BRILL
NIJHOFF

TILBURG LAW REVIEW 20 (2015) 14-34

Tilburg
Law Review

brill.com/tilr

Data Retention and its Implications for the Fundamental Right to Privacy

A European Perspective

Arianna Vedaschi
Associate Professor of Public Law, Bocconi University of Milan
arianna.vedaschi@unibocconi.it

Valerio Lubello
Postdoctoral Scholar of Comparative Public Law, Bocconi University
valerio.lubello@unibocconi.it

Abstract

The Data Retention Directive is one of the most controversial acts adopted by the EU. The storage of an indeterminate amount of data – concerning every citizen of the EU – requires finding a balance between the need to fight terrorism and the rights to privacy and data protection, as declared in the Charter of Fundamental Rights of the EU, the ECHR, and by the common constitutional values shared by Member States. According to the CJEU (joined cases C-293/12 and C-594/12), the Directive 'treats everyone as a suspect', 'monitors everyone' and 'puts everyone under surveillance' and represents a 'serious interference' to citizens' rights to privacy.

The aim of this paper is to define – through a comparative analysis – the main features of the CJEU balancing process, trying to assess possible future scenarios for data retention in the European and domestic legal frameworks. The challenge remains the same: how to prevent serious crime and terrorism while preserving our fundamental rights?

Keywords

data retention – privacy – data protection – mass surveillance – national security

---

* Valerio Lubello authored paragraphs 4 and 5 while Arianna Vedaschi is the author of the paragraphs 1–3, 6 and concluding remarks. The authors would like to thank Gabriele Marino for his invaluable assistance with research and footnotes.

 | DOI 10.1163/22112596-02001005

1 Introduction

The post-9/11 era can be characterized by the desire and ability of governments to develop a global mass surveillance system, largely unseen and until recently unsuspected, which impinges not only upon European and American citizens, but also on anyone of potential interest to the security and intelligence services.[1] In fact, despite a disparity in approaches among western countries to deal with terrorist threats,[2] a common trend can be discerned whereby governments monitor the communications and online behaviour of the vast majority of ordinary citizens.[3] As a result, the right to data protection and, above all, the fundamental right to privacy are now vulnerable to a degree unimaginable pre-9/11.[4]

Recent revelations concerning data surveillance have focused attention on the issue of mass data collection in both the USA and the EU. In particular, the USA National Security Agency (NSA) has been able covertly to gather

1 C Kuner, *Transborder Data Flows and Data Privacy Law* (OUP 2013); T Konstadinides, 'Mass Surveillance and Data Protection in EU Law: The Data Retention Directive Saga' in M Bergstrom and A Jonsson Cornell (eds), *European Police and Criminal Law Co-Operation* (Hart Publishing 2014) 69–84. See also J Goldsmith and T Wu, *Who Controls the Internet? Illusions of a Borderless World* (OUP 2006) 179 (underlining the transnational dimension of privacy concerns); C Cocq, 'Regional legal framework of intelligence and information sharing comparative analysis between the European Union and the ASEAN' in this Special Issue (provides a comparative analysis of regional frameworks); V Mitsilegas, 'Transatlantic counter-terrorism cooperation and European values: constitutional accommodation or a race to the bottom' in this Special Issue; K Lachmayer, 'Rethinking privacy beyond borders' in this Special Issue (both address crucial aspects of issues arising from the question of transnational privacy). See also I Tourkochoriti, 'The Transatlantic Flow of Data and the National Security Exception in the European Data Privacy Regulation: In Search for Legal Protection', (2014) University of Pennsylvania Journal of International Law 36 (forthcoming); D Cole and F Fabbrini, 'Transatlantic cleavages? Counter-terrorism, data protection and the re-appropriation of constitutional values on a transnational scale' in F Fabbrini and V Jackson (eds), *Constitutionalism Across Borders in the Struggle Against Terrorism* (Elgar Publishing 2016) (forthcoming) (both providing a comparative analysis of the USA and the EU).

2 A Vedaschi, *À la guerre comme à la guerre? La disciplina della guerra nel diritto costituzionale comparato* (Giappichelli 2007) 75 ff and 504 ff.

3 S Gutwirth, Y Poullet and P De Hert (eds), *Data Protection in a Profiled World* (Springer 2010). See also M Levi and DS Wall, 'Technology, Security and Privacy in the Post-9/11 European Information Society' (2004) 31(2) Journal of Law and Society 194 ff.

4 J Kokott and C Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' (2013) 3(4) International Data Privacy Law 222 ff.

information regarding emails and data files,[5] etc., with evident implications on the rights of privacy and data protection of citizens. In this regard, President Obama called for 'a more robust public discussion about the balance between security and liberty (…)'.[6] Meanwhile, in Europe voices have been raised over the access of governments to metadata–a situation both facilitated and symbolised by EU Directive 2006/24,[7] the so-called Data Retention Directive, which obliges telephone and Internet service providers to collect and retain metadata, including that of emails and phone calls, for up to two years.[8] In doing so, the Directive 'treats everyone as a suspect', 'monitors everyone' and 'puts everyone under surveillance',[9] and for this reason the European Court of Justice (CJEU, the Court)–in a landmark judgment–held that the Data Retention Directive 'constitutes a particularly serious interference' with the fundamental right of citizens to privacy. As a consequence, on 8th April 2014,

5 J Yoo, 'The Legality of the National Security Agency's Bulk Data Surveillance Programs' (2013) UC Berkeley Public Law Research Paper 2369192 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2369192 ##> accessed 31 August 2014.

6 President Obama focused on this crucial question in his speech on potential NSA surveillance reforms by emphasizing the challenge governments face and highlighting that –at least at a theoretical level– 'it is not enough for leaders to say: trust us, we won't abuse the data we collect', especially when one considers the fact that there exist 'too many examples when that trust has been breached', because '[o]ur system of government is built on the premise that our liberty cannot depend on the good intentions of those in power; it depends on the law to constrain those in power': B Obama, 'Remarks by the President on Review of Signals Intelligence' (17 January 2014) <http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence > accessed 31 August 2014.

