5

Mass Surveillance and Data Protection in EU Law – The Data Retention Directive Saga

THEODORE KONSTADINIDES*

1 Introduction

Mass surveillance in the European Union (EU) through the so-called Data Retention Directive (2006/24/EC) has been subject to intense controversy in the Member States. This chapter examines the contribution of the CJEU in unpacking the constitutional and human rights implications arising out of the retention of private data for the purpose of law enforcement. In spite of intense litigation, this chapter argues that the CJEU has not yet had the opportunity to rule on a number of essential constitutional and human rights questions related to the disproportionate invasion of the Directive on the right to privacy. The chapter commences with an account of how the Directive came into being as well as the main challenges met by the EU legislature in the process of adopting it. It then moves on to consider how the CJEU has defended the Directive in relevant cases regarding its interpretation or validity. The CJEU has so far dealt with the legal basis / competence aspect of the Directive. Although unconvincing, the CJEU's rationale for far-reaching supranational action in the field of criminal justice has been endorsed by the Treaty of Lisbon.

To use a colloquialism often employed by EU lawyers, the Communitarisation of what used to be the Third EU Pillar seems to have washed away any hanging questions with regard to the criminal justice spillover effect of internal market legislation. In light of this change, the main argument against Directive 2006/24/EC remains that the smooth functioning of the internal market and maintenance of internal security cannot compromise the fundamental right to privacy and the rule of law – i.e. the values on which the EU is founded. However, the CJEU has not yet had the opportunity to rule on the encroaching impact of EU harmonisation legislation on digital civil liberties. The uniform retention of communication and location data throughout the EU has further raised questions on the dubious limits of EU regulation upon the conduct of

* School of Law, University of Surrey. The author would like to thank Maria Bergström for her helpful suggestions. All errors are obviously entirely mine.

public enforcement authorities and private market actors through a mandatory data retention law. Hence, it is argued that the above questions exposed in recent litigation have not yet been properly addressed by the CJEU. It is further suggested that the CJEU's jurisprudence does not imply that a set of strict criteria for justifying non-consensual, blanket and indiscriminate retention and therefore interference with a person's right to privacy have been established.

2 The adoption of Directive 2006/24/EC

The Data Retention Directive (2006/24/EC), which provides for *a priori* mandatory storage by a state and/or exchange between Member States of telecommunications traffic and location data (i.e. data generated in the ordinary course of service - excluding content),[1] has been in force since 2007. The Directive requires telephone and Internet service providers to retain details of Internet and call data for not less than six months and not more than two years, in order to ensure that the data is available for the purpose of the investigation, detection and prosecution of serious crime. The overall implementation of the Directive in the Member States has been well overdue. Although all Member States have either formally implemented the Directive or have made a start at doing so, effective transposition across the EU is far from reality. The Commission has initiated infringement proceedings under Article 258 TFEU against a number of Member States including those, such as Germany and Romania, that originally transposed the Directive into national law, but whose constitutional courts later ruled that such legislation was unconstitutional.[2] The Commission has also handed down an Article 260 TFEU judgment against Sweden (examined later in this chapter)[3] and is expected to do the same against Germany.[4] Ineffective transposition of the Directive owes to the diversity of practice and difference of opinion between Member States on issues such as the duration and purpose of data retention, the procedures regulating access to personal data; and the cost of data retention for economic operators. The purpose of this section is to reveal the legal uncertainties that were somewhat disregarded

[1] This is taken to mean the source of a communication as well as its destination. It includes the telephone number and the subscriber's name and address as well as the number(s) called (telecommunications) and the user's ID and name and address of the subscriber or registered user (Internet). The duration of the communication and geographical location of the equipment used is also included in the retained data.

[2] See for instance the German Data Retention Judgment, BVerfG, 2 BvE 2/08 of 30.06.2009, Absatz-Nr. (1-421) and the Romanian Data Retention Judgment, Decision no.1258 of 8.10.2009, Official Gazette no.798 of 3.11.2009. See also for more details on national implementation: European Commission, 'Evaluation report on the Data Retention Directive (Directive 2006/24/EC)', 18.4.2011, COM (2011) 225 final. What is more, an up-to-date table of the infringement actions taken by the Commission against the Member States for failure to implement the Directive is available at:
<http://ec.europa.eu/home-affairs/news/infringements/infringements_by_policy_police_co-operation_and_access_to_information_en.htm>

[3] Case C-270/11, *Commission v. Sweden* [2011] OJ C 226/33.

[4] See Reuters, 'EU to take hard line on German resistance to data storage', 29 May 2012. Available at < http://www.reuters.com/article/2012/05/29/eu-dataprivacy-idUSL5E8GTE4C20120529>

during the drafting process of the Directive. This analysis will serve to explain why the Directive has been the subject of intense litigation before the CJEU.

