scripted

Volume 10, Issue 3, October 2013

THE WAY TO LUXEMBURG: NATIONAL COURT DECISIONS ON THE COMPATIBILITY OF THE DATA RETENTION DIRECTIVE WITH THE RIGHTS TO PRIVACY AND DATA PROTECTION

Eleni Kosta[*]

Abstract

The Data Retention Directive has given rise to significant concerns within the European Union regarding its compatibility with existing fundamental rights, and more specifically with the rights to privacy and data protection. Since 2008 numerous national courts have declared unconstitutional specific provisions of the national laws transposing the Directive on the basis that they violate the rights to privacy and data protection. Although a first impression may be created that the national courts have decided upon the compatibility of the Directive with those rights, a closer look into the reasoning of the various courts reveals that this might not be the case. To date, two requests for a preliminary ruling on the compatibility of the Data Retention Directive with fundamental rights have been filed at the Court of Justice of the European Union. This paper studies the rationale of the decisions of the national courts that have dealt with data retention with regard to the rights to privacy and data protection in order to identify the main arguments in the reasoning of the courts. The paper also examines whether these national court decisions could influence the Court of Justice, in view of its anticipated decision with regard to the cases pending before it.

DOI: 10.2966/scrip.100313.339

[*] Assistant Professor, Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, Tilburg, The Netherlands. The author would like to thank Bert-Jaap Koops, Ronald Leenes, Judith Rauhofer and Alexin Zoltán for their valuable comments. Any mistakes remain the authors' alone.

1. Introduction

The adoption of the Data Retention Directive[1] placed an obligation on providers of publicly available electronic communications services and of public communications networks ("communication service providers") to retain certain communications data for law enforcement purposes. Prior to the introduction of the Directive, the debate surrounding the adoption of a European legal instrument had primarily focused on the issue of its legal basis. Specifically it was debated whether data retention should be regulated via a first or third pillar legal instrument, namely whether it would be a Directive or a Framework Decision. The adoption of the Data Retention Directive and the confirmation from the European Court of Justice that it was correctly adopted as a first pillar legal instrument[2] has since put an end to this initial debate. However, the Directive has subsequently given rise to significant concerns within the European Union regarding its compatibility with existing fundamental rights, and more specifically with the rights to privacy and data protection.

Since 2008 numerous national courts have declared unconstitutional specific provisions of the national laws transposing the Directive on the basis that they violate the rights to privacy and data protection. They include the Bulgarian Supreme Administrative Court[3] (2008), the Romanian Supreme Court[4] (2009), the German Constitutional Court[5] (2010), the Czech Constitutional Court[6] and the Cyprus Supreme Court[7] (both 2011). In addition, similar cases are pending in front of national

---

[1] Directive 2006/24/EC of the European Parliament and of the Council 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, Official Journal L105/54 (March 15 2006).

[2] Case C-301/06 *Ireland v European Parliament and Council of the European Union* [2009] ECR I-00593

[3] Bulgarian Supreme Administrative Court, No 13627, 11 December 2008, available only in Bulgarian at http://www.capital.bg/getatt.php?filename=o_598746.pdf (accessed 10 Jul 2013).

[4] Decision of the Romanian Constitutional Court 1258, 08 October 2009. The original decision in Romanian is available at http://www.legi-internet.ro/fileadmin/editor_folder/pdf/Decizie_curtea_constitutionala_pastrarea_datelor_de_trafic.pdf (accessed 10 July 2013) Unofficial translation by Bogdan Manolea and Anca Argesiu, available at http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf (accessed 10 Jul 2013), upon which the analysis of the author relied.

[5] German Constitutional Court (Bundesverfassungsgericht), Decision of 02 March 2010, *NJW* 2010, 833, para. 204; A-B 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* 503-517 at 512.

[6] Czech Constitutional Court, Decision of 22 March 2011 on petition Pl. ÚS 24/10, available online in Czech at http://www.usoud.cz/fileadmin/user_upload/ustavni_soud_www/Aktualne_prilohy/2011_03_31b.pdf. Translation by the Constitutional Court in English, available online at http://www.usoud.cz/en/decisions/?tx_ttnews%5Btt_news%5D=40&cHash=bbaa1c5b1a7d6704af6370fdfce5d34c (accessed 08 Jul 2013).