7 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] OJ2006 L105/54 (Directive 2006/24/EC).

8 P Breyer, 'Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with ECHR' (2005) 11(3) European Law Journal365; FE Bignami, 'Protecting Privacy Against the Police in the European Union: The Data Retention Directive' (2006) GWU Legal Studies Paper No 2013–43 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2230611> accessed 31 August 2014. See also CC Murphy, *EU Counter-Terrorism Law* (Hart Publishing 2012).

9 TJ McIntyre–who took the case to the High Court of Ireland–is chair of Digital Rights Ireland Ltd, a limited liability company which promotes civil liberties and human rights, with specific regard to communication technologies. This company has sued the Irish authorities for claiming unlawful control over data related to its communications. TJ McIntyre's opinion is cited by N Nielsen, 'EU Data Retention Law Said to Breach Privacy Rights', <www.eurobserver.com/justice/122459> accessed 15 September 2014.

the CJEU, sitting in Grand Chamber, declared Directive 2006/24/EC invalid since it violates the right to privacy (Article 7 of the Charter) and the right to protection of personal data (Article 8 of the Charter), read in light of Article 52 of the Charter of Fundamental Rights of the European Union (the Charter). In adopting Directive 2006/24, the EU legislature exceeded the limits imposed by the principle of proportionality.[10]

For the first time, the CJEU has declared the full invalidity of the European data retention regulation due to a violation of fundamental rights as laid down by the Charter. In this context, the decision taken on 8th April 2014 underlines the Court's role as a proper "constitutional Court" of the EU which legitimates its position through a complete use of its "Bill of Rights" (i.e. the Charter).

From this perspective, this paper addresses the question whether the data retention constraints placed by Directive 2006/24 on fundamental rights are consistent with the Charter.[11] With regard to this aspect we agree with the CJEU decision and argue that the Data Retention Directive is indeed illegitimate. Furthermore, this paper discusses what happens after the CJEU decision and outlines different possible scenarios both at domestic and European levels.

To this end, this paper is structured as follows. Paragraph two sketches the background of the Data Retention Directive in order to point out the dangerous switch in EU focus following the terrorist attacks in the early years of the 21st century. Paragraph three analyses the main features of the Data Retention Directive and its problematic aspects, in order to underline the impact of the consequent restrictions on the rights to privacy and data protection. Paragraph four examines the fundamental rights concerns raised by national courts. Paragraph five focuses on the compatibility between the Data Retention Directive and fundamental rights enshrined in the Charter, as reviewed by the CJEU. Finally, paragraph six discusses the legal effect of the ruling of the CJEU and considers possible future developments.

10 Joined Cases C-293/12 and 594/12 *Digital Rights Ireland Ltd* v. *Minister for Communication et al and Kärtner Landesregierung et al* (CJEU, 8 April 2014). See also Joined Cases C-293/12 and 594/12 *Digital Rights Ireland Ltd* v. *Minister for Communication et al and Kärtner Landesregierung et al* (CJEU, 8 April 2014), Opinion of AG Villalón; F Fabbrini, 'Human Rights in the Digital Age, The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the US' (2015) 28(1) Harvard Human Rights Journal (forthcoming).

11 K Roach, 'Secret Evidence and Its Alternatives' in A Masferrer (ed), *Post 9/11 and the State of Permanent Legal Emergency. Security and Human Rights in Countering Terrorism* (Springer 2012) 179 ff.

2 European Law on Metadata During the Post-9/11 Era: From Protection to Retention

From a European vantage point, it is worth noting the correlation between the scale of the terrorist threat and the scope of mass surveillance programmes, which undoubtedly became more prevalent post-9/11. In Europe the perceived level of threat increased dramatically following the Madrid and London bombings. Consequently, the European policy focus has shifted subtly but with enormous implications from one of data protection to data retention, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crimes, including terrorist offences. This radical change in policy, enacted in the relative blandness and dry language of a Directive, has been made largely without the media attention that the dramatic revelations of covert government surveillance have attracted in the USA. It should be recalled that Directive 95/46/EC–the so called Data Protection Directive–was originally enacted in order to protect fundamental rights, above all the right to privacy, with regard to the processing of personal data and to the free movement of such data within EU Member States.[12] By contrast, the aim of Directive 2006/24/EC,[13] issued in the wake of the Madrid and London attacks, was to harmonize the obligations placed on Internet and telecommunications service providers to collect and retain certain data and to ensure that those data are available for the purposes of the investigation, detection and the

12 Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (Directive 95/46/EC). Cf 'G8 and ILETS discussed problems of "data retention and implications of data protection legislation" in 1999' (*Statewatch News Online*, May 2001) <http://database.statewatch.org/article.asp?aid=6289> accessed 31 August 2014; J Fromholz, 'The European Union Data Privacy Directive' (2000) 15(1) Berkeley Technology Law Journal 461; S Gutwirth, R Leenes and P De Hert, *Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges* (Springer 2014). Different concepts of privacy also in a comparative perspective are well summarized by DJ Slove, *Understanding Privacy* (Harvard University Press 2008).

13 Directive 2006/24/EC (n 7), Recitals 10–11. See also Council, 'EU Plan of Action on Combating Terrorism' (2004) 10586/04; Council, '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' (2004) 8958/04; D Rowland, 'Data Retention and the War Against Terrorism–A Considered and Proportionate Response?' (2004) 3 The Journal of Information, Law and Technology <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004_3/rowland/>accessed 31 August 2014.

prosecution of serious crimes.[14] This significant change in the EU approach, more oriented toward security, had already emerged with the increased EU attention on electronic communications sector triggered by Directive 2002/58/EC.[15] The so-called Electronic Communications Directive states that Member States can adopt legislative measures to restrict the scope of rights, if this is necessary in order to safeguard national security.[16]

Assuming that it is justified by emergency circumstances, this shift in favour of security–marked by the transition from a fundamental concern with *protection* to the pragmatic desire for *retention*–should entail guarantees in order to safeguard the interests of all citizens within the EU, as was originally intended. Whether the Directive does in fact contain sufficient guarantees for the rights to privacy and to data protection is the question, which will be addressed in the following paragraph.