The Data Retention Directive is the misshapen child of the aftermath of the London terrorist attacks in 2005, where it was commonly agreed between Member States that increased control over telecommunications is essential in order to investigate and prosecute terrorism and organised crime. Despite the strong political will of the governments of the Member States in favour of the establishment of EU surveillance tools, there was a significant gap in both national and EU legislation vis-à-vis data retention. Traffic data was either not stored systematically in the Member States or merely stored for billing purposes and in order to settle customer disputes. In some Member States, however, such data was not stored at all. As such, traffic data was not always available for public enforcement authorities to use against criminals for anti-terrorism purposes. Hence, following the Brussels EU Summit of 25 and 26 March 2004,[5] a group of four Member States[6] presented a Draft Framework Decision to be adopted under the former Third Pillar as a criminal law measure. It is noteworthy that Sweden was one of the states that helped put forward the proposal and made an argument about extending the scope of data retention beyond judicial cooperation to all kinds of police cooperation. The Draft Framework Decision proposed a retention period between twelve to thirty-six months depending on the value of the data in relation to countering crime and the cost of retention.[7] Finally, the Commission decided that in tune with ex Article 47 TEU (now Article 40 TEU)[8] the harmonisation of retention periods across the EU and exchange of traffic data by law enforcement authorities should be adopted under the former First Pillar. A Directive was thus considered as the most appropriate EU legislative instrument to regulate the obligation on providers of electronic communication services to retain their subscribers' telephone and Internet data. Indeed, a Directive is less stringent compared to a Regulation and it allows considerable room for implementation manoeuvre to national governments vis-à-

[5] See the Declaration on Combating Terrorism adopted by the European Council on 25 March 2004, Presidency Conclusions available at:
<www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/ec/79696.pdf>; See also

[6] The proposal was presented by France, Ireland, Sweden and the UK.

[7] Council of the European Union, 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, Brussels, 2 April 2004. Available at
<http://register.consilium.eu.int/pdf/en/04/st08/st08958.en04.pdf>
The Draft mentioned that under Article 15 of Directive 2002/58/EC the EU could adopt secondary legislation on data retention for the purposes of the prevention, investigation, detection or prosecution of crime. The Framework Decision, however, was not designed to achieve other Article 15 objectives – such as provide for data retention rules in order to safeguard national security, defence and public security.

[8] Former Article 47 TEU regulated the relationship between the Treaty on European Union (TEU) and the EC Treaty stipulating that no legal instruments adopted under the TEU may affect the legislative framework adopted under the EC Treaty.

vis the appropriate public authorities to have access to the retained data.[9] According to Recital 5 of the Preamble to Directive 2006/24/EC, different requirements and technical differences between national provisions concerning data retention presented obstacles to the internal market and were to be harmonised. Moreover, the Commission set the time limit for the cross availability of data to a period between six months and two years from the date of communication.

The inception and adoption of the Data Retention Directive constitutes a pre-Lisbon example of cross-EU pillar interaction. In this case, a proposal for a Framework Decision by certain Member States inspired the Commission to put forward a proposal for a Directive. This is reminiscent of pre-Lisbon examples which demonstrate temporary synergy between the former EU pillars. For instance, with reference to the ship-source solution, while Directive 2005/35/EC ensured that polluters would be liable to criminal penalties in order to improve maritime safety, Framework Decision 2005/667/JHA contained the nature, types and levels of such penalties as a means of supplementing the Directive. The Framework Decision was, however, annulled by the CJEU which held that Articles 1 to 7 had as their main purpose the protection of the environment and, as such, they could have been properly adopted by using a former First Pillar legal basis (ex Article 175 EC – now Article 192 TFEU). Thus, similar to the Data Retention Directive, in the case of ship source pollution, a Directive was proposed on 13 March 2001 for the protection of the environment through criminal law. This is now Directive 2008/99/EC adopted on 19 November 2008.[10]

To return to our analysis on data retention, it needs to be stressed that had Directive 2006/24/EC been adopted now, the Commission would have most likely resorted to Article 83 TFEU as its legal basis. One should also note that the Treaty of Lisbon provides for a separate legal basis in the form of Article 16(2) TFEU, which is specific for the adoption of rules relating to the protection of individuals with regard to the processing of personal data by EU institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of EU law, and the rules relating to the free movement of such data.[11] Back in 2005, however, the Commission had to justify the appropriateness of using a Directive (a First Pillar instrument) as a means of obliging Member States to establish a system for retaining communications data in order to tackle serious crime (a Third Pillar objective). In other words, the Commission had to find a 'market' angle. Hence, the argument was that diverse

[9] Commission Proposal for a Directive on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, Brussels, 21.09.2005, COM (2005) 438 final.

[10] Directive 2008/99/EC on the protection of the environment through criminal law [2008] OJ L 328/28.

