10. The fate of the Data Retention Directive: about mass surveillance and fundamental rights in the EU legal order

Luisa Marin

1. INTRODUCTION

In the past couple of years, the public debate in Europe and in the United States has been dominated by Edward Snowden's revelations regarding mass surveillance programs, adopted by the US National Security Agency (NSA) and by its British intelligence counterpart, the Government Communications Headquarters (GCHQ), to carry out extensive and secret surveillance activities in respect of private communications. The clandestine anti-terrorism data-mining program PRISM collects stored Internet communications from requests made to Internet companies such as Google, Yahoo, Microsoft, Facebook, AOL, Skype, Apple and other companies of the Internet 2.0. Before Snowden, the public debate had centred since 2010 around another whistleblower, Julian Assange, whose leaks had begun to unveil the illicit activities carried out by the US government in the framework of the fight against terrorism and radical Islam.[1] In 2013 and 2014, illicit mass surveillance practices carried out by governmental agencies, on both sides of the Atlantic, against private citizens and also (European) politicians,[2] therefore came under the scrutiny of public opinion.

These revelations disclosed a 'datagate' scandal, in which law enforcement agencies systematically collected extensive telecommunications data from private citizens, operating according to methods and instruments normally prohibited by the law.[3] The salient feature of surveillance under PRISM and other questioned computer programs (such as Tempora and Boundless Informant), as has emerged in the past two years, is the secretive nature of the programs, allowing 'extensive in depth surveillance on live communications and stored informations'.[4] This has led to profound criticism of such surveillance practices, but also of the governments involved with them, in particular the Obama administration: eventually, what 'ended up in the dock' is the post 9/11 2001

[1] See the special section on this at www.theguardian.com/us-news/the-nsa-files.

[2] See www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies.

[3] Protect America Act of 2007 and the FISA Foreign Intelligence Surveillance Act Amendments of 2008; they immunize private companies when they cooperate with US government agencies in intelligence collection. Source Wikipedia page on PRISM, at http://en.wikipedia.org/wiki/PRISM_(surveillance_program).

[4] *Ibid.*

idea that security can legitimate all types of (pre-emptive) governmental surveillance practices, with no concern at all for (and actually in radical contrast with) the rule of law.[5]

Against this background, and in another perspective, 2014 has been a crucial year for privacy and data protection. After Snowden's revelations and probably also because of the 'datagate' scandal, the Court of Justice of the European Union (CJEU) instituted in 2014 its own 'Privacy Spring',[6] delivering two judgments, *Google Spain*[7] and *Digital Rights Ireland*,[8] of crucial importance for privacy and data protection in Europe, and whose effects and consequences will also be felt on the other side of the Atlantic.

In a nutshell, in *Google Spain* the Court specified that the right to rectification, erasure and blocking of personal data, under article 12 of the Data Protection Directive 1995/46/EC (DPD), together with the right of the data subject to object to the processing of data relating to him (article 14 DPD) applies also to search engines, such as Google, which therefore come within the definition of 'controller' in the meaning of the Directive.[9] The *Google Spain* judgment interprets the right to rectification and the right to objection as the 'right to be forgotten'. Whereas the scope of *Google Spain* concerns actors such as Internet search engines, and therefore private companies, in *Digital Rights Ireland*, the CJEU declared invalid and void for breach of the fundamental rights to privacy and data protection the Data Retention Directive 2006/24/EC.[10] This was the first time in EU law that the CJEU had completely annulled a European legislative instrument for its non-compliance with fundamental rights as enshrined in the Charter of Fundamental Rights of the EU (the 'Charter'), which has (since 1 December 2009) the same status as the Treaties. The *Digital Rights Ireland* judgment was and will remain one of the 'grand cases' of the CJEU, for many reasons: first, because the Court intervened in the debate on a much contested instrument associated with the fight against terrorism; secondly, for its relevance to

---

[5] On the dilemma between State of Terror and State of Law, see G. De Minico, 'A Tale of Two States: Rule of Law in the Age of Terrorism', available at www.verfassungsblog.de. On European counter-terrorism, see also C.C. Murphy, *EU Counter-Terrorism Law: Pre-Emption and the Rule of Law* (Oxford, Hart, 2012).

[6] The quote is from S. Peers, 'The Domino Effect: How Many EU Treaties Violate the Rights to Privacy and Data Protection?', available at http://eulawanalysis.blogspot.nl/2014/11/the-domino-effect-how-many-eu-treaties.html.

[7] C-131/12 *Google Spain* v. *AEPD*, CJEU (Grand Chamber), Judgment of 13 May 2014 (nyr).

[8] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd* v. *Ireland*, CJEU (Grand Chamber), Judgment of 8 April 2014 (nyr).

[9] In the *Google Spain* judgment, Google was held to be a data controller for its activity as a search engine. Collecting, retrieving, storing, and disclosing data from the Internet, even without altering the text, is to be interpreted as processing personal data in the meaning of the Data Protection Directive (DPD). After clarifying the territorial scope of the DPD, the Court stated that Google was responsible for removing information on data subjects from search engine results.

[10] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54.

European constitutional law, namely, in interpreting data protection rights as enshrined in the Charter; thirdly, for its implications for the legal orders of the Member States; fourthly, for its implications as regards other surveillance instruments of the EU, embracing both other domestic instruments, and also external agreements which have implications for surveillance.

This chapter will address the *Digital Rights Ireland* judgment and (some of) its implications. In order to do so, it will proceed as follows: after this introduction, the chapter will discuss the Data Retention Directive and the domestic resistance and contestations the Directive has met; it will then move on to focus on the judgment, its most relevant legal reasoning and motivations; it will then present its implications for national data retention legislation, before discussing the effects of this case for other European databases or instruments, even those not focusing on surveillance but which nevertheless include provisions on the access of law enforcement authorities to data, before concluding.

2. ABOUT PRIVACY, DATA PROTECTION AND 'THEIR ENEMIES': THE DATA RETENTION DIRECTIVE

In the aftermath of the terrorist attacks in Madrid and London in 2004 and 2005, respectively, law enforcement agencies became interested in gaining access to location and traffic data in the context of the fight against terrorism and serious crime. According to the Commission, up to six months of telephone data were investigated.[11] Some states enacted data retention legislation in the context of domestic anti-terrorism measures. Therefore, a pro-security lobby gained support at EU level and provisions for the retention of data for the purpose of prevention, investigation, detection and prosecution of criminal offences were adopted by the EU, under the British Presidency, in the form of the Data Retention Directive 2006/24/EC (DRD).[12]

The Directive sought to harmonize the obligations of private providers of communications to retain data. The DRD obliges telecommunication providers to monitor and store meta-data about the Internet and (mobile and landline) telephony activities of their customers for periods ranging from six months to a maximum of two years. Meta-data are data about location (source and destination), date, time and duration, as well as data to identify the type of communication equipment used. The DRD, adopted in an attempt to combat terrorism, requires all service providers to store traffic data for all communications, and therefore it applies without distinction to everybody, and thus

[11] 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, SEC(2005)1131, and Commission Staff Working Document, COM(2005)438 final.

