistic perception is increasingly contested. In certain instances, even a single communications event can reveal as much of someone's personal circumstances as the interception of the communications content (take, for example, calling help-lines for victims of domestic violence). What is even more disturbing, the Directive makes it possible to construct rich longitudinal metadata about a person's activities over an extended period. Six months of metadata from a mobile phone reveal the user's social network, location profile, commuting patterns, and so on.[93] The retention, use and abuse of metadata are thus liable to affect the essence of the right to privacy as much as the interception of communication content.

Data collection and privacy

The Court of Justice is closing ranks with the ECtHR when it treats the collection and the use of the data as two separate instances of interference with the right to privacy under art.7 CFR and art.8 ECHR (at [34] and [35]).[94] Consequently, data collection (and not just use and access) must meet the criteria of art.52(1) CFR. The Court's application in *Digital Rights Ireland* of a rigorous proportionality test will put to the test other EU schemes collecting personal data.[95] It provides a restrictive frame for the ongoing EU

[91] *Pringle v Ireland* (C-370/12) [2012] E.C.R. I-756; [2013] 2 C.M.L.R. 2.

[92] Guild and Carrera, "The Political and Judicial Life of Metadata" (May 29, 2014), p.5, *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2445901* [Accessed October 20, 2014].

[93] E.g. on the visualisation of six months of retained mobile communications data of a German member of parliament, see K. Biermann, "Betrayed by our own data" (March 26, 2011), Die Zeit, *http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz* [Accessed October 21, 2014]; see for another example from Switzerland, Digital Society, "The life of National Councillor Balthasar Glättli under surveillance" (2014), *https://www.digitale-gesellschaft.ch/dr.html* [Accessed October 21, 2014].

[94] *Leander v Sweden* (1987) 9 E.H.R.R. 433 ECtHR; *Kopp v Switzerland* (1998) 27 E.H.R.R. 91 ECtHR at [53]; *Amann v Switzerland* (2000) 30 E.H.R.R. 843 at [69].

[95] For an assessment of other EU data retention measures, see Boehm and Cole, "Data Retention after the Judgement of the Court of Justice of the European Union" (June 30, 2014), *http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf* [Accessed October 20, 2014]; H. Hijmans, "De ongeldigverklaring van de Dataretentierichtlijn: een nieuwe stap in de bescherming van de grondrechten door het Hof van Justitie" (2014) 7 NtEr 245, 251.

data protection reform, notably the Proposal for a Directive on data protection in the field of law enforcement.[96]

Orphaned national data retention laws and the Charter's umbrella

Sets of instructions, detailed in the following sections, can be derived, a contrario, from the Court's criticisms of the Directive. These principles should be respected by any future EU act, as well as by related national measures. First of all, now that the Data Retention Directive is out, national data retention must comply with the pre-existing ePrivacy Directive; in particular, with its art.15(1), which suggests that a data retention scheme must respect human rights. Furthermore, the Charter applies not only to the EU institutions, but also to Member States when they "implement" EU law (art.51(1) CFR), which the Court has interpreted broadly to include situations falling within the scope of application of EU law, in line with its previous case law.[97] That means that Member States must respect the Charter when they apply, implement and enforce EU measures, but also when they derogate from EU rules.[98] Since data retention schemes are clearly derogations from the data protection principles set out in the Data Protection and ePrivacy Directives, national measures—whether they pre-existed the Data Retention Directive or were adopted to transpose it—must comply with the rights of privacy and data protection guaranteed by the Charter, as interpreted by the Court in *Digital Rights Ireland*.

Judicial instructions to European legislators

Pursuant to *Digital Rights Ireland*, public authorities have to construct a holistic governance system that includes specific safeguards and incorporates extensive checks and balances. The ruling requires guarantees at all stages of the data processing cycle, namely the collection as well as the conditions of retention, access and use of the data, and their monitoring.