[11] See the Commission's Proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, Brussels, 25.01.2012, COM (2012) 10 final.

regulatory and technical national provisions concerning the retention of traffic data subjected service providers to different requirements regarding the types of data to be retained and the conditions of retention. In light of this argument, a Directive on Data Retention was regarded necessary in order to bring down the internal market obstacles caused by such legal diversity in the Member States. It was, therefore, adopted under the legal basis of current Article 114 TFEU, the basis for harmonisation measures for the internal market. To avoid criticism, the Commission noted that data retention had constituted the subject matter of previous legislative instruments based on the former First Pillar, in particular Directives 2002/58/EC and 95/46/EC.[12]

With reference to the protection of fundamental rights, the Commission recognised the Directive's impact upon the privacy right of citizens as guaranteed under Articles 7 (private and family life) and 8 (protection of personal data) of the EU Charter of Fundamental Rights proclaimed and signed in 2000.[13] According to Article 6 (1) TEU, the Charter is legally binding and can be invoked as a guarantee of justice and constitutional recognition of the right to data protection. This is all the more important since the right to protection of personal data included in Article 8 of the Charter is unique and has no equivalent in the ECHR. Yet, the rights guaranteed by the Charter are not unconditional. Article 52 of the Charter provides justification for interference with the right to privacy and protection of personal data. According to Article 52 (1) of the Charter, '[s]ubject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.' Article 52 of the Charter, therefore, sets the (limited) scope of the right to respect private and family life and the right to the protection of personal data.

Indeed, the cross-border nature of organised crime and terrorism and the fact that Directive 2006/24/EC only deals with the processing of traffic data by service providers and not their content was considered enough evidence by the EU legislature that the principles of subsidiarity and proportionality had been complied with.[14] The Commission stressed that limitations to privacy and the protection of personal data are proportionate and necessary to meet the objectives of countering serious crime and terrorism. As a result, no general provisions were proposed or adopted by the EU legislature vis-à-vis the safeguarding of the retention of communications data from potential abuses. This was the case especially since, according to the EU legislature, relevant data protection provisions were inherent in previous EU Directives.[15] Despite criticism by the

[12] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201/37; 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 L 281/31.

[13] The text of the Charter was not given full legal effect until 1 December 2009, as part of the Lisbon Treaty.

[14] This was stressed in the Preamble of the Directive (para 21).

[15] See Directives 95/46/EC and 2002/58/EC (see above).

European Data Protection Supervisor (EDPS) and the European Economic and Social Committee (EESC) that a mere reference to the existing legal framework on data protection was insufficient to satisfy the intrusive character of the Directive,[16] the EU legislature adopted a rather 'flimsy' and 'flawed' human rights test to ensure full compliance with citizens' fundamental rights as enshrined in Articles 7 and 8 of the Charter.[17] Directive 2006/24/EC was therefore adopted on 15 March 2006 and entered into force on 4 May 2006[18] with only two Member States voting against it in the Council - Ireland and the Slovak Republic.

3 The CJEU's response to challenges against the Directive

As the above discussion illustrates, the Data Retention Directive appeared irreconcilable with both EU and national law. First, in the pre-Lisbon pillarised system, it was hard to see how the Directive's centre of gravity concerned the functioning of the internal market and not public safety and crime prevention. Second, the Directive raised concerns with regard to the extent of the interference with individual privacy rights protected by EU law, the ECHR and national constitutions. This section will look into the two challenges that have taken place against the Directive: a direct challenge on the correctness of its legal basis and an indirect one on its compatibility with fundamental rights. The CJEU has, so far, only dealt with the procedural/ legal basis aspect of the Directive in *Ireland v. Parliament and Council*.[19] In this case, Ireland brought an action under Article 263 TFEU before the CJEU seeking the Directive's annulment. With reference to the validity of Directive 2006/24/EC vis-à-vis its fundamental rights compatibility, in an action brought by the civil rights advocacy group Digital Rights Ireland (DRI) against the relevant Minister for Communications, the Irish High Court decided to request under Article 267 TFEU a preliminary ruling from the CJEU. Both challenges will be considered in turn hereafter.

Looking back at the first challenge against the Directive in *Ireland v. Parliament and Council* one may conclude that it was a wasted opportunity. This is because Ireland that brought action against the EU legislature based its case solely on the grounds that the Directive had not been adopted on an appropriate

[16] Opinion of the European Data Protection Supervisor 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, 26.09.2005, COM (2005) 438 final.

[17] Opinion of the European Economic and Social Committee 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, COM (2005) 438 final - 2005/0182 (COD).

[18] Directive 2006/24/EC 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 L 105/54.

[19] Case C-301/06, Ireland v. European Parliament and European Council [2009] ECR I-593.

legal basis - i.e. that it should have been adopted under a legal basis stemming from the 'Third' rather than the 'First' Pillar (i.e. not the internal market provision of Article 114 TFEU).[20] Staying faithful to its *tobacco saga* judgments, in particular, its *BAT dicta*[21] the CJEU held once again in favour of Article 114 TFEU. The CJEU also resorted to the 'preference clause' of former Article 47 TEU (current Article 40 TEU) as a means of determining the threshold for connecting a particular measure with the internal market.[22] It was rather revealing at the time that the CJEU approved the indirect approximation of criminal law through internal market legislation. Yet, this aspect of the judgment has evaporated post-Lisbon given that the EC-EU dichotomy has ceased to exist and the field of judicial cooperation in criminal matters has become a fully-fledged EU policy. Indeed, under the current Title V of the TFEU, future measures in the area of police and judicial cooperation in criminal matters will take the form of Regulations and Directives adopted under the ordinary legislative procedure.