[12] C. Jones, *Background to the EU Data Retention Directive* (7 April 2014), available at http://eulawanalysis.blogspot.nl/2014/04/background-to-eu-data-retention.html.

to persons against whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect and remote one, with terrorism and serious crime.[13]

Because of the scope of the collection of data it enabled, the Directive represented an exception and derogation from consolidated data protection principles, namely, the principles of purpose specification and purpose limitation, next to data quality principles, such as relevancy and limited retention period, and proportionality. The Directive therefore catalyzed a constitutional conflict without precedent in the history of EU law. Before the DRD, the European Arrest Warrant (EAW) also encountered significant resistance and opposition from the Member States, whether through legislative organs, at the enforcement level or from the judiciary.[14] It is interesting to note that both the DRD and the EAW have been part of the mainstream security discourse post 9/11. But how was this resistance manifested, after publication of the DRD in the Official Journal of the EU?

First, transposition of the DRD was opposed and delayed. The Commission initiated infringement proceedings against Austria, the Netherlands, Sweden, Greece and Ireland for having failed to transpose the Directive within the prescribed period. Secondly, enforcement of the Directive was sporadic, for example, as regards the duration and purpose of retention of data, the procedures regulating access to personal data and the costs of retention for operators.[15] Sweden was faced with infringement proceedings for a very late transposition of the Directive and received a lump sum fine of 3 million Euros for this.[16] The Commission had also initiated infringement proceedings against Germany, whose BundesVerfassungsgerichthof had totally invalidated the national transposition law, when the CJEU pronounced its judgment in the *Digital Rights Ireland* case.[17]

However, this is not the most notable part of the story. What is most significant about the DRD is the degree of legal contestation advanced by higher national courts. Indeed, several domestic constitutional courts (or courts vested with constitutional adjudication functions) have challenged (at least partially) the domestic provisions implementing the DRD for breach of constitutional rights: this is the case for the Bulgarian Supreme Administrative Court (2008), the Romanian Constitutional Court (2009), the German

---

[13] J.P. Mifsud-Bonnici, 'Redefining the Relationship Between Security, Data Retention and Human Rights' in R.L. Holzhacker and P. Luif (eds), *Freedom, Security and Justice in the European Union* (New York, Springer, 2014), p. 49.

[14] E. Guild and L. Marin (eds), *Still Not Resolved? Constitutional Challenges to the European Arrest Warrant* (Nijmegen, 2009).

[15] T. Konstadinides, 'Destroying Democracy on the Ground of Defending It? The Data Retention Directive, the Surveillance State and Our Constitutional Ecosystem' (2011) *European Law Review* 722, 723.

[16] Ex Art. 260 TFEU. See C-270/11 *Commission* v. *Sweden*, CJEU, Judgment of 30 May 2013.

[17] C-329/12 *Commission* v. *Germany*, withdrawn after *Digital Rights Ireland*.

Federal Constitutional Court (2010), the Czech Constitutional Court (2011)[18] and in Cyprus (2011).[19]

This is an unprecedented circumstance in EU law and is a symptom of a deep malaise, of serious concerns regarding a legislative instrument. As is well known, constitutional courts cannot challenge domestically the validity of a European instrument,[20] but may only channel their complaints regarding domestic legislation implementing a European instrument. In all these proceedings, the courts complained about the massive impact of the surveillance measures, and the legality and proportionality of the same.

In addition to this widespread and decentralized contestation, the DRD not only met resistance within the Member States, at the stage of its transposition and enforcement. Earlier it was also challenged directly by Ireland before the CJEU on the ground of the legal basis used for its adoption.[21] Ireland challenged the validity of the DRD via an annulment procedure under Article 263 of the Treaty on the Functioning of the European Union (TFEU), contesting the legal basis of Article 114 TFEU (under Article 95 TEC).[22] This is the so-called residual legal basis of the internal market, and Ireland contested whether Article 95 TEC, and the whole EC pillar in general, was the right basis enabling the adoption of a legal instrument aiming at 'facilitat[ing] the investigation, detection and prosecution of crime, including terrorism'.[23]

The CJEU, consistently with its case law on Article 95 TEC, did not challenge the political reasons underlying the Directive, but, observing the emergence of national legislation on the retention of data relating to electronic communications, stated that 'the differences between the various national rules adopted on the retention of data were liable to have a direct impact on the functioning of the internal market and that it was foreseeable that the impact would become more serious with the passage of time'. Based on this and on other arguments, such as the fact the DRD amended e-Privacy Directive 2002/58/EC,[24] and after a substantive examination of its provisions, the Court concluded that the desired effect of the Directive was the harmonization of the

---

[18] On Bulgaria, see www.aip-bg.org/documents/data_retention_campaign_11122008eng.htm; on Romania, see http://archive.news.softpedia.com/news/Romanian-Data-Retention-Law-Ruled-Unconstitutional-123908.shtml; on Germany, see https://edri.org/edrigramnumber8-5german-decision-data-retention-unconstitutional/; on Cyprus, see https://edri.org/edrigramnumber9-3data-retention-un-lawful-cyprus/; on the Czech Constitutional Court, see http://jurist.org/paperchase/2011/03/czech-constitutional-court-overturns-parts-of-data-retention-law.php.

[19] Cyprus Supreme Court, Judgment of 1 February 2011, available at www.supremecourt.gov.cy/judicial/sc.nsf/0/5B67A764B86AA78EC225782F004F6D28/$file/65-09.pdf. For information in English, see the EDRI blog at https://edri.org/edrigramnumber9-3data-retention-un-lawful-cyprus/.

[20] 314/85 *Fotofrost*, CJEU, Judgment of 22 October 1987.

[21] C-202/09 *Commission* v. *Ireland* [2009] OJ C167.

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

[23] *Ibid.* para. 28.