3 Problematic Aspects of Directive 2006/24/EC

This paragraph analyses the content of the Data Retention Directive. In order to perform a meaningful assessment of the impact on the fundamental rights, we need to highlight its most problematic aspects. The core of the Directive is the data retention obligation; in fact, as already underlined, Directive 2006/24 binds EU Member States to impose upon Internet service providers (usually private companies) the duty to collect and store, for a significant period, a large and varied amount of metadata, which may be of use to public security authorities in the fight against serious crime, including terrorism. This obligation and its rules are problematic in a number of ways.

First of all, it is important to stress, once again, that data collection obligations apply to every electronic communication within the EU territory and involve any individual (whether they be a European citizen or not) using a

14 Directive 2006/24/EC (n 7), Recital 21. See also Case C-301/06 *Ireland* v. *European Parliament* [2009] ECR I-00593 (according to this ruling the Data Retention Directive is primarily market-oriented).

15 Directive 2002/58/EC of the European Parliament and the Council of 31 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 L201/37.

16 C Jones and B Hayes, 'The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy' (SECILE Project D2.4, SECILE 2013) 17 <http://secile.eu/wp-content/uploads/2013/11/Data-Retention-Directive-in-Europe-A-Case-Study.pdf> accessed 31 August 2014.

telephone or the Internet, without distinguishing between criminal suspects and ordinary citizens. Indeed, although Directive 2006/24 identifies the aim of retention as fighting serious crime, the Directive does not explain what should be understood by such a broad term as 'serious crime', leaving the definition up to each Member State. In practice, Member States have taken very different paths in order to define this open-ended concept with an adequately exhaustive meaning: some have adopted specific lists of serious crimes, while others have referred to a minimum term of imprisonment prescribed by law; yet others (including Italy) have gone beyond the scope of the Directive by prescribing data retention obligations–and granting full access to public security authorities–even for pre-emptive purposes.[17]

With regard to data categories, the Directive requires the collection and retention of metadata relating to the source and recipient, type, date, time and duration of the communication and geolocation data. The collection and retention of such records require service providers to rely increasingly on technology capable of automatically gathering unprecedentedly large amounts of information and storing it in ever-expanding databanks. This potentially facilitates the cross-referencing of personal data, thereby leveraging neutral data to generate significant information when used in combination. Thus, even if the core information of the communication conveyed is explicitly excluded from the scope of the Directive, one cannot disregard the enormous profiling potential of metadata, if accurately combined and contextualised.[18]

In addition, the Directive requires service providers not to interfere with the prompt availability of data to the competent authorities.[19] But Article 4 of the

17 FE Bignami, 'Privacy and Law Enforcement in the European Union: the Data Retention Directive' (2007) 8(1) Chicago Journal of International Law 233; Commission, 'Evaluation report on the Data Retention Directive (Directive 2006/24/EC)' (Report) COM (2011) 225 final; C Cocq and F Galli, 'Comparative paper on data retention regulation in a sample of EU Member States' (Surveille Project D4.3, Surveille 2013) 11ff <http://www.surveille.eu/PDFs/D4.3%20Comparative%20law%20paper%20on%20data%20retention%20regulation%20in%20a%20sample%20of%20EU%20member%20states.pdf> accessed 31 August 2014. Regarding the concept of metadata see also Article 29 Data Protection Working Party, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes (10 April 2014) <http://ec.europa.eu/justice/data-protection/index_en.htm> accessed 22 September 2014.

18 H Roberts and J Palfrey, 'The EU Data Retention Directive in an Era of Internet Surveillance' in R Deibert and others (eds), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (MIT Press 2010). Cf *Big Brother Watch and others* v. *Kingdom* App no 58170/13 (ECtHR, lodged on 4 September 2013).

19 Bignami, 'Privacy and Law Enforcement in the European Union: the Data Retention Directive' (n 17).

Directive does not specify who these authorities are or should be. As a consequence, for example, 14 out of 28 Member States have included intelligence agencies within the definition of 'competent authorities'.[20] Moreover, with no general framework criteria or defined access conditions provided by the Directive to regulate the availability of collected data, there is the risk of an asymmetry in national legislation and a corresponding lack of guarantees. With specific regard to collecting and handling operations, Article 3 of Directive 2006/24 introduces an express exception to Arts. 5–6 and 9 of Directive 2002/58, which are aimed at protecting the confidentiality of communications over public telephone networks and the Internet, including any related metadata, prohibiting wiretapping and surveillance and prescribing the immediate anonymisation of traffic and geolocation data. According to Article 15 of Directive 2002/58, as amended by Directive 2006/24,[21] guarantees provided by Article 13, para. 1, of Directive 95/46 may be restricted due to 'specific public order purposes'. This revised legal standard goes beyond the pre-existing regulatory framework, which placed on Member States the responsibility for specific exceptions and data retention duties, within the scope of the aforementioned Article 13. In the Directive's own wording, service providers are duty-bound to store and handle collected data respecting the 'minimum' level of security standards and protection principles defined in previous Directives. As a result, the retention of metadata also increases the risk of privacy violations due to misuse or unauthorised access of data. Furthermore, no prescription is imposed upon providers regarding the physical location of databanks, which may be freely located overseas, beyond national and EU jurisdiction.