The CJEU's decision in *Ireland v. Parliament and Council* contains elements of both fundamental rights enhancement and human rights restraint. On the one hand, Ireland's defeat before the CJEU meant that the Irish government could no longer afford to maintain a three-year retention period for telephone data under section 63(1) of the Criminal Justice (Terrorist Offences) Act 2005, which was significantly longer to the one suggested by Article 6 of the Directive (six months and two years respectively). On the other hand, however, the Communications (Retention of Data) Act 2011 - which transposed Directive 2006/24/EC into national legislation - requires Internet service providers to retain Internet data, previously not required by Irish law to be monitored or retained. This brings us to the second challenge against the Directive on fundamental rights grounds. The seeds to this challenge against the Directive before the CJEU were planted in 2009, almost at the same time that the Irish government sought to annul the Data Retention Directive on procedural grounds. It is also worth noting that there was a parallel legal universe behind these challenges as in November 2009 the CJEU delivered a judgment against Ireland following an Article 258 TFEU action taken by the Commission for failure to transpose the Directive within the prescribed period.[23]

---

[20] The legal grounds for the choice of Article 114 TFEU as the legal basis for Directive 2006/24/EC had also been disputed in 2006 by the Land of Schleswig-Holstein (Germany) which successfully requested full access to internal Commission documents related to using Article 114 TFEU as the legal basis for the Directive. See Case C-406/06, *Landtag Schleswig-Holstein v. Commission of the European Communities* [2006] OJ L 105/54.

[21] Case C-491/01, *R v. Secretary of State ex p BAT and Imperial Tobacco* [2002] ECR I-11453. See especially para 62: '….provided that the conditions for recourse to Article 95 EC as a legal basis are fulfilled, the Community legislature cannot be prevented from relying on that legal basis on the grounds that public health protection is a decisive factor in the choices to be made…'

[22] See for further analysis T. Konstadinides, 'Wavering between Centres of Gravity: Comment on *Ireland v. Parliament and Council*' (2010) 35 *European Law Review* 88; E. Herlin-Karnell, 'Annotation of *Ireland v. Parliament and Council*' (2009) 46 *Common Market Law Review* 1667.

[23] Case C-202/09, *Commission v. Ireland* [2009] OJ C 167.

As mentioned earlier, in the second (human rights) challenge against the Directive, Digital Rights Ireland (DRI) brought a case before the High Court of Ireland against the Minister for Communications.[24] DRI challenged the Communications (Retention of Data) Act 2011, in particular the extent to which the State can require telecommunications providers to retain and to provide to the State, data on how customers use their services. In May 2010, the High Court held that DRI had sufficient standing to challenge the Communications (Retention of Data) Act 2011 and agreed to make a preliminary reference to the CJEU on the validity of Directive 2006/24/EC vis-à-vis its compatibility with the right to privacy.[25] At the request of the Irish Human Rights Commission (IHRC),[26] the High Court also sought guidance from the CJEU on whether national transposition legislation of an EU Directive must be in compliance with the human rights standards set out in the EU Charter of Fundamental Rights in order to be compatible with EU law. In August 2012, the High Court made a reference for a preliminary ruling seeking interpretation of Articles 3,4, and 6 of Directive 2006/24/EC vis-à-vis their compatibility with Articles 7,8, 11 and 41 of the EU Charter of Fundamental Rights[27]

Let us now make some speculations about how the CJEU may approach the *DRI* case. One would agree that the first High Court's question regarding the compatibility of the Directive with the right to privacy was a matter of balancing necessity with proportionality. The CJEU may probably avoid engaging in a human rights discussion. Similar to *Ireland v. Parliament and Council* the CJEU may point out that Directive 2006/24 only goes as far as harmonising the obligations of providers of publicly available electronic communications to retain individual data for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. As such, the retained data shall be disclosed to the relevant public enforcement authorities in accordance with the national laws of each Member State. One could argue that this would not be the first time the CJEU adopted far-reaching legislation and subsequently left it to the Member States to determine the practicalities vis-à-vis the level of intrusiveness with regard to fundamental rights. The CJEU took a similar stance in *Advocaten voor de Wereld* on the definitions of the extraditable offences listed in the Framework Decision on the European Arrest Warrant (EAW).[28] It merely left the formulation of definitions of all-encompassing crimes such as terrorism and computer crime, to name but a few, to the competent authorities of the Member States. Of course the same could happen with

[24] *DRI v. Minister for Communications et al*, Irish High Court, 5 May 2010, [2010] IEHC 221. Available at: <http://www.bailii.org/ie/cases/IEHC/2010/H221.html>

[25] At the time of writing (May 2012) there is no numerical reference or evidence on the CJEU's website that a preliminary reference has been made and that there is currently a ruling pending by the CJEU.