[24] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive) [2002] OJ L201/37.

legislation of Member States concerning an aspect of the functioning of the internal market.[25]

Why so much resistance against a Directive? What are its main provisions and consequences? The main objectives of the DRD are to harmonize providers' obligations to retain meta-data, and, secondly, to ensure that the data retained are available for the purpose of the investigation, detection and prosecution of serious crime.[26] As such, its provisions create two main effects: first, providers are required to store data, and this has relevant economic implications; and, secondly, the DRD's provisions significantly affect individuals. As recalled above, the Directive does not cover the content of the communications, but applies to traffic and location data of both natural persons and legal entities.[27] It provides for an obligation to retain data and to provide such data to competent national authorities: 'Member States shall adopt measures to ensure that the data specified in Article 5 ... are retained ... to ensure that data retained are provided only to the competent national authorities in specific cases and in accordance with national law'.[28]

The data to be retained are the ones that are necessary to trace and identify the source of a communication, the destination of a communication, the date, time and duration of the same, the type of communication, and to identify users' communication equipment.[29] The period of retention varies from 6 to 24 months from the date of the communication.[30] In the aftermath of the London and Madrid terrorist bombings, law enforcement authorities pushed to have access to this type of data and legislators reacted to these requests; hence the Directive provides that the retained data and any other necessary information relating to such data must be transmitted upon request to the competent authorities without undue delay.[31]

The DRD provides for some data protection and data security guarantees and for a supervisory independent authority monitoring respect for the data security principles.[32] These are that (a) the retained data must be of the same quality, and subject to the same security and protection as those data on the network; (b) measures must be taken to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorized or unlawful storage, processing, access or disclosure; (c) other measures must be taken to guarantee that retained data can be accessed by specially authorized personnel only; and (d) retained data must be destroyed at the end of the retention period.[33]

---

[25] T. Konstadinides, 'Mass Surveillance and Data Protection in EU Law: the Data Retention Directive Saga' in *European Police and Criminal Law Co-operation*, Oxford Swedish Studies in European Law (Oxford, Hart Publishing, 69). See also *Ireland* v. *European Parliament and European Council*, above n. 22, para. 73 *et seq.*

[26] DRD, Preamble, recital 21.

[27] *Ibid.* art. 1.

[28] *Ibid.* arts 3 and 4.

[29] *Ibid.* art. 5.

[30] *Ibid.* art. 6.

[31] *Ibid.* art. 8.

[32] *Ibid.* art. 9.

[33] *Ibid.* art. 7.

As such the DRD constituted an important erosion of the principles of the DPD and of the e-Privacy Directive,[34] which form the foundations of the data protection legislation in the EU and which substantiate the fundamental rights provided for in the Charter, under Article 8.

3. WHEN A DIRECTIVE CONFLICTS WITH EU'S FUNDAMENTAL RIGHTS: THE *DIGITAL RIGHTS IRELAND* JUDGMENT

In 2012, two preliminary references were lodged at the CJEU; one originated from Ireland, where an Irish NGO, Digital Rights Ireland, challenged the legality of the national legislative and administrative measures on data retention; the second originated from Austria, where 11,130 constitutional complaints have been lodged by private parties, among them Mr Seitlinger and Mr Tschohl, and also by the Carinthian government. In their actions, the applicants questioned the legality of the implementing national legislation and of the DRD for alleged breaches with fundamental rights. The questions referred to the CJEU by Ireland were whether the provisions on the retention of meta-data, on the law enforcement authorities having access to those data, and on the time of retention were in conflict with the principle of proportionality, the freedom of movement and residence granted to the citizens of the EU, with the right to privacy, with the right of protection of personal data, with the right to freedom of expression and with the right to good administration under Article 41 Charter.[35]

Similarly, the Austrian Constitutional Court referred questions on the compatibility of the DRD with the Charter for allowing the storage of 'so many types of data in relation to an unlimited number of persons for a long time'. The Austrian Court stressed that the retention of data concerned 'almost exclusively persons whose conduct in no way justifies the retention of data relating to them'.[36] The DRD allowed for a 'unquantifiable number of persons having access to the data for a minimum period of six months',[37] therefore raising doubts as to the adequacy and the proportionality of the interference with fundamental rights. However, the Austrian Court narrowed the scope of the scrutiny requested by the CJEU, focusing on the right to privacy, right to data protection and right to freedom of expression; it nevertheless posed interesting constitutional questions as to the interaction between primary law and secondary law, between the Charter and the European Convention on Human Rights (ECHR); under the former, the Austrian Court explored the relevance of the secondary law (more precisely, the DPD and the regulation of data protection by Union institutions) for the interpretation of fundamental rights and of their limitations; under the latter, it also

---

[34] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

[35] *Digital Rights Ireland*, above n. 8, Judgment, paras 17–18.

[36] *Ibid.* para. 20.

[37] *Ibid.* para. 20.

inquired whether the case law of the European Court of Human Rights (ECtHR) could provide assistance for the interpretation of the right of privacy in Article 7 Charter.

The CJEU decided to tackle the challenge to the validity of the DRD from the perspective of the right to privacy, data protection and freedom of expression. It focused more specifically on privacy and data protection, though it recognized that the Directive might also have an impact on freedom of expression. On this latter point, the Court stated that although:

> the directive does not permit the retention of the content of the communication or of information consulted using an electronic communication network, it is not inconceivable that the retention … might have an effect on the use, by subscribers or registered users, of the means of communication covered by that directive, and consequently, on their exercise of the freedom of expression.[38]

The Court referred here to the 'chilling effect', i.e., the inhibition or discouragement of the legitimate exercise of natural and legal rights by the threat of legal sanction, although the emphasis is not strictly on legal sanctions, but rather on extensive surveillance by a private 'Big Brother'.

However, the core of the legal reasoning referred to Articles 7 and 8 Charter. The question was framed by the Court as a question of retention of a broad set of meta-data concerning communications, data which enabled knowledge of the identity of the person with whom a subscriber or registered user has communicated, the means, the time and place of the communication, and its frequency. Following retention by telecommunication providers, the DRD allowed access to the data by competent national authorities; it therefore derogated from the system of protection of privacy created by the DPD and the e-Privacy Directive. While tackling the questions arising on privacy and data protection, the Court here addressed a relevant constitutional adjudication question, i.e., the relevance of secondary law for the definition of the fundamental rights defined in the Charter, which is now part of the primary law of the EU. And the Court answered those questions affirmatively, in the sense that it considered the right to privacy included the 'confidentiality of communications and of traffic data as well as the obligation to erase or make those data anonymous where they are no longer needed'.[39]

Interestingly, the CJEU framed the obligation to retain data and to make them accessible to the national law enforcement authorities as two distinct interferences with privacy.[40] As regards the second, the Court also considered the case law of the ECtHR.[41] Similarly to the Opinion of the Advocate General, the interferences with privacy and data protection were deemed to be wide-ranging and particularly serious.