Lastly, the retention period raises further serious concern, since under Article 6 of Directive 2006/24 it is left to each State's discretion, within a range of 6 to 24 months. Additionally, Article 12 allows Member States, under unspecified circumstances, to extend the retention period beyond two years. Even though it could be assumed that any potential analysis of retained data would be performed by 'competent authorities' in accordance with the EU regulatory framework, it is undeniable that the right to privacy may be violated during the retention period.[22] Such a situation emphasises the relevance of the restrictions that Directive 2006/24 places on fundamental rights.[23]

20 Jones and Hayes (n 16) 17 ff.

21 Directive 2006/24/EC (n 7), Art.15 para 1-bis.

22 Commission (n 17).

23 Cocq and Galli (n 17) (provides a comparative study of the use of retained data within national jurisdictions).

In the light of these considerations, one can underline the fact that the Directive interferes with fundamental rights by placing ordinary citizens under surveillance without them having committed any serious crime, a concept that is not explicitly defined by the Directive. In the same way, the Directive neither codifies, in a strict manner, the procedure to access data, nor does it specify the competent authorities which can access data over a long duration of time and which enables profiling. From the combined effects of these rules the clear tendency of EU legislation is towards ensuring collective security at the expend of individual liberties.

4 Implementing Directive 2006/24: The Proportionality Test at the National Level

Against this backdrop, the relationships between data retention provisions and fundamental rights have raised significant concerns relating to the transposition provisions in Member States, namely the Supreme Courts of Bulgaria and Cyprus,[24] and the Constitutional Courts of Romania,[25] Germany,[26] the Czech Republic,[27] and, following the ruling of CJEU, the Austrian Constitutional Court.[28] Other cases are also pending in the Constitutional Courts of Poland,[29]

24 Bulgarian Supreme Administrative Court, No 13627, 11 December 2008 <http://www.capital.bg/getatt.php?filename=0_598746.pdf> accessed 1 September 2014; Supreme Court of Cyprus, Decision of civil applications 65/2009, 78/2009, 82/2009 & 15/2010-22/2010, 01 February 2011 <http://www.supremecourt.gov.cy/judicial/sc.nsf/0/5B67A764B86AA78EC225782F004F6D28/$file/65-09.pdf> accessed 1 September 2014.

25 Constitutional Court of Romania, No. 1258, 8 October 2009 <http://www.legi-internet.ro/fileadmin/editor_folder/pdf/Decizie_curtea_constitutionala_pastrarea_datelor_de_trafic.pdf> and unofficial translation at <http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf> accessed 1 September 2014.

26 German Constitutional Court, No. 11/2010, 2 March 2010, <http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html> accessed 1 September 2014.

27 Czech Constitutional Court, PI US 24/10, 22 March 2011 <http://www.usoud.cz/fileadmin/user_upload/ustavni_soud_www/Aktualne_prilohy/2011_03_31b.pdf> and official translation at <http://www.usoud.cz/en/decisions/?tx_ttnews%5Btt_news%5D=40&cHash=bbaa1c5b1a7d6704af6370fdfce5d34c> accessed 1 September 2014.

28 Austrian Constitutional Court, G 47/2012, 27 June 2014 <http://www.vfgh.gv.at/cms/vfgh-site/attachments/5/0/0/CH0003/CMS1403853653944/press_releasedataretention.pdf> accessed 1 September 2014.

29 A Adamski, 'The telecommunication data retention in Poland: does the legal regulation pass the proportionality test?' (2013) 1 Przegląd Prawa Technologii Informacyjnych/ICT

Slovakia,[30] Slovenia,[31] and Hungary.[32] While waiting for the decision of the CJEU, the Slovakian Constitutional Court stopped the application of the transposition provisions while Slovenian judges suspended their decision in anticipation of the judgment of the CJEU. These decisions reveal a complex horizontal and vertical judicial dialogue between national courts and the CJEU and the European Court of Human Rights (ECtHR). In this respect, national decisions facilitate a better understanding of the proportionality test, as shaped by the ECtHR, the CJEU and national courts as well.

As is clear from the discussion above, national rulings anticipate the debate on the proportionality test, focusing on points which are now part of the reasoning through which the CJEU has declared the invalidity of the Data Retention Directive. In this light, it is noteworthy that all the national decisions involved have steered clear of a direct debate over the legitimacy of the Data Retention Directive. Rather than rejecting Directive 2006/24, these courts have preferred to focus their decisions on implementation provisions, applying the proportionality test only to national laws. While the Romanian Court has differed by articulating a sense of unease with respect to the Data Retention Directive, other courts have preferred a 'silent' and implied dialogue with the European Institutions.

Law Review 4–11 <http://www.ictlaw.umk.pl/wp-content/uploads/Przegl%C4%85d-Prawa-Technologii-Informacyjnych.ICTLaw-Review.pdf > accessed 22 September 2014.

30 See the pending case PL. ÚS 10/2014.

31 See Judgment I-65/13-19 of 3 July 2014. For an overview see S Bardutzky, 'The Timing of Dialogue: Slovenian Constitutional Court and the Data Retention Directive', in www.verfassungsblog.de, 10 September 2014, <http://www.verfassungsblog.de/en/timing-dialogue-slovenian-constitutional-court-data-retention-directive/#.VBcYp_l_v2A> accessed 22 September 2014.

32 The Hungarian ruling has been suspended due to the adoption, in April 2011, of the new Fundamental Law, which abolished the *action popularis* and imposed the end of all pending cases. K Kelemen, 'The Hungarian Constitutional Court in the new constitutional framework' (draft version) <http://www.academia.edu/1760644/The_Hungarian_Constitutional_Court_in_the_new_constitutional_framework> accessed 1 September 2014; V Lubello, 'Ungheria. Flusso di modifica alla Legge fondamentale' (2013) 2 DPCE online <http://www.dpce.it/online/images/stories/Ungheria_Lubello.pdf> accessed 1 September 2014. For an overview about national cases see E Kosta, 'The Way to Luxembourg: National Court Decisions on the Compatibility of the Data Retention Directive with the Right to Privacy and Data Protection' (2013) 10(3) SCRIPTed 339 and more recently F Boehm, D Cole, 'Data Retention after the Judgment of the Court of Justice of the European Union', The Greens, European Free Alliance in the European Parliament, 30 June 2014 <http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf>.