[26] The IHRC appeared as *amicus curiae* in the DRI case before the High Court.

[27] Case C-293/12, *DRI v Minister for Communications et al.* The preliminary reference was made on 10/08/2012.
See: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:258:0011:0011:EN:PDF>

[28] Case C-303/05, *Advocaten voor de Wereld* [2007] ECR I-03633. See also a case note by F. Geyer (2008) 4 *European Constitutional Law Review* 149.

reference to Article 1 of the Data Retention Directive in relation to 'serious crime' which is not defined at EU level.[29]

Advocaten voor de Wereld consists of the first national challenge against the Framework Decision on the European Arrest Warrant (EAW). The case explored the practical consequences stemming from the application of the principle of mutual recognition in criminal matters vis-à-vis the conformity of the abolition of the principle of double criminality with the principle of legality. The CJEU stressed that because harmonisation of national criminal law is not a precondition for the application of the EAW, the absence of definitions for the thirty-two listed offences in Article 2 (2) of the Framework Decision does not imply an inconsistency with the principles of equality and legality in criminal proceedings. The CJEU emphasised that whilst the EAW determines the scope of a procedural rule (the condition for surrendering criminals), it leaves it to the Member States to both define the extraditable offences listed in the EAW and provide for the appropriate penalties. As such, the CJEU held that the EAW is compatible with fundamental rights. The aftermath of *Advocaten* suggested a certain inconsistency deriving from the hesitation on the part of the EU institutions to address issues that are not raised in secondary legislation. It also unveiled the national courts' disinclination to question the protection of fundamental rights in EU law beyond a selfish critique related to the constitutional safeguards against the application of EU legislation upon their own nationals.

The case of data retention is different to extradition. The hesitation of the EU institutions to address the right to privacy owes to the fact that the Directive does not contain any rules governing the activities of public authorities for law enforcement purposes.[30] Perhaps the CJEU had a point in *Ireland v. Parliament and Council* not to delve into a human rights discussion. Had the Directive contained a detailed system of data access and safeguards it would have been encroaching into the activities of the State in areas of criminal law and it would have had to be struck down as *ultra vires*. The *Passenger Name Records (PNR)* dicta is indicative of the thin red line that lies between EU legislation on data processing for a supply of services (*intra vires*) and data processing for safeguarding public security (*ultra vires*).[31] In the *PNR* case, a Decision adopted under Article 114 TFEU enabling the transfer of air passenger name records from the EU to the US Bureau of Customs and Border Protection was annulled. The CJEU held that the internal market measure of Article 114 TFEU could not justify EU competence to conclude an agreement with the United States on data processing for law enforcement purposes. Setting the *PNR* case aside, following the coming into force of the Treaty of Lisbon, a new proposal for a Directive was put forward under Title V of the TFEU for establishing an EU-wide framework governing the collection, retention and use of PNR data - allowing Member

[29] See Joint Statement by the Council and the Commission in relation to Art. 12 Evaluation of the Draft Directive, 5888/06 ADD1, 10.02.2006.
[30] Case C-301/06, Ireland v. Parliament and Council, paras 86-92.
[31] Joined cases C-317/04 and C-318/04, *European Parliament v. Council and Commission* [2006] ECR I-04721.

States to collect PNR data from intra-EU flights in order to counter terrorism and serious crime.[32] What is more, in April 2012, the European Parliament approved a new EU-US PNR deal which allows US authorities to retain PNR data for up to five years.[33] It is argued that these developments will generate further litigation with reference to the scope of privacy rights in EU law.

As the present author has explored in a different paper, the Data Retention Directive was further fuelled during 2008-2010 by a number of constitutionality claims before the courts of the Member States.[34] The transposition saga of Directive 2006/24/EC reveals that national courts have been reticent to question the protection of fundamental rights in EU law. They have merely resorted to an esoteric criticism of the constitutional safeguards against the right to privacy available in the national constitutions they defend and uphold. In light of these developments one may ask whether the EU Charter of Fundamental Rights is likely to raise the threshold of human rights in EU law and help enhance the external scrutiny of EU legislation. Indeed, as pointed out earlier, post-2009 the Charter has become a formal source of EU law and comprises a standard of review for the validity of EU acts (Article 6 TEU). The case of *Schecke* forms an early example where the Charter was employed as a standard of review of the legality of EU secondary legislation on transparency laws in the management of Common Agricultural Policy (CAP) funding.[35] The judgment is relevant to the question of the legality of the Data Retention Directive since the main provisions invoked in *Schecke* were those on the protection of private life and personal data under Articles 7 and 8 of the Charter, as well as Article 8 of the ECHR.