---

[38] *Ibid.* para. 28.

[39] *Ibid.* para. 32.

[40] *Ibid.* paras 34–5.

[41] *Leander* v. *Sweden*, Application no. 9248/81, Series A no. 116, ECtHR, Judgment of 26 March 1987, para. 48; *Rotaru* v. *Romania*, Application no. 28341/95, ECtHR, Judgment of 4 May 2000, para. 46; *Weber and Saravia* v. *Germany* (dec.), Application no. 54934/00, Admissibility Decision of 29 June 2000, para. 79.

Having established the existence of an interference, the analysis then moved on to the justification and proportionality of the same, carried out through the medium of Article 52(4) Charter. In the view of the Court, the essence of the protection of the right to privacy was not violated because the DRD did not allow the retention of the content of the communication, but only of traffic data. Similarly, the essence of data protection was not violated by the DRD because Member States were to ensure that appropriate technical and organizational measures were adopted against accidental or unlawful destruction, accidental loss or alteration of the data. However, even if not touching the core of privacy and data protection, were those interferences proportionate?

The next step of the proportionality scrutiny required an assessment of whether the interference satisfied an objective of general interest, recognized by the Court in the fight against serious crime and ultimately the enhancement of public security. Those aims, under the case law of the CJEU, are to be considered as objectives of general interest, as established in the *Kadi and Al Barakaat* and in the *Tsakouridis* case law.

The core of the Court's judgment centred on proportionality control, which required that the DRD was appropriate for the attainment of a legitimate aim and did not exceed the limits of what was appropriate and legitimate in order to achieve those aims. On this point, the Court considered that EU legislation involves a limited discretion, with the implication that the review of such discretion should be strict, because of the 'important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference'.[42]

On the appropriateness of the Directive, the Court's assessment was positive. It was, however, on the ground of its necessity that the Court rejected mass surveillance.[43] This position was particularly important as it represented the CJEU's doctrine on the normalization of a state of exception and of a state of emergency: the highest court of the EU legal order considered that the fight against serious crime, in particular against organized crime and terrorism, however important it may be for public security, did not in itself justify the extensive surveillance of the whole population in the EU as necessary.[44] In the reasoning of the Court, the respect for private life is subject to derogations and limitations that must apply only in so far as strictly necessary, recalling its judgment in *IPI*.[45] So, the Court here anchored the respect for privacy to the principle of strict legality, meaning that the law had to specify with some precision the cases and conditions in which the right to privacy could be limited, and that such limitations must be subject to judicial scrutiny.[46] For this purpose, the Court, while it considered data protection as a distinct legal framework, nevertheless seemed to interpret it as functional to the protection of privacy. Indeed it stated that:

> In that regard, it should be noted that 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.[47]

---

[42] *Digital Rights Ireland*, above n. 8, Judgment, para. 48.
[43] *Ibid.* para. 51 *et seq.*
[44] *Ibid.* para. 51.
[45] *Ibid.* para. 52.
[46] Recalling C-73/07 *Satakunnan Markkinapörssi and Satamedia* [2008] ECR I-09831.
[47] *Digital Rights Ireland*, above n. 8, Judgment, para. 53.

This statement, on the one hand, recognizes the distinct nature of data protection as compared to privacy, whereas, on the other hand, the Court seems to frame data protection as a right functional to the protection of privacy. However, the consequence of the establishment of this connection is that the Court held that the right to data protection must also involve the same guarantees as privacy, namely, the principle of strict legality. Therefore, the Court considered that EU legislation must lay down 'clear and precise rules governing the scope and application of the measures in question and imposing minimum safeguards' in the form of guarantees granting effective protection in case of abuse, unlawful access and use of those data. And it is precisely there that the DRD failed in its mission, by providing automatic processing of a great amount of data from 'practically the entire European population'.[48] The Directive covered all means of electronic communication, and it therefore targeted in a generalized manner all persons and all means of communication, and traffic data; secondly, no differentiation, limitation or exception was made in the light of the objective of fighting against serious crime. The lack of connection, even indirect, with a situation which was liable to give rise to a criminal prosecution, and lack of exception for communications covered under national law by the obligations of professional secrecy, in the view of the Court went beyond what was strictly necessary. In its reasoning on the scope of the surveillance, the Court rejected the pre-emptive logic which has animated many of the counter-terrorist measures, the logic according to which total surveillance is needed because the fight is targeting an absolute evil.[49] It is the same logic underlying the principle of availability, which is in sharp contrast with the principles of collection limitation and purpose specification, and also with the e-Privacy Directive, which requires data to be deleted once no longer needed for billing purposes.[50] The rationale of *Digital Rights Ireland* echoes the *Kadi* judgment,[51] in the sense that the Court rejected the necessity of an EU legal instrument derogating from the principles of the constitutional state based on the rule of law. Here, the Court clearly rejected the 'panopticism' underlying this and other measures adopted in the surveillance package of EU law.[52]

Another point stressed by the CJEU is the lack of an objective criterion by which to determine the limits of the access of law enforcement agencies to the retained data and their use.[53] Article 4 of the DRD 'does not expressly provide that the access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal

---

[48] *Ibid.* paras 55–7.

[49] The reference is to George W. Bush's framing of terrorism after 9/11 as a war on terror against an 'axis of evil'. See also 'Statement by the President in His Address to the Nation', 11 September 2001, where he stated 'Today, our nation saw evil, the very worst of human nature', available at http://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010911-16.html.

[50] Murphy, *EU Counter-Terrorism Law*, above n. 5, at 149.

[51] Joined Cases C-402/05P and C-415/05P *Kadi and Al Barakaat* v. *Council*, CJEU (Grand Chamber), Judgment of 3 September 2008.