With regard to the parameters, the reasoning of constitutional and supreme courts differs. Sometimes the parameter is the right to private life as enshrined by national Constitutions,[33] by Article 8 of the European Convention on Human Rights (ECHR) and by Article 7 of the Charter read in conjunction with the right to protection of personal data provided by Article 8. The Bulgarian, Romanian,[34] and Czech Courts and, more recently, the Austrian Constitutional Court have expressly referred to the right to private life provided by Article 8 of the ECHR and, sometimes, to its interpretation made by the ECtHR.[35] In this light, Romanian and Czech judges have clearly referred to the conditions and arguments settled by the ECtHR for Article 8 of the ECHR.[36] At other times, the parameter is fixed on the privacy of communications. In this light, the German Constitutional Court begins its reasoning from Article 10 of the *Grundgesetz* (GG) read together with the right to informational self-determination (*Recht auf informationelle Selbstbestimmung*), part of the German historical jurisprudential background on privacy matters.[37] Additionally, the Supreme Court of Cyprus held that transposition provisions breached both the right to private life and the secrecy of correspondence.[38]

National courts seem to accept the data retention in principle, while requesting a more complete application of proportionality. The Romanian Constitutional Court admitted 'that there is an urgent need to ensure adequate and efficient legal tools' able to keep pace with constantly-improving technology in order to fight crime. However, the Court emphasised that the collection

33 Bulgarian Constitution, Arts. 32 and 34; Romanian Constitution, Art. 26; Czech Charter of Fundamental Rights and Freedoms, Arts. 10(2)–10(3).

34 It is noteworthy that Romanian judges referred to the right to private life such is enshrined by Art. 17 of the International Covenant on Civil and Political Rights as well as by Art. 12 of the Universal Declaration of Human Rights.

35 J Durica, 'Directive on the retention of data on electronic communication in the rulings of the constitutional Courts of EU Member States and efforts for its renewed implementation' (2013) 2 The Lawyer Quarterly <http://www.ilaw.cas.cz/tlq/index.php/tlq/article/view/73 TLQ 2/2013> accessed 1 September 2014. See also CC Murphy, 'Note on Romanian Constitutional Court, Decision No 1258 of 8 October 2009' (2010) 47(3) Common Market Law Review 933.

36 *Klass and Others* v. *Germany* (1978) 2 EHRR 214, paras 33–37; Jones and Hayes (n 16) 24. See also T Konstadinides, 'Destroying Democracy on the Ground of Defending It? The Data Retention Directive, the Surveillance State and Our Constitutional Ecosystem' (2011) 6 European Law Review 722.

37 Y Poullet and A Rouvroy, 'Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie' in K Benyekhlef and P Trudel (eds), *État de droit et virtualité* (Thémis 2009).

38 Constitution of Cyprus, Arts. 15(1) and 17(1).

of data pertaining to all citizens, regardless of any involvement in criminal investigations, 'is likely to overturn the presumption of innocence',[39] transforming all users of electronic communication services into potential suspects. Similarly, the German Constitutional Court accepted the idea of data retention. The Court rejected the procedure provided by Article 267 of the TFEU and also avoided an open conflict with the EU system.[40] The decision is limited to national provisions implementing the Directive in the German legal system. Thus, the Data Retention Directive 'can be implemented in German law without violating the fundamental rights guaranteed by the Basic Law'.[41] In this respect, the Czech Court referred to the self-determination right as established by the German Constitutional Court and, following the German Court, held that the Data Retention Directive is not unconstitutional in itself, but that the transposition provisions exceeded the requirements of the Directive.

The concerns exposed by national courts are clearly taken into account by the CJEU. This is true for several issues, such as: the number and the kind of authorities with access to retained data (Czech Constitutional Court); the people involved in the data retention (Romanian Constitutional Court and Supreme Court of Cyprus); the length of the retention period (Czech Constitutional Court); the seriousness of the crimes (German Constitutional Court); the access to data without knowledge and consent (Supreme Court of Cyprus); and, more generally, the proportionality principle. The reasoning of the German Constitutional Court is especially significant. According to the Court, if the collection and retention of data provided by transposition provisions are 'integrated into a legislative structure which is appropriate to the encroachment' then 'it is capable of satisfying the proportionality requirements'.[42] Hence, the lack of these proportionality measures permitted the Court to declare the disputed provisions null and void. Indeed, the Court found that the same provisions 'guarantee neither adequate data security nor an adequate restriction of the purposes of use of the data. Nor do they in

39 Constitutional Court of Romania, No. 1258, 8 October 2009 <http://www.legi-internet.ro/fileadmin/editor_folder/pdf/Decizie_curtea_constitutionala_pastrarea_datelor_de_trafic.pdf> and unofficial translation at <http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf> accessed 1 September 2014, 10.

40 AB Kaiser, 'German Federal Constitutional Court: German Data Retention Provisions Unconstitutional in Their Present Form; Decision of 2 March 2010, *NJW* 2010, p. 833' (2010) 6(3) European Constitutional Law Review 503.

41 German Constitutional Court, No. 11/2010, 2 March 2010, <http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html> accessed 1 September 2014, para 10.

42 Ibid para 12.

every respect satisfy the constitutional requirements of transparency and legal protection'.[43] Moreover, the Court, like the CJEU, provided 'detailed guidelines' for legislation, affirming the need of a proportionality test which requires the respect of the following four criteria: 1) proportional data security standards; 2) proportional purpose limitation; 3) transparency; 4) judicial control and effective legal remedies.[44] As the following paragraphs will make clear it will be clear these types of guidelines are very similar to the suggestions that the CJEU provides for the future European legislator in the field of data retention.

5 The Data Retention Directive and the Issue of its Legitimacy

This paragraph assesses the compatibility of the restrictions Directive 2006/24 places on some fundamental rights with the protective standards provided by the Charter. To that end, it is necessary to identify the essential parameters of the evaluation and then to focus on the proportionality test, which lies at the heart of this paper and entails striking a balance between liberty and security in the post-9/11 era.