The CJEU's decision in *Schecke* suggests that despite the limitations to the right to privacy vis-à-vis Article 52 (1) of the Charter, the threshold for allowing data retention in EU law is high. The role of the principle of proportionality is ever crucial. The CJEU interpreted the 'necessary' requirement in the challenged Directive to mean 'strictly necessary' in the context of disclosure of personal data. In light of *Schecke*, the Data Retention Directive may have to be weighed against its alleged impact on privacy, and its overall design regarding its necessity and proportionality. The CJEU's case law may further inform the second question addressed to the CJEU by the Irish High Court in the *DRI* case – i.e. whether national implementation legislation of an EU Directive must be in

[32] Proposal for a Directive of the Council and the European Parliament on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, 23 April 2012.
Available at <http://register.consilium.europa.eu/pdf/en/12/st08/st08916.en12.pdf>

[33] Council of the EU, 'Council adopts new EU-US agreement on Passenger Name Records (PNR)', Luxembourg, 26 April 2012, 9186/12 PRESSE 173.

[34] See for transposition problems related to Directive 2006/24/EC: T. Konstadinides, 'Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem' (2011) 36 (5) *European Law Review* 722-736.

[35] Joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen* [2010] OJ C 13/6. See for detail A-S. Lind & M. Strand, 'A New Proportionality Test for Fundamental Rights? The Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR* (C-92/09) and *Hartmut Eifert* (C-93/09) *v. Land Hessen'* SIEPS European Policy Analysis 2011:7epa. Available at <www.sieps.se/sites/default/files/2011_7epa.pdf>

compliance with the human rights standards set out in the Charter in order to be compatible with EU law. It is accepted that the Charter only binds EU institutions and Member States when they are implementing EU law. As such, the CJEU's reply will most likely be positive: Whilst EU institutions can be reviewed for compliance with the Charter, national governments may only be reviewed when they act within the scope of EU law or when they transpose EU legislation into domestic law. It follows that the Charter applies not only when Member States directly implement a Directive, but also when they choose to derogate from it. The CJEU will soon be called to determine the external boundaries of the Charter's application in light of two Austrian preliminary references made in 2013 to the CJEU on the compatibility of Directive 2006/24/EC with Articles 7,8 and 11 of the Charter.[36]

4 Letters from Sweden

One would agree that the much-loathed Data Retention Directive constitutes a radical step in fighting crime in the EU. At the same time, it is hard to dispute that the Directive endorses state interference with the right to private life. Whilst waiting for the CJEU's *DRI* preliminary ruling on the Directive's legality, this final section will attempt to review current litigation before the CJEU and demonstrate the legal problems that Sweden has been called to resolve with reference to the transposition and interpretation of the scope of Directive 2006/24/EC. The section begins by considering the relevant infringement proceedings against Sweden, the first Member State so far to have received a hefty fine for failing to implement the Directive within the prescribed period. It then moves on to discuss the recent case of *Bonnier Audio AB*, which arose from a preliminary reference made by the Swedish Supreme Court. The CJEU's judgment is most controversial in terms of 'floodgates opening' given that the Luxembourg Court did not exclude the extended use of Directive 2006/24/EC by Member States for any offence committed using telecom networks, including copyright infringements.

The EU adopted the Data Retention Directive in March 2006 and Member States were required to transpose it before 15 September 2007, with the option of postponing until 15 March 2009 the implementation of retention obligations relating to Internet data. Although most Member States have for some time operated a voluntary system of data retention of communications traffic data, they faced infringement proceedings by the Commission and were forced to

[36] See Case C-594/12, *Seitlinger*, Preliminary reference made by Austrian Federal Constitutional Court on 1 March 2013; Case C-46/13, *H*, Preliminary reference made by the Austrian Data Commission (*Datenschutzkommission*) on 28 January 2013. See for a critique of the Charter F. Fontanelli, The European Union's Charter of Fundamental Rights: Two Years Later', (2011) 3 (3) *Perspectives on Federalism*, Available at <www.on-federalism.eu/attachments/104_download.pdf >

adopt new legislation in light of the threat of further action.[37] In Sweden, the implementation of the Data Retention Directive has been delayed due to fundamental rights concerns. Sweden, which as mentioned earlier was initially in favour of Data Retention legislation, had a change of government in 2006, which resulted in minimal implementation of the Directive. The consequence of this was that in 2010, the Commission started infringement proceedings against Sweden under Article 258 TFEU and held that the government had failed to fulfil its obligations under the Directive.[38] This action was followed by further Commission proceedings against Sweden in May 2011 under Article 260 TFEU. This time the Commission claimed that under Article 260 (2) TFEU, Sweden should pay financial penalties due to its failure to comply with the CJEU's earlier judgment.[39] In particular, the Commission proposed that the CJEU imposes on Sweden a daily penalty payment of EUR 40,947.20 and a fixed daily amount of EUR 9,597 for each day that the necessary measures were not taken to implement the Directive. Almost a year later, the CJEU is still expected to rule on the case against Sweden. However, on 31 May 2012, in light of Sweden's full implementation of Directive 2006/24/EC, the Commission made a partial withdrawal of the case.[40] This effectively means that although the Commission decided to withdraw the daily penalty payment, it has maintained the request to the Swedish government to pay the lump sum. The aim of the lump sum in this case is to penalise the continuation of Sweden's infringement between the initial Article 258 TFEU judgment and the subsequent Article 260 TFEU judgment.