[7] Supreme Court of Cyprus, Decision of civil applications 65/2009, 78/2009, 82/2009 & 15/2010-22/2010, 01 February 2011, available in Greek at

courts in Poland, Slovenia and Slovakia, while a case that was initiated in 2008 by the Hungarian Ombudsman has been terminated because of changes to the procedures before the Hungarian Constitutional Court. Although a first impression may be created that the national courts have decided upon the compatibility of the Directive with the rights to privacy and data protection, a closer look into the reasoning of the various courts will reveal that this might not be the case.

Despite the fact that it was often requested by the claimants, none of the aforementioned courts decided to send a request for a preliminary ruling on the compatibility of the Data Retention Directive with fundamental rights to the Court of Justice of the European Union ("Court of Justice"). The Irish High Court[8] eventually made such a request in June 2012 followed by a similar request from the Austrian Constitutional Court six months later[9]. At the time of writing the Court of Justice's decision on these cases is still outstanding.

This paper will study the decisions of the national courts that have dealt with data retention with regard to the right to privacy and data protection in order to identify potential similarities and differences in their reasoning. The aim of this paper is to provide an overview of the arguments that were presented and the rationale followed by the national courts when dealing with specific facets of data retention. The paper will also examine whether these national court decisions could influence the Court of Justice, with a view to its anticipated decision on the cases pending before it.

2. Overview of the Data Retention Directive

The Data Retention Directive harmonises national laws on communication service providers' obligations to retain certain communications data generated or processed by them so that they are available for the purpose of investigation, detection and prosecution of serious crime[10]. The Directive itself does not include a definition of the term "serious crime"; this is left to the Member States to regulate in their national legislation. The Council urged the Member States to have due regard to the criminal offences listed in Article 2(2) of the Framework Decision on the European Arrest Warrant[11] and crime involving telecommunications.[12]

---

http://www.supremecourt.gov.cy/judicial/sc.nsf/0/5B67A764B86AA78EC225782F004F6D28/$file/65-09.pdf (accessed 08 Jul 2013).

[8] Reference for a preliminary ruling from High Court of Ireland made on 11 June 2012 — Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, Case C-293/12, O.J. C258/11 (25.08.2012).

[9] Request for a preliminary ruling from the Verfassungsgerichtshof (Austria) lodged on 19 December 2012 — Kärntner Landesregierung and Others, Case C-594/12, O.J. C79/7 (16.03.2013). This referral was soon followed by a second request for a preliminary ruling originating this time from the Austrian Data Protection Commissioner, dealing specifically with Article 7 of the Data Retention Directive. One of the questions referred to the Court dealt with the interpretation of Article 7(c) of the Data Retention Directive (Case C-46/13) and, among others, its compatibility with Article 8(2) ECHR, Pending Case, H (C-46/13), OJ C147/3 (25.05.2013). Due to the specific scope of this question, the request for a preliminary ruling will not be further discussed.

[10] Data Retention Directive, Art.1(1).

[11] Council Framework Decision 2002/584/JHA on the European Arrest Warrant and the surrender procedures between Member States, O.J. 2002 L190/1.

The data to be retained are traffic data (that is, data about the sender, recipient and time of a communication), location data and data necessary to identify the subscriber or registered user.[13] The content of a communication is specifically excluded from the retention requirement.[14] Furthermore, traffic data relating to web browsing are not to be retained. With regard to Internet traffic the Directive only covers data relating to Internet access, Internet email and Internet telephony. The Directive provides that the data must be retained for a period between six months and two years from the date of the communication.[15]

The Data Retention Directive requires that retained data are provided only to the competent national authorities and in accordance with national law. The Directive left it to the Member States to specify the procedures that have to be followed and the conditions to be fulfilled in order for the competent national authorities to gain access to retained data.[16] These procedures and conditions have to be defined in accordance with the requirements of necessity and proportionality, in the light of the European Convention of Human Rights (ECHR) as interpreted by the European Court of Human Rights.[17]