As regards the parameters, Arts. 7 and 8–read in the light of Article 52– of the Charter safeguard the right to privacy and the right to protection of personal data respectively. The right to privacy is enshrined in all the national constitutions of Member States within the EU. It is also expressly guaranteed by the ECHR and recognised by every liberal democracy, both in Europe and beyond.[45] Specifically, the same Article states that 'any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms.' In requiring limitations to be imposed by law, the Charter therefore bans generic formulas from those acts, which limit fundamental rights, and requires such national measures to be adopted by means of primary sources of law. Moreover, Article 52 also provides that, '[s]ubject to the principle of proportionality, limitations [to fundamental rights] may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others'; as a consequence–and as repeatedly

43 Ibid para 8.

44 K de Vries and others, 'The German Constitutional Court Judgment on Data Retention: Proportionality Overrides Unlimited Surveillance (Doesn't It?)' in S Gutwirth and others (eds), *Computer, Privacy and Data Protection: an Element of Choice* (Springer 2011) 3.

45 Gutwirth and others, *Computers, Privacy and Data Protection: an Element of Choice* (n 44).

stated by the CJEU–a strict balance should be maintained between restrictions on civil liberties and the purposes that underlie them.

None of the above-mentioned conditions are met by Directive 2006/24. As noted above, the Directive does not define the concepts of 'serious crime' and 'competent authorities' nor limit the metadata to be collected, thus leaving the provisions unacceptably generic, and it does not prevent Member States from implementing the Directive by means of secondary sources, such as Government regulations. Moreover, it is difficult to reconcile the excessive length of the retention period with the stated aims of the Directive, especially considering that this issue of proportionality–one of great relevance in light of Arts. 7 and 52 of the Charter–remains unsubstantiated in the Directive.

As a result, the CJEU held that 'the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality' and in so doing the Court rejected the practice of universal surveillance. In fact, the core of the Court's decision lies in the rejection of mass surveillance and in particular indiscriminate monitoring of 'the entire European population', which interferes with fundamental rights, especially the right to privacy and the right to data protection.[46] This main argument of the Court's decision can also been seen as an indirect warning regarding any future negotiations between the US and EU in this field.

According to the CJEU it is necessary to read Arts. 7 and 8 of the Charter together, since their implicit connection has also been indicated by the Court in other judgements.[47] The Court used both the parameters of the Charter and those codified by the ECHR,[48] along with the case-law of ECtHR–underlining

46 *Digital Rights Ireland* (n 10) para 56. It should also be noted that the Court is well aware that a vast amount of data is capable of influencing the use of the services affected by the Directive and, as a consequence, it can limit the freedom of expression as guaranteed by Art. 11 of the Charter (and by Art. 10 ECHR, see para. 28 of the dec.). Nevertheless, under the potential violation of the limits imposed by Arts. 7–8 and 52(1) of the Charter, the Court affirms that 'There is no need to examine the validity of Directive 2006/24 in the light of Article 11 of the Charter' (para 28). See also A Vedaschi, 'I programmi di sorveglianza di massa nello Stato di diritto. La data retention al test di legittimità' (2014) 3 Diritto pubblico comparato ed europeo (forthcoming).

47 *Digital Rights Ireland* (n 10) para 29; Case C-92/09 *Volker und Markus Schecke and Eifer* [2010]ECR I-11063, para 47.

48 Note that the Court hereby answers the question posed by the Austrian Verfassungsgerichtshof, asking whether the interpretation of Art. 7 of the Charter can be derived from 'the case-law of the European Court of Human Rights for the purpose of interpreting Article 8 of the Charter such as to influence the interpretation of that latter Article'. Case C-594/12 *Kärntner Landesregierung and Others* (request for a preliminary ruling, 19 December 2012).

the strong relationship between the two courts and their dialogue in the field of human rights.[49]

In order to determine whether the Directive interferes with both abovementioned rights, the CJEU analysed the most problematic rules of date retention as imposed by the Directive. In particular, regarding the nature of the data collected, the Court–following the concerns raised by the Advocate General–affirmed in its reasoning that, even if such data do not refer to the content of the communications, they permit profiling of the user regardless of who that individual may be. More exactly, according to the Court, the data indicated by Article 5 —'taken as a whole'— allow specific and precise deductions to be made regarding the private lives of the persons whose data has been retained, including their habits, movements, activities and relationships.[50] For the Court this result does not comply with the right to privacy, as enshrined in the Charter. Furthermore, the Court established that interference with the rights to privacy could be merely 'potential' since 'it does not matter (…) whether the persons concerned have been inconvenienced in any way', in the same way that it does not matter 'whether the information on the private lives concerned is sensitive'.[51] From this perspective, the Court has grasped the tremendous potential interference inherent in the obligations introduced by Directive 2006/24, stating that data retention 'directly and specifically affects private life' as guaranteed by Article 7 of the Charter. In addition, the same obligations of collecting and retaining metadata also interfere with the protection of personal data, a further right guaranteed by Article 8 of the Charter.[52]

After establishing an interference with Arts. 7 and 8 of the Charter, the Court emphasised that the principle of proportionality requires that a certain act adopted by the EU Institutions has to be 'appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives'.[53] Furthermore, where interference with fundamental rights is particularly serious, as in the case under discussion, any judicial review of the EU legislature's

49 Cf Treaty on the Functioning of the European Union, Art. 6.

50 *Digital Rights Ireland* (n 10) para 27.

51 Ibid para 33; Joined Cases C-465/00, 138/01 and 139/01 *Österreichischer Rundfunk and Others* [2003] CJEU I-04989, para 75.

52 *Digital Rights Ireland* (n 10) para 29; *Volker und Markus Schecke and Eifert* (n 47).