On top of the Commission's infringement proceedings related to the Directive's delayed implementation, Sweden has been confronted with yet another value judgment related to the interpretation of the Directive's scope with regard to who can have access to the retained data and the purpose for which such data can be used. The uncertainty related to the scope of Directive 2006/24/EC stems from the fact that Article 1 of the Directive provides that the relevant data retained is destined for the competent national authorities in specific cases and in accordance with national law, without, however, listing any such authorities. This provision allows ample room for national discretion where Member States may choose to widen data access beyond law enforcement authorities and in any case they regard it appropriate. Such sloppy drafting of the Directive implies that apart from law enforcement authorities, both natural and legal persons may often obtain access to confidential data retained under Directive 2006/24/EC. This practice of 'function creep' was approved by the CJEU in a judgment delivered on 19 April 2012 from a preliminary reference

[37] During 2009-2010 only there are a number of public enforcement actions by the Commission: Case C-394/10, *Commission v. Luxembourg* [2010] OJ C 274/26; Case C-189/09, *Commission v Austria* [2010] OJ C 246/12; Case C-192/09, *Commission v. the Netherlands* [2009] OJ/C 180/58; Case C-211/09, *Commission v. Greece* [2009] OJ/C 193/17; Case C-202/09, *Commission v. Ireland* [2010] OJ/C 24/26.
[38] Case C-185/09, *Commission v. Sweden* [2010] OJ C 80/10.
[39] Case C-270/11, *Commission v. Sweden* [2011] OJ C 226/33.
[40] European Commission Press Release, 'Data Retention: Commission takes Germany to Court Requesting that fines be imposed' IP/12/530, 31.05.2012.

made by the Supreme Court of Sweden on the interpretation of Articles 3 to 5 and 11 of Directive 2006/24/EC on the enforcement of intellectual property rights.[41]

In this case Bonnier Audio, a copyright holder of audio books, requested access to retained telecommunications data (name, address, and IP address) from an Internet service provider in order to identify a subscriber whose Internet Protocol address had been used for intellectual property infringing purposes. In the absence of a provision in Directive 2006/24 which prevents a party to a civil dispute from being ordered to disclose subscriber data to someone other than a public authority, the CJEU held that Member States are not precluded from using the Directive to enforce intellectual property rights. The CJEU held that the right to respect private and family life inherent in Article 7 of the EU Charter of Fundamental Rights has to be balanced against the protection of intellectual property enshrined in Article 17 of the Charter. The CJEU further established for future cases that in the event a private party requests access to personal data, such access would have to be ordered by a national judge taking into account the principle of proportionality. The language of proportionality employed here by the CJEU is reminiscent of that in *Rottmann*.[42] The proportionality assessment suggested by the CJEU in both cases lacks detail and guidance and, as such, leaves Member States considerable leeway to undermine the fundamental rights of their citizens in favour of large-scale data retention.

5 Conclusion

The purpose of this chapter was to unveil the main complex issues surrounding the so-called Data Retention Directive as well as the CJEU's contribution in assessing the internalities of the blanket harmonisation of the length of time that telecom operators and Internet providers must retain data under EU legislation. The chapter has provided insight into the blurry scope and objectives of the Data Retention Directive and, by extension, the future of telecommunications data retention in Europe which will have to be proportionality-friendly and subject to judicial oversight. It has been argued that the regime forged by Directive 2006/24 lacks adequate legal safeguards in order to limit the risk of abuses of a host of rights guaranteed by both EU primary and secondary law as well as the European Convention of Human Rights (ECHR).[43] This is all the more crucial since certain

[41] Case C-461/10, *Bonnier Audio AB and Others v Perfect Communication Sweden AB*, Judgment of the Court, 19.04.2012.

[42] Case C-135/08, *Janko Rottman v. Freistaat Bayern* [2010] ECR I-01449. See also T. Konstadinides, 'La Fraternité Européenne? The Extent of National Competence to Condition the Acquisition and Loss of Nationality from the perspective of EU Citizenship' (2010) 35 (3) *European Law Review* 401.

[43] The right to protection of personal data exists in Article 16 TFEU, which includes provisions for a general application in areas such as judicial cooperation in criminal matters and Article 39 TEU where data protection is relevant in the sphere of Common Foreign and Security Policy. See also Directives 95/46/EC and 2002/58/EC; Regulation (EC) 45/2001 and Articles 7 and 8 of the EU Charter of Fundamental Rights.

studies on the application of the Directive in the Member States have demonstrated that blanket harmonisation of the length of time that telecom operators and Internet providers must retain data has proven to be superfluous for the investigation and prosecution of serious crime.[44] The empirical evidence to support the necessity of data retention is overall poor. This is confirmed by the very revealing consultation paper published in late 2011 by the European Commission services on reforming the Directive.[45] Among other things it is noted that the alleged value of historic communications data in terrorism or other cases involving serious crime has only been confirmed by eleven out of the twenty-seven Member States. It is also reported that the lack of clarification by EU institutions with regard to the type of data retained for combating crime or business purposes has resulted in confusion. For instance, some Member States have encouraged the storage of data (such as instant messaging and chat) which falls outside the scope of Directive 2006/24. As such, clarity with reference to the purpose and scope of the Directive as well as the establishment of safeguards for access and use of the retained data constitute high priority areas.