[52] Murphy, *EU Counter-Terrorism Law*, above n. 5, at 147 *et seq.*; V. Mitsilegas, *EU Criminal Law* (Oxford, Hart, 2009), p. 235 *et seq.*

[53] *Digital Rights Ireland*, above n. 8, Judgment, para. 60 *et seq.*

prosecutions relating thereto'.[54] Furthermore, the Court complained that the Directive did not provide for a judicial review or a form of review controlling the extent of the access to the data by the national authorities.[55] The third argument and requirement indicated by the Court related to the time of the retention, which varied from six to 24 months, without objective criteria ensuring that the retention was limited to what was strictly necessary.[56] The fourth argument concerned the rules on security and protection of the data retained by TLC providers. In this aspect, the DRD failed to ensure that a 'high level of protection and security is applied' by the providers by means of organizational and technical measures, but rather left it up to the providers to determine the level of security which they applied, including in light of economic considerations on the costs of such measures. Lastly, by not requiring that the data in question were retained within the EU, the Directive failed to comply with the guarantee of the control by an independent authority required by Article 8(3) Charter.

The challenge to the Directive was not examined under the question of freedom of expression, as the DRD was declared invalid, on the grounds that it provided for extensive surveillance of persons, mainly unconnected with any crimes, and that it left it up to the providers to decide on the level of protection of the data retained.

4. A SURFACE AVALANCHE OR DEEP SEISMIC WAVES? IMPLICATIONS OF *DIGITAL RIGHTS IRELAND* ON MEMBER STATES' LEGAL ORDERS

The consequence of the *Digital Rights Ireland* judgment was the invalidation of the DRD. Considering that the CJEU has the power to limit the effects of its judgments under article 264 TFEU, and also that it did not make use of it, the correct interpretation is that the effects of the invalidation are *ex tunc*, i.e., that the Court determined the total invalidity of the Directive *ab initio*. This means that the European Commission may, at any time, initiate a new legislation on data retention in order to fill the legislative void left by the judgment.

So then the question remains as to the effects of the judgment on national legal orders. This question is all the more relevant considering the resistance encountered by the DRD in its transposition process into Member States' legal orders. What dynamics will occur within their legal orders? Here, legislators, governments and judiciaries will play a decisive role, alongside private actors who might initiate judicial challenges to the implementing legislation.

The impact of the judgment on national legislation under EU law, however, is not so clear: in EU law, it has not been established what happens to national legislation once a European instrument is invalidated. Of course, one has to consider those effects in the context of the general doctrines of EU law, in particular having regard to the principle of the primacy of EU law over national law, which includes also the case law of the

---

[54] *Ibid.* para. 61.
[55] *Ibid.* para. 62.
[56] *Ibid.* para. 64.

CJEU, and the principle of effectiveness of EU law. Secondly, one should also consider that the *Digital Rights Ireland* judgment interprets fundamental rights as being enshrined in the Charter and also as general principles of EU law (Article 6 of the Treaty on European Union (TEU)). So that, even where a Directive is invalidated, and national laws therefore no longer 'implement' (narrowly interpreted) EU law, according to established case law of the CJEU, Member States have to abide by fundamental rights when they derogate from EU law.[57] More recently, in *Åkerberg Fransson*, the CJEU stated that its case law concerning the scope of the general principles of EU law also applied to the Charter.[58]

The reasoning of the Court is especially relevant in this judgment, because the DRD has not been invalidated for procedural reasons, but for substantive ones, for reasons concerning the protection of fundamental rights as enshrined in the Charter and as specified by secondary law, namely, the e-Privacy Directive and the DPD. This has several implications: first, the reasoning of the Court indicates the requirements and therefore specifies the limits that the European and the national legislators should abide by, in assessing the current national legislation on data retention, and in passing new legislation on data retention and on data in general. Secondly, not only the national legislators, but also the national judges, as the 'outposts' of the EU legal order within the Member States, will be confronted with questions concerning the implementation of national measures in the field and will therefore have to assess them according to the construction and specifications of the rights as set out by the CJEU in this judgment. In such a situation, many actors could activate a process of challenge of the national laws on data retention, especially now that the national legislation can no longer be framed as implementing EU law (under Article 51 Charter), since the DRD has been invalidated.[59]

Considering the dissent triggered within the EU by such a Directive, it is easy to imagine that national measures will also be litigated in other legal orders, and in such cases the national courts will have to stick to the criteria defined by the CJEU.

If we look at it from the perspective of the Member States, we have several options: first, to start a process of revision or repealing of the national laws, as announced by, e.g., Luxembourg, on the same day as the judgment.[60] So far, for example, Denmark and the United Kingdom have already reassessed their national legislation. In Denmark, however, it was concluded that the Danish legislation was in line with the *Digital Rights Ireland* requirements and therefore no reform was needed. The United Kingdom

---

[57] The reference is to C-260/89 *ERT* [1991] ECR I-02925, CJEU, Judgment of 18 June 1991, and to C-368/95 *Vereinigte Familiapress Zeitungsverlags- und vertriebs GmbH* v. *Heinrich Bauer Verlag*, CJEU, Judgment of 26 June 1997.

[58] C-617/10 *Åklagaren* v. *Hans Åkerberg Fransson*, CJEU (Grand Chamber), Judgment of 26 February 2013, and see S. Peers, 'Are National Data Retention Laws Within the Scope of the Charter?', *EU Law Analysis*, 20 April 2014, available at http://eulawanalysis.blogspot.nl/2014/04/are-national-data-retention-laws-within.html.

[59] On the issue, see Peers, 'Are National Data Retention Laws Within the Scope of the Charter?', above n. 58.

[60] F. Boehm and M.D. Cole, *Data Retention after the Judgment of the Court of Justice of the European Union* (June 2014), p. 49, available at www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf.

has already amended the national legislation on the issue: the Data Retention and Investigatory Powers Act 2014 was passed in a fast-tracked legislative procedure. Presented and adopted in the swift time-span of three days, the Act however triggered the reactions of some MPs and a civil rights organization, which have challenged the Act before the courts.[61] Under this Act, communication service providers may be required to continue to retain communication data through retention notices, and provisions guarantee oversight and transparency. So, it does not seem to discontinue the approach adopted by the previous Regulation and Investigatory Powers Act 2000.

Secondly, another option is to wait until national courts clarify the fate of the national legislation, perhaps at the initiative of economic operators or of private groups, which might have an interest in challenging the legislation; another option is to give the CJEU another opportunity to 'speak' on these laws, by investing it once again with the issue by a preliminary reference on the relation between the annulled European Directive and the implementing national laws. Considering the significant resistance met by the DRD even before the *Digital Rights Ireland* judgment, it is not unlikely that other higher courts will follow the option of declaring the national legislation unconstitutional. For example, actors such as Digital Rights could challenge national laws. This is already the case in Austria, where after the judgment of the CJEU, the Constitutional Court declared its transposition law void.[62] The Slovenian Court followed this example.[63] In Romania, the Constitutional Court on 8 July 2014 also declared the second transposing law void (following its similar judgment in 2009). And in September 2014, the Romanian law on the obligation for all users of pre-paid Sim cards to register has been declared invalid, also mainly for lack of data protection guarantees.[64] Another challenge is pending in Slovakia, where the national Constitutional Court has provisionally suspended the applicability of some national provisions, as an interim measure and in the process of adjudicating on the same law.