First, indiscriminate data retention (the "blanket approach") in the field of law enforcement is not acceptable.[99] Data collection must thus be confined to situations which pose a threat to public security by restricting the measure to a time period, to a geographical zone, or to groups of persons likely to be involved in a serious crime or, more broadly, to persons whose communications data can otherwise contribute to law enforcement.[100] Data retention periods must be determined on the basis of the data's potential usefulness and should remain as short as possible. This "instruction to discriminate" undermines the whole basis of data retention schemes, and suggests a return to more targeted data preservation techniques.

Secondly, while personal data is retained, there should be effective mechanisms ensuring a very high level of protection and security; in particular, data retention should be under the control of an independent authority and reside within the European Union.[101]

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

[97] *Åkerberg v Fransson* (C-617/10) [2013] E.C.R. I-280; [2013] 2 C.M.L.R. 46; *Cruciano Siragusa v Regione Sicilia - Soprintendenza Beni Culturali e Ambientali di Palermo* (C-206/13) [2014] E.C.R. I-126; [2014] 3 C.M.L.R. 13.

[98] *Elliniki Radiophonia Tileorassi v Dimotiki Etairia Pliroforissis and Sotirios Kouvelas (ERT v DEB)* (C-260/89) [1991] E.C.R. I- 2925; [1994] 4 C.M.L.R. 540.

[99] See Guild and Carrera, "The Political and Judicial Life of Metadata" (May 29, 2014), *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2445901* [Accessed October 20, 2014]; H. Hijmans, "De ongeldigverklaring van de Dataretentierichtlijn" (2014) 7 NtEr 245, 250.

[100] *Digital Rights Ireland* (C-293/12) [2013] E.C.R. I-845 at [59].

[101] See the statement by the Article 29 Data Protection Working Party (WP29), *Statement on the ruling of the Court of Justice of the European Union which invalidates the Data Retention Directive* (2014) 14/EN WP 220.

Thirdly, retroactive access to and use of retained data should be restricted to what is "strictly necessary", and must respect procedural and substantive conditions. Access and use by the competent national authorities should be limited to the purposes of preventing, detecting, and prosecuting precisely defined serious offences. Requests for access to retained data should be reasoned, and subjected to prior review by a court or an independent administrative body charged with ensuring compliance with constitutional and legislative limits to data access and use. There should also be safeguards that authorise only a limited number of persons to access and subsequently use the data in line with a specific request.[102]

The public-private divide in data retention and global data flows

While private sector organisations can facilitate data collection and retention, the rules that govern these private deputies of law enforcement must be strict and ensure a high level of protection; for example, they should not allow service providers to take account of economic considerations in order to determine security levels.

The EU judges display an acute awareness of today's global data flows and the possibility for data to reside in cloud services worldwide (at [68]). The ruling could be interpreted as preventing transfer of data by private operators—but also possibly, EU institutions and public authorities—outside the European Union, since access and use would then be removed from control by an independent authority, contrary to art.8(3) CFR (at [68]). [103]

Yet, the victory against mandatory data retention may be largely symbolic, as metadata lives a long life in the private sector. Under art.6(1) of the ePrivacy Directive, network operators and providers of electronic communications services can keep metadata as long as necessary for billing purposes, or if the subscriber or user has given her consent to the processing of traffic and location data for marketing purposes. Consequently, such data will often be available, even without a mandatory data retention scheme.

Conclusions

The subsequent *Google Spain* ruling is now taking the spotlight.[104] Yet, *Digital Rights Ireland* qualifies as a landmark ruling on a number of accounts. First, it imposes on the EU legislator a new level of responsibility to protect fundamental rights. Secondly, it subjects it to a novel strict judicial scrutiny test. Thirdly, it declares invalid an EU framework law for violation of Charter rights. Fourthly, it composes substantive instructions for the attention of law-makers at EU and national levels, in order to guarantee suitable protection for the rights to privacy and data protection in a context of increased securitisation and exceptionalism. We conclude that *Digital Rights Ireland* not only imposes a strict framework for future laws and policies which interfere with personal data in Europe; it also has the potential to reconfigure inter-institutional relationships in the European Union, and to bring human rights and constitutionalism more to the core of the European project in a way that could impact on the future trajectory of European integration.