53 *Digital Rights Ireland* (n 10) para 46. See also *Volker und Markus Schecke and Eifert* (n 47); Case C-343/09 *Afton Chemical* [2010] CJEU I-07027; Joined Cases C-581/10 and 629/10 *Nelson* (CJEU, 23 October 2012); Case C-283/11 *Sky Österreich* (CJEU, 22 January 2013); Case C-101/12 *Schaible* (CJEU, 17 October 2013).

discretion should be particularly strict, in order to grant such rights a satisfactory level of protection.[54]

In this light, the features of the Directive that do not pass the test of proportionality are numerous and summarised well by the Court, which follows a reasoning analogous to that of national constitutional and supreme courts, as discussed above. In particular, the Court pointed out how the retention of all traffic data concerning any type of communication impacts 'the entire European population', highlighting that the Directive places every person under surveillance.[55] Thus, the Court exposed the absence of any relationship between the huge amount of retained data and persons likely to be involved in committing serious crimes. As the Court held, Directive 2006/24 affects —'in a comprehensive manner'— the traffic data of people, 'without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions'.[56] In practice, Directive 2006/24 has left the crucial definition of serious crime to the national lawmakers of each Member State. On the contrary, in the opinion of the Court, the EU legislation must provide more specific criteria in order to define exactly what constitutes 'serious crime'. Moreover, there is no differentiation, limitation or exception made for the essential aim of fighting serious crime.[57] The Court further affirmed national decisions by deciding that the Directive, as transposed by Member States, has also failed to lay down 'any objective criterion' to establish limits of access to the metadata by the competent national authorities.[58] Furthermore, the Court deemed that the Directive is too vague in defining the 'procedural conditions related to the access' of and to the use of the data.[59] Subsequent regulation must take into account the concerns of the Court relating to this point.

Regarding the retention period, the Court found that it is not determined by an objective criterion able to pass the 'strictly necessary' scrutiny required by the proportionality test.[60] The Court further established that the Directive does not ensure a high level of protection since it does not guarantee the 'destruction of the data at the end of the data retention period' and, more

54 *Digital Rights Ireland* (n 10) para 47. The Court cites the ECHR and ECtHR case law on Article 8 of the ECHR; in particular: *S. and Marper* v. *The United Kingdom*, App nos. 30562/04 and 30566/04 (ECtHR, 4 December 2008).

55 Ibid para 56.

56 Ibid paras 58–59.

57 Ibid para 57.

58 Ibid para 60.

59 Ibid paras 61–62.

60 Ibid para 64.

importantly, it does not require that the data in question is 'to be retained within the European Union'.[61] As a result, the data could be held in a territory beyond European jurisdiction, with potential unforeseeable effects. In order to avoid this risk, the Court required the collection and retention of the data to take place within the EU. This request would necessitate the reorganization of all online services provided by the major Internet companies, who usually collect data using servers installed all over the world, without any sort of geographical limitation.

For all these reasons, taken as a whole, the Court argued that the Data Retention Directive has exceeded the limits imposed by the proportionality test as enshrined in Arts.7, 8 and 52 of the Charter and declared the Directive 2006/24 completely invalid.

6 The Consequences of the CJEU Decision

The consequences of this decision must be viewed in the light of Arts. 267 and 264 of the TFEU as interpreted by the Court itself: when a decision of invalidity is given in a preliminary ruling, the effects of this declaration have the same effect as a judgment adopted by Article 264 TFEU.[62] The effects of the decision are retroactive (i.e. from the point when the Data Retention Directive came into force) and impinge on all national courts across the EU.[63] Consequently, when a preliminary ruling declares a directive invalid, it binds not only European Institutions, but also domestic courts. The decision therefore constitutes a *de facto* annulment and must be considered as *erga omnes*.

From a European legislative point of view, it is clear that both the European Parliament and the Council need to recast data retention legislation in the light of the principles as set forth by the CJEU, following the precise guidelines given in its reasoning. Any new legislative framework must, therefore, address all the concerns raised by the Court in its decision. In particular, under a new legislative framework, data should not be collected in a generalised, indiscriminate manner, but rather a clear relationship between the data collected and a serious crime should be established. The exact definition of a 'serious crime' should be made explicit. Additionally, the identity of the competent authorities with access to the retained data and the procedural steps required for obtaining data should be spelled out. Similarly, the data should be destroyed

61 Ibid paras 67–68.

62 Joined Cases C-120/06P and 121/06P *FIAMM and Others* [2008] ECR I-06513, para 123.

63 Case C-453/00 *Kühne & Heitz NV* [2004] CJEU I-00837.

after a determined period, which needs to be reduced to the minimum possible. Also, it is essential that any data collected be retained within the EU.

With regard to the national legislative dimension, there is a corresponding need to revise and reconstruct national provisions in order to transpose the principles established by the CJEU to the legal framework of each Member State. Until there is a new legislative framework for data retention that addresses the concerns expressed by the Court, domestic courts must have regard to the principles expressed in the guidelines presented by the CJEU. The main legal basis for arguing in favour of the definitive nature and the *erga omnes* effect of the decision rest on the fundamental principles of legal certainty and the uniform application of European law. A second legal basis which supports the applicability of the decision in all Member States of the EU is Article 51 of the Charter. This Article defines the scope of the Charter itself and states that its provisions 'are addressed to the institution and bodies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law'.[64] With the invalidity of the Directive at issue, it is necessary now to identify another European legal basis, essential for the direct application of the Charter across Member States. Article 15 of the Electronic Communications Directive could achieve this objective.[65] This Article recognizes that all the restrictions on the Electronic Communications Directive adopted by Member States 'shall be in accordance with the general principles of Community law, including those referred to in Arts.6(a) and (2) of the Treaty on European Union'. This means that national lawmakers have to adopt laws in accordance with the Charter and the ECHR and, in turn, with their interpretation provided by the CJEU and the ECtHR.