Another possibility, less direct and limited by the necessity of exhaustion of the system of national judicial remedies, is adjudication by the ECtHR: affected parties, such as telecommunication companies, individuals and interest groups, could litigate acts of their national authorities before the ECtHR.[65] However, this does not seem to be a remedy which is going to provide early answers as regards the national laws implementing the DRD.

Although all these options are available, the current political and legal scenario seems to indicate that data retention is returning to national legislatures and governments. At European level, after the invalidation of the Directive, it has been uncertain

---

[61] European Parliament, Legal Opinion, 'Questions relating to the judgments of the Court of Justice of 1 April 2014 in Joined Cases C-293/12 and C/594/12, *Digital Rights Ireland* and *Seitlinger and others*–Directive 2006/24/EC on data retention–Consequences of the Judgment, SJ-0890/14 (22 December 2014), p. 19, available at www.statewatch.org.

[62] Press information available at http://country.eiu.com/article.aspx?articleid=711971855&Country=Austria&topic=Politics&subtopic=F_1 and also https://edri.org/edrigramnumber11-1data-retention-austria/.

[63] Boehm and Cole, *Data Retention after the Judgment*, above n. 60, at 56.

[64] See https://edri.org/romania-mandatory-prepaid-sim-registration-ruled-unconstitutional/ and also www.ccr.ro/noutati/COMUNICAT-DE-PRES-103.

[65] Boehm and Cole, *Data Retention after the Judgment*, above n. 60, at 52.

whether any new data retention legislation would have been proposed. The European Commission, at the plenary session of 16 April 2014, indicated that there would not be a replacement of the Directive in the short term. Elections have been held, and the new commissioner Mr Avramopoulos has taken office. Though the point was addressed during the hearing of the commissioner-designate before the European Parliament on 30 September 2014, Commissioner Avramopoulos stated that, in light of the strict parameters set by the CJEU, common rules would be needed.[66] After terrorist attacks at *Charlie Hebdo* in Paris[67] and in Belgium, it seemed that the debate on data retention in Brussels was revitalized. For example, in a document of the Counter-Terrorism Coordinator to the national delegations, it has been suggested that 'the Commission could be invited to present as soon as possible a new legislative proposal for data retention'.[68] However, this did not happen and more recently the Commission has ruled out presenting a new proposal on data retention.[69] Thus, conversely, it seems that the topic of data retention has been 're-nationalized'. However, even if Member States 'regained' their sovereignty on the matter, they are nevertheless bound by the general principles of EU law and the legacy of *Digital Rights Ireland* on the interpretation of fundamental rights is here to stay.

Having analysed the implications of the judgment in the Member States, and knowing that the exchange of information and data is still a topical issue also at EU level, the next section explores the meaning of the judgment for other EU law instruments.

5. *DIGITAL RIGHTS IRELAND* AND ITS CONSEQUENCES WITHIN THE EU LEGAL ORDER: REASONS FOR RE-THINKING THE EUROPEAN *PANOPTICON*?

Digital Rights Ireland, by outlawing mass surveillance against European citizens, also set clear parameters for the compliance of the data retention legislation with fundamental rights, specifying the European legislation in the domain. However, by doing so, it also defined limits that apply to other European instruments. This is especially interesting and topical because the EU has enacted, since 9/11 2001, an abundant proliferation of instruments which imply the collection, the storage and the exchange of personal data, including databases and other surveillance instruments.[70] Many of these instruments provide for the exchange of information with the United States and other third countries. Among the first reactions to the judgment of the Court, the European

---

[66] Available at www.europarl.europa.eu/EPRS/Commissioner_hearings/EPRS-Briefing-538935-Migration-Home-Affairs-FINAL.pdf.

[67] On 7 and 9 January 2015.

[68] Council of the European Union, Meeting Document DS 1035/15, 17 January 2015 LIMITE, p. 9. The document is available at www.statewatch.org.

[69] See the European Commission's Statement on National Data Retention Laws, Brussels, 16 September 2015, available at http://europa.eu/rapid/press-release_STATEMENT-15-5654_en.htm.

[70] Mitsilegas, *EU Criminal Law*, above n. 52, at 235.

Data Protection Supervisor (EDPS) recognized that '[t]he judgment also means that the EU should take a firm position in discussions with third countries, particularly the USA, on the access and use of communications data of EU residents'.[71]

The reasoning of the CJEU does not imply that any collection and storage of data as such is in violation of the essence of privacy. This means that the Court does not exclude per se the usefulness of data retention, a point that has been contested, since the beginning, by civil society and also by the EDPS. The DRD was declared void because it was in breach of proportionality: this means that the European legislator could adopt another legislation on data retention that would be in line with the limits specified and requirements set in *Digital Rights Ireland*.

These requirements, as indicated in the judgment are, that the Directive must lay down clear and precise rules governing its scope and application; it must provide minimum safeguards to protect personal data against abuse, and clear safeguards against unlawful access to data; the need for such rules is even greater in case of automated processing of personal data and where there is significant risk of unlawful access to those data; there should be differentiation of retention regimes in light of the objective of fighting against serious crime; the collection of personal data must be limited, in terms of authorized period of retention, geographical area and/or to persons likely to be involved in particularly serious crimes.

Another set of requirements concerns the access of law enforcement authorities to data when use should be limited and constrained by substantive and procedural conditions. The Directive should lay down objective criteria by which the number of persons authorized to access and subsequently use the data retained is limited. Furthermore, there should be an instance of prior review by a court or independent administrative body, whose decisions may limit the access to data and their use to what is strictly necessary for the purpose of attaining the objective (strict legality scrutiny), and which may intervene following a reasoned request of the authorities involved in the process of prevention and detection of crime (in connection with an investigation into a crime). Another requirement derived from the reasoning of the Court is that a distinction has to be made between different categories of data, on the basis of their possible usefulness for the purposes pursued or on the basis of the persons concerned. The Directive should link the determination of the period of retention to objective criteria in order to ensure that retention is limited to what is strictly necessary.[72]

Additional limitations come from the fundamental right to data protection, which entails safeguards against the risk of abuse and against any unlawful access to and use of data. This is necessary because of the vast quantity of data, the sensitive nature of the same and the risk of unlawful access, which requires guarantees of the protection and security of such data, in order to ensure their full integrity and confidentiality. Furthermore, the data must be retained exclusively within the EU, in order to ensure that the control provided for in Article 8(3) Charter (control by an independent

---

[71] European Data Protection Supervisor, 'Press Statement: The CJEU Rules that Data Retention Directive is Invalid', 8 April 2014, available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2014/14-04-08_Press_statement_DRD_EN.pdf.