In light of these developments, the present author welcomes alternative legal instruments to Directive 2006/24 - in particular, the proposal on data preservation put through by Peter Schaar, the German Federal Commissioner for Data Protection and Freedom of Information. The proposal, also mentioned by the Council's Working Party on Data Protection and Information Exchange, suggests the substitution of the Directive on data retention with a 'quick freeze' system, which would make data storage dependent on a court order.[46] Such a *Kadi*-equivalent system would allegedly constitute a more efficient arrangement from the rule of law point of view, for the prosecution of serious cross-border crime than the current framework on blanket data retention. Such a system would discourage intense and all-encompassing telecommunications surveillance. It would also be fit for resolving civil disputes, which are unrelated to the fight against terrorism and organised crime. But still, in order to do so, the EU legislature has to come to a decision as to what constitutes 'serious crime' – a term which lies undefined in the Directive and, as seen in *Bonnier Audio AB*, gives complete discretion to Member States to hijack the Directive by using retained data for infringements which lie outside the scope of criminal

[44] See Working Party on Data Protection and Information Exchange (DAPIX - Data Protection) Evaluation report on the Data Retention Directive (Directive 2006/24/EC 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), 4 May 2011, DG H 2B, 10806/11; European Digital Rights, Shadow evaluation report on the Data Retention Directive (2006/24/EC), 17 April 2011, p.4. Available at <www.edri.org/files/shadow_drd_report_110417.pdf>

[45] Council of the EU, Commission Services, 'Consultation on Reform of Data Retention Directive: Emerging themes and next steps', 18620/11,15.12.2011.

[46] The Federal Commissioner for Data Protection and Freedom of Information, Press Release: 'Peter Schaar: "Quick Freeze" instead of data retention', 14.06.2010. Available at: <www.bfdi.bund.de/EN/PublicRelations/PressReleases/2010/22_%22QuickFreeze%22.html?nn=410156> See also note 40 above with regard to the relevant report by the Working Party on Data Protection and Information Exchange.

investigation. This study indicates that the lack of an exact determination of the area of data necessary for the identification of natural or legal persons ('related data') does not merely constitute a transposition problem that can simply be remedied through national legislation in one Member State. Data controllers established in several Member States will still have to make themselves familiar with diverse national legislation within the EU. The result is a fragmented legal environment that not only results in legal uncertainty but is also incredibly expensive for businesses.[47]

Despite the overall dark picture painted in this chapter with regard to the alleged necessity of large-scale retention of traffic data, the new proposal for a Directive on the protection of individuals vis-à-vis the processing of personal data by law enforcement authorities for crime prevention is a positive development.[48] If adopted, such a Directive will give meaning to Article 16 TFEU both as a source of the right to protection of personal data and as a specific legal basis for the adoption of rules on the protection of personal data within the context of judicial co-operation in criminal matters and police co-operation. The character of the proposal is generally innovative in that it goes further than Directive 95/46/EC.[49] For instance, it provides for the 'right to be forgotten' that allows individuals to demand that data collectors delete their retained data when there are no legitimate grounds to retain data. What is more, Article 54 provides for compensation by the Member States, controllers or processors for the damage suffered in cases of an unlawful data processing operation. The proposed Directive may not, however, be met with enthusiasm by all national governments which may be reticent towards witnessing the conduct of their public authorities being restrained by EU law. This is because the proposed Directive would extend the scope of data protection rules to 'domestic' processing.

To reflect on the title of this edited volume, it seems that the once cooperative model of 'European Police and Criminal Law' has shifted towards a coercive one. Such a model is based on rapid and intrusive action against potentially serious security threats. The EU is, therefore, promoting a system whereby mere suspicion suffices to resort to actions, such as intense and all-encompassing telecommunications surveillance. Judging from the infringement proceedings against a host of Member States, it appears that not all national governments are ready to adapt to the coercive EU criminal law model (although Commission

[47] See Commission Staff Working Paper, Executive Summary of the Impact Assessment on the proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, Brussels, 25.1.2012 SEC (2012) 73 final.

[48] See the Commission's Proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, Brussels, 25.01.2012, COM (2012) 10 final.

[49] 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 L 281/31.

infringement proceedings against them gradually force them to do so). As seen in this chapter, the effective transposition of the Directive goes further than merely establishing a legislative framework for the free flow of personal data in the internal market. The proposed Directive on data protection with regard to the processing of personal data by competent authorities may provide some relief to certain Member States with reference to the protection of individual privacy. It then depends on whether, in every day practice, national governments will choose the pervasive Orwellian surveillance state model over one based on a high threshold of individual data protection rights.