In the context of domestic courts dealing with the transposition of the Directive into national legislation as well as the guidelines and principles arising from the current ruling, several different scenarios are possible. In the first of these, judges across Europe, who are requested to apply transposition provisions of the invalid Directive, have to disapply provisions that are no longer in line with European law following the invalidity decision taken by the CJEU. This principle has also been confirmed in the case *Åklagaren*, according to which there is an obligation for the national courts to disapply 'any provision contrary to a fundamental right guaranteed by the Charter conditional upon that infringement being clear from the text of the Charter or the case-law related

64 S Peers, 'Are national data retention laws within the scope of the Charter?' (*EU Law Analysis*, 20 April 2014 <http://eulawanalysis.blogspot.nl/2014/04/are-national-data-retention-laws-within.html> accessed 1 September 2014.

65 Directive 58/2002; cf Directive 95/46/EC, Art. 13.

to it'.[66] In the second scenario, it is possible for any domestic Court to request a new preliminary ruling by the CJEU regarding the compatibility of the provisions of Member States with the new European framework. The Court will certainly confirm its precedent decision declaring the incompatibility of the national law with the EU law. In the third scenario, national transposition provisions could be challenged in constitutional courts by national judges on the ground of the right to privacy and/or the supremacy of the EU law. The fourth scenario envisages countries waiting for a proper implementation of the now-invalid Directive. In this spectrum there are Member States, including Germany and Sweden, where circumstances are somewhat paradoxical. Following the ruling of the German Constitutional Court declaring the illegitimacy of the transposition provisions, the European Commission started an infringement proceeding against Germany because it had refused to adopt a new transposition.[67] Similarly, Sweden, one of the last countries to have transposed the Directive, was fined twice by the European Commission for incomplete fulfilment of the Directive.[68] In this fourth scenario we should also consider Member States in which cases are pending before constitutional courts. Within this category, the experience of Slovakia is peculiar since its Constitutional Court had suspended the national transposition of the Directive in order to wait for the decision of the CJEU.[69] Now that the ruling has been adopted the Slovakian Constitutional Court is expected to conclude its judgment and declare the illegitimacy of the transposition laws. Equally, the Slovenian Constitutional Court had suspended proceedings (although not the transposition law) while waiting for the ruling of the CJEU,[70] which is now available to them. Consequently, in a recent judgement the Slovenian Constitutional Court has struck down the national law.

In declaring the Data Retention Directive invalid, the CJEU has removed the legal basis for the mass surveillance of the entire European population, opening up the prospect of a future of more robust protection of fundamental rights - in particular the right to privacy within the information and

66 Case C-617/10 *Åklagaren*v. *Hans ÅkerbergFransson* (CJEU, 26 February 2013) para 48.

67 Case C-329/12 *European Commission* v. *Germany* (CJEU, 5 June 2014).

68 Case C-185/09 *Commission* v. *Kingdom of Sweden* [2010] ECR I-00014; Case C-270/11 *European Commission* v. *Kingdom of Sweden* (CJEU, 30 May 2013).

69 'Ústavnýsúdpozastavilsledovanieobčanov' (*European Information Society Institute*, 25 April 2014) <http://www.eisionline.org/index.php/projekty-m/ochrana-sukromia/75-ussr-pozastavil-sledovanie> accessed 1 September 2014.

70 In fact, the Slovenian Court has recently held that data retention is unconstitutional; see <http://www.digitalrights.ie/data-retention-slovenia-unconstitutional> accessed 1 September 2014.

communication society. In this instance, the individual's right to privacy has prevailed over the interests of collective security[71] due to the action of the Court in placing the fundamental right at the centre of its reasoning.

7 Conclusion

The original Data Retention Directive represented an example of the securitarian approach taken after 9/11, which has subsequently become the default legislative stance throughout the world. In fact, the Directive's obligations to collect and retain metadata in order to investigate, detect and prosecute serious crimes, including terrorism, has raised grave concerns about the impact on fundamental rights in the name of public security. The need for robust security has prevailed over the protection of fundamental rights. On the contrary, legislation affecting citizens of the EU must strike a balance between legitimate security concerns on the one hand, and fundamental rights guaranteed by the Charter and national Constitutions on the other.

The above-mentioned concerns are even more important when they affect European law: the Directive created an echo effect among Member States, as its transposition into national legislation has carried into domestic fields additional concerns about fundamental rights. Consequently, the transposition of the Directive at the national level has multiplied the inherent problems of the legislation and abridged the protection of fundamental rights in EU countries.

Directive 2006/24 placed several serious restrictions on fundamental rights – in particular the right to privacy and the right to protection of personal data – and for this reason, in light of Article 52 of the Charter, the CJEU has declared the Directive invalid. This decision has profound and long-lasting implications which will colour future European and national legislation in this field. By reaffirming the principle that fundamental rights, as laid down in the Charter and the ECHR, must be respected, the CJEU has in effect established the boundaries within which any legislation concerning privacy and data protection and its transposition at the national level should be taken. In so doing, the Court played the role of a quasi-constitutional court. In light of the decision of 8th April 2014, Member States can no longer restrict or limit the right to privacy on the basis of an extensive interpretation of the open language employed in the Directive. For example, the measures adopted as part of the

71 Cf A Vedaschi, 'Has the balancing of rights given way to a hierarchy of values?' (2010) 1 Comparative Law Review 1 ff.

counterterrorism effort have also been applied indiscriminately to other serious crimes. Such an extensive interpretation is not in accordance with the principle that restrictions on fundamental rights have to be interpreted narrowly.

In this judgment, the CJEU applied the proportionality test as strictly as the ECtHR does in case-law on similar matters. In fact, the CJEU employed principles set forth by the ECtHR, making it clear that, when fundamental rights such as the right to privacy are at stake, any abridgement of these rights should correspond to a 'pressing social need'.[72] Furthermore, proportionality between such pressing need and the measures taken should be demonstrated on the basis of relevant reasons. Treating each and every European citizen as a potential suspect goes far beyond the scope of the global fight against international terrorism. It should, therefore, be rejected: 'taking surveillance measures without adequate and sufficient safeguards can lead to destroying democracy on the ground of defending it'.[73]

72 *S. and Marper* (n 54).

73 *Klass* v. *Germany* (n 36).