[72] *Digital Rights Ireland*, above n. 8, Judgment, paras 63–4.

authority) is established. The Directive should lay down precise and clear rules governing the extent of the interference with the fundamental rights to privacy and data protection, in compliance with the strict legality principle.

To sum up, the core meaning of the *Digital Rights Ireland* judgment is to outlaw generalized mass surveillance as in breach of EU fundamental rights. The question remains what are the consequences of *Digital Rights Ireland* within the EU's legal order, with special attention to the many instruments that provide for the collection and storage of personal data.

There is a broad range of instruments for which *Digital Rights Ireland* may have consequences. On the one hand, we have internal EU instruments, and on the other hand, we have external agreements, providing for the extensive storage of personal data of persons not suspected of having committed any crime whatsoever.

First of all, we should consider the PNR (passenger name record) systems, including the PNR agreements between the EU-United States, EU-Canada and EU-Australia. In addition to those agreements, the EU has had a proposal for a EU PNR Directive on the table since 2011, with a complex and difficult gestation. Though an analysis of the meaning and purpose of the PNR systems is outside the scope of this chapter, it is worth mentioning here that the EU PNR Directive present several similarities with the DRD, as it enables the massive storage of data referring to persons not suspected of any crime. Commentators have already expressed their concern over the compliance of the PNR systems with *Digital Rights Ireland*, for the same reasons that motivated the CJEU to strike down the DRD.[73]

To mention only some of the issues with PNR, there is systematic and indiscriminate storage and analysis of data of non-suspicious persons; independent oversight is not guaranteed; and a link between the data stored and a threat to public security is also missing. In the latest EU-United States PNR agreement, for example, there is quite a broad interpretation and formulation of crimes enabling the collection of PNR: these include terrorism and related crimes as well as other crimes punishable by a sentence of imprisonment of at least three years which are transnational in nature. There are reasons to question whether the criterion of clear and precise rules governing the scope and application of the measure in question is being met. As regards other aspects, the retention period in the EU-United States PNR agreement is especially long, five years in relation to an 'active' database, and up to 10 years in relation to a 'dormant' database, from which data can however be 're-personalized' in connection with law enforcement operations. The agreement makes no distinction between categories of data, nor according to the persons concerned, as required by *Digital Rights Ireland*. The definition of data-sets is also very broad and not connected with a threat to public

[73] See E. Brouwer, *Ignoring Dissent and Legality: The EU's Proposal to Share the Personal Information of All Passengers*, CEPS Papers in Liberty and Security in Europe (Centre for European Policy Studies, Brussels, 2011); see also the Opinion of the FRA on the Proposal for a Directive on the use of Passenger Name Record (PNR) data, Opinion no. 1/2011, available at http://fra.europa.eu/sites/default/files/fra_uploads/1786-FRA-PNR-Opinion-2011_EN.pdf; 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 Paper No. 65 (29 May 2014), available at www.ceps.eu; Boehm and Cole, *Data Retention after the Judgment*, above n. 60, at 58–71.

security, as required by *Digital Rights Ireland*. According to the *Digital Rights Ireland* criteria, the safeguards provided for should enable an individual to challenge the illegitimate use of data. The EU-United States PNR agreement, it has been observed, refers to US laws, thus making the practical enforcement of remedies in the United States for European citizens rather difficult.[74]

However, it is on the Safe Harbour Scheme that *Digital Rights Ireland* has already displayed some 'extra-territorial effects.'[75] The Safe Harbour Scheme or Decision (SHD), adopted under Commission Decision 2000/520/EC, is the consequence of the fact that the United States do not fulfil the requirement for an adequate level of protection, provided for by the Data Protection Directive (articles 25 and 26). The SHD sets out a framework of data protection standards which allow the free flow of personal data from EEA data controllers to the US organizations part of the scheme. It means that some US companies (part of the scheme) are deemed to provide an adequate level of protection that satisfies EU standards, reducing the administrative burden on American companies doing business with Europe. The Decision enabled important trans-border data flows, relying basically on (US) self-regulation in a field regulated in Europe by provisions concerning the protection of fundamental rights.[76]

After Snowden's revelations regarding the NSA PRISM surveillance program, involving also companies certified under the SHD, it became questionable whether the Safe Harbour was still fulfilling its aims, considering the amount of data of European citizens made accessible to US NSA. The European Parliament asked the Commission to propose a revision of the scheme, and the negotiations on a new EU-US Umbrella Agreement are at the final stage.

In the meantime, a privacy activist, Max Schrems, contested the validity of the Safe Harbour Scheme in light of Snowden's revelations regarding US surveillance for violation of the privacy, data protection and effective legal protection rights, enshrined in the Charter (Articles 7, 8 and 47) and the Court declared the SHD invalid in a request for preliminary reference raised by the Irish High Court. In its judgment of 6 October 2015, the Court also stressed the role of national supervisory authorities as the first controllers on the adequacy of the level of protection of the transfer of data protection, implying that a scheme such as the Safe Harbour does not prevent them from scrutinizing such a claim. However, the heart of the judgment is the declaration of invalidity of the whole SHD and the motivation of the Court relies greatly on the requirements of *Digital Rights Ireland*. In particular, the Court recalls that for the transfer of data outside the EU, 'the third country must in fact ensure, by reasons of its domestic law or international commitments, a level of protection of fundamental rights

---

[74] Boehm and Cole, *Data Retention after the Judgment*, above n. 60, at 65.

[75] At the time of writing, judgment in *Maximilian Schrems (Europe* v. *Facebook)* has been delivered (C-362/14 *Maximillian Schrems* v. *Data Protection Commissioner*, Grand Chamber, Judgment of 6 October 2015). While a thorough discussion of the case is not possible, the chapter will nevertheless take into account its main significance.