With this ruling, the Court not only mobilises the Charter's rights of privacy and data protection against blanket data retention, and the resulting potential misuse and abuse of personal data. It also shows a firm determination to rein in the state of exception and securitisation trends that infuse recent European

[102] *Digital Rights Ireland* (C-293/12) [2013] E.C.R. I-845 at [61]–[62].

[103] See K. Irion, "Government Cloud Computing and National Data Sovereignty" (2012) 4 *Policy & Internet* 40; Kuner "The Data Retention Judgment, the Irish Facebook Case, and the Future of EU Data Transfer Regulation" (June 19, 2014), *http://www.concurringopinions.com/archives/2014/06/the-data-retention-judgment-the-irish-facebook-case-and-the-future-of-eu-data-transfer-regulation.html* [Accessed October 21, 2014].

[104] *Google Spain SL and Google Inc v Agencia Espagnola de Proteccion de Datos (EPD) and Mario Costeja Gonzales* (C-131/12) [2014] E.C.R. I-317; [2014] 3 W.L.R. 659.

anti-terrorist laws, and works to minimise their interference with important fundamental rights. Taken together, the *Digital Rights Ireland* and *Google Spain* rulings confirm that high standards of privacy and data protection are applicable to the public and private sectors in the European Union in the Big Data era. Legal proceedings are already lining up in front of Luxembourg and Strasbourg to test the further implications of Europe's protective approach for other EU and national data-related measures.[105]

The scope of the European Union's responsibility to protect human rights and of the related strict scrutiny test remain uncertain, and we should be careful not to overestimate the Court's willingness to apply rigorous human rights monitoring across the board of EU activities. However, if Luxembourg persists in this direction, *Digital Rights Ireland* could mark a "foundational moment" in EU constitutionalism[106] which could reorient European integration more broadly. This ruling contributes to the transformation of the relationship between the Court of Justice and the EU legislator, from one of reciprocal deference into one of mutual control. The Court's more welcoming attitude towards preliminary references contesting the validity of directives could encourage more litigants to try this avenue. From an "instrument of integration", this emblematic procedure may well mutate into a "disintegrative device" or, more appropriately, a real constitutional review instrument. In this redefined constitutional context, human rights would eventually supersede the internal market as the core aim of the integration project,[107] and the Court would slowly reinvent itself, evolving from the engine of integration into a proper constitutional court, whose core task would consist in ensuring respect for human rights and democratic checks and balances when EU institutions or national authorities are failing. There is, however, a risk that the resulting heightened scrutiny of the EU legislator would encourage EU institutions and Member States to resort to "unorthodox" modes of action outside of the EU legal framework, as they did with the European Stability Mechanism in the context of the euro zone crisis (and to which the Court did not object in *Pringle*), or let private actors do the job.

There is a symbolic dimension to the fact that the strict scrutiny test was first applied to the right to privacy: "the" human right in the information age. While *Digital Rights Ireland* clearly marks an important step for the protection of fundamental rights at EU level, and for data protection and the right to privacy in Europe, only time will tell whether it will also go down as one of the "great cases" in European integration.

[105] E.g. *Schrems v Data Protection Commissioner (Facebook)* (C-362/14) and *Centrum för rättvisa v Sweden* (35252/08), application of July 14, 2008; *Big Brother Watch v United Kingdom* (58170/13), application of September 4, 2013.

[106] S. Peers, "The Data Retention Judgment: The CJEU prohibits Mass Surveillance" (April 8, 2014), *http://eulawanalysis.blogspot.hu/2014/04/the-data-retention-judgment-cjeu.html* [Accessed October 21, 2014].

[107] On the desirability of such a transformation, see A. von Bogdandy "The European Union as a Human Rights Organization and the Core of the European Union" (2000) 37 C.M.L. Rev. 1307.