[76] The Decision is based on Safe Harbour Privacy Principles and Frequently Asked Questions. A company wanting to join the scheme must, first, prove that it adheres to the Principles in its publicly available privacy policy and, secondly, self-certify to the US Department of Commerce that it is in compliance with the Principles.

and freedoms that is essentially equivalent to that guaranteed within the EU'.[77] Together with an adequate level of protection, the transfer must be granted by effective means of protection. Therein, the Commission has reduced discretion when assessing the adequacy of the level of protection ensured by a third country.[78] One of the main problems of the Safe Harbour is that (Article 1) companies under the scheme are also subject to US law, which has primacy on the principles of the SHD. Secondly, US public authorities are not required to comply with it. This entails that the principles of *Digital Rights Ireland* on the limitation of interference with the fundamental right to respect of private life, are not satisfied. For these reasons, the SHD is invalid because, under it, mass transfer of data of individuals is possible, without compliance with the data protection and privacy provisions. In addition, the Decision also limits the powers of national supervisory authorities.

Schrems should be read in the perspective of the *Digital Rights Ireland* judgment, which outlawed mass surveillance deprived of adequate guarantees within the EU. The transfer of European 'data subjects' to US companies cannot follow a different path. This case offers a good example that the *Digital Rights Ireland* judgment is displaying some effects beyond the borders of the EU.

Another interesting question concerns the implications of *Digital Rights Ireland* on 'European' databases. This refers to the Visa Information System (VIS), to EURODAC, but more recently also to the so-called Smart Borders Package (Entry-Exit System – EES – and Registered Travellers Program – RTP). Under the EES, a significant amount of personal data of third country nationals is collected and stored without any connection to criminal activities. These databases provide an interesting case: often they have been set up for a specific reason, and then later on, law enforcement authorities have been granted access to them. The case of the Entry-Exit System of the Smart Borders package is illustrative: the technical design of the system was conceived from the beginning not according to the criterion of privacy-by-design but in order to enable, in the future, access to be granted to law enforcement authorities.[79]

In another perspective, *Digital Rights Ireland* is of paramount importance also for Internet law, welcomed as 'the most significant legal opinion from any court in the world on the risks of big data and on the ongoing importance of privacy protection'.[80] Read together with the judgment in *Google Spain*, mentioned above, the CJEU has released two important judgments on data protection and privacy in the governance of the Internet. These judgments aim to create a level playing field for Internet operators, and will provide guarantees and limitations of crucial importance in light of the development of cloud computing and of 'big data'.[81] As stated by the newly appointed

---

[77] *Schrems*, above n. 75, para. 73.

[78] *Ibid.* para. 78.

[79] See *Note of the Meijers Committee on the Smart Borders Proposals (COM(2013)95 final, COM(2013)96 final and COM(2013)97 final)*, CM1307 (3 May 2013), available at www.commissie-meijers.nl/assets/commissiemeijers/CM1307%20Note%20Meijers%20Committee%20on%20the%20Smart%20Borders%20proposals.pdf.

[80] See www.epic.org.

[81] Guild and Carrera, *The Political and Judicial Life of Metadata*, above n. 73, at 11–12.

EDPS chairman, Giovanni Buttarelli, the advent of 'big data' requires 'big rights'.[82] And by limiting access by law enforcement authorities through respect for the principle of legality, the governance of the Internet is definitely more strongly embedded in the principles of the rule of law.

All in all, there are reasons to conclude that *Digital Rights Ireland* has marked an important development on privacy, data protection and proportionality in delimiting the enjoyment of fundamental rights falling within the scope of EU law. The Commission, Council and Parliament are all aware of this judgment, and will without doubt have to take it into consideration in designing new instruments affecting such core fundamental rights of the EU citizens.

6. CONCLUSIONS: *DIGITAL RIGHTS IRELAND* IN THE PERSPECTIVE OF THE TRANS-ATLANTIC DIALOGUE

Digital Rights Ireland is a landmark judgment in EU law. It is the first time that the CJEU has completely annulled a European Directive for breach of fundamental rights (in the previous *Test-Achats* case, the Court decided only on a partial annulment).[83] This chapter has aimed to highlight some of its consequences: first, on Member States' legal orders, where legislation implementing *Digital Rights Ireland* might be in compliance (or not) with the limitations and requirements specified by the Court on the basis of the Charter of Fundamental Rights, but also on the basis of the secondary law in the domain, i.e., the DPD and the e-Privacy Directive, the cornerstones of data protection in EU law, prior to the Charter. Secondly, it has described the deep seismic waves created by *Digital Rights Ireland* on other instruments and databases which allow indiscriminate mass collection and storage of personal data, suggesting how the recent *Schrems* judgment invalidating the Safe Harbour Scheme demonstrates how *Digital Rights Ireland* is already creating extra-territorial consequences. The CJEU has taken a critical stance on the DRD and assessed it as a disproportionate invasion into the privacy of individuals. For this reason, *Digital Rights Ireland* can be placed next to *Kadi*. In this perspective, *Digital Rights Ireland* is a new step in the process of

---

[82] 'In a nutshell, big data needs equally big data protection solutions … We don't need to reinvent data protection principles, but we do need to "go digital". We need innovative thinking.' This is a quote from Giovanni Búttarelli, the new European Data Protection Supervisor, from his speech 'Our World in 2015' of 5 January 2015, available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2015/15-01-14_Article_NE_GB_EN.pdf.

[83] According to Craig and De Búrca there are not many successful challenges to the EU legislation on the basis of fundamental rights. For example, in the Dutch case challenging the legality of the Biotechnology Directive 98/44/EC (C-377/98 *Netherlands* v. *Council and Parliament* [2001] ECR I-7079) arguing that the patentability of isolated parts of the body violated the right to human dignity and to human integrity, the CJEU found that human dignity and human integrity were respected, dismissing the claims. Another technique consists in suggesting that Member States had enough margin of appreciation in order to implement the Directive in a way complying with fundamental rights. See P. Craig and G. De Búrca, *EU Law: Text, Cases and Materials* (OUP, 2011), pp. 390–1.

reconciling anti-terrorism legislation with the principles of the rule of law, which is at the heart of European constitutionalism. It is an attempt to turn a page of the history of trans-Atlantic relations, marked by a resort to policies and instruments under the claim of a 'state of exception'. Unfortunately, the EU has often been not capable of reacting to or contradicting the ideas and plans developed by the United States, and therefore, too often has agreed to, or at least acquiesced in, the pressure received from the United States in the name of the fight against terrorism.[84] *Digital Rights Ireland* is a clear step in the direction of consolidating European values and stating them also in the relations between the EU and United States.

[84] M. de Goede, 'Beyond Risk: Premediation and the Post-9/11 Security Imagination' (2008) 39(2–3) *Security Dialogue* 155.