According to the Data Retention Directive the providers must comply with four fundamental obligations related to the security of data retained by them. They must ensure that the retained data are of the same quality and subject to the same security measures and protections as other data on the network;[18] the retained data must be subject to appropriate technical and organisational measures to protect them against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;[19] appropriate technical and organisational measures must be taken in order to ensure that the retained data can only be accessed by specially authorised personnel;[20] and all other retained data, except those that have been accessed and preserved, must be destroyed at the end of the retention period.[21] The data must be retained in such a way that they (as well as any other necessary information relating to such data) can be transmitted upon request to the competent authorities without undue delay.[22]

---

[12] Council of the European Union, 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, [first reading] – Statements", 5777/06 ADD 1, February 10, 2006.

[13] A detailed list with the categories of data to be retained is contained in Aricle 5 of the Data Retention Directive.

[14] Article 5(2) Data Retention Directive.

[15] Article 6 Data retention Directive.

[16] Article 4 Data Retention Directive.

[17] Article 4 Data Retention Directive.

[11] Article 7(a) Data Retention Directive.

[12] Article 7(b) Data Retention Directive.

[13] Article 7(c) Data Retention Directive.

[14] Article 7(d) Data Retention Directive.

3. Early Reflections on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection

The potential impact of the Data Retention Directive on the rights to privacy and data protection was already acknowledged prior to the national court procedures discussed in this paper. The European Commission, when presenting its proposal for the Directive in 2005, admitted that the Directive would have an effect on the rights to privacy and to protection of personal data, which are protected in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (EU Charter) respectively. However, the Commission found that any interference with these rights by the Directive was justified as it was in line with Article 52 of the EU Charter, which delineates the scope of the guaranteed rights.[23] In particular, the Commission argued that "the limitations on these rights provided for by the proposal are proportionate and necessary to meet the generally recognised objectives of preventing and combating crime and terrorism".[24]

The Article 29 Data Protection Working Party took a position against the blanket retention of user data even before the adoption of the Data Retention Directive. In one of its first opinions on data retention, it concluded that "the mandatory retention of all types of data on every use of telecommunication services for public order purposes, under the conditions provided…, is not acceptable within the legal framework set in Art. 8 ECHR."[25] Consistent with this position, the Working Party criticised the Commission's 2005 Proposal for the Data Retention Directive on the grounds that the Directive should not undermine fundamental human rights, including the right to data privacy.[26] The European Data Protection Supervisor (EDPS) also warned that "notwithstanding the importance of the proposal for law enforcement, it may not result in people being deprived of their fundamental right to have their privacy protected."[27] The EDPS requested further safeguards and criticised "the simple

---

[23] Article 52(1) of the EU Charter reads as follows "1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others".

[24] Commission of the European Communities, 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, COM(2005) 438 final (21 September 2005).

[25] Article 29 Data Protection Working Party, Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism. [Proposal presented by France, Ireland, Sweden and Great Britain (Council doc. 8958/04 – April 28, 2004)], WP99, (November 09, 2004), p.5

[26] Article 29 Data Protection Working Party, Opinion 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 of 21.09.2005), WP113, (October 21, 2005), p. 2

[27] 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 (COM(2005) 438 final), OJ298/1, 29.11.2005, para. 4.

reference to the existing legal framework on data protection" in the Commission proposal as insufficient.[28]

Soon after the adoption of the Data Retention Directive, its legal basis was challenged by Ireland, supported by the Slovak Republic, before the Court of Justice. Ireland sought the annulment of the Directive on the grounds that it was not adopted on an appropriate legal basis.[29] It argued that the purpose of the Directive was to facilitate the investigation, detection and prosecution of serious crime, including terrorism, and that data retention should therefore be regulated under a framework decision adopted under the "third pillar" legislative procedure.[30] Despite the fact that the case did not focus on the content of the Directive, the non-profit organisation Working Group on Data Retention (Arbeitskreis Vorratsdatenspeicherung), supported by 43 European NGOs, submitted to the Court of Justice an *amicus curiae* brief ("friends of the court") urging the Court to base its decision on the incompatibility of the Directive with human rights.[31] The *amicus curiae* brief[32] provided an analysis arguing that the Data Retention Directive violated the right to privacy, as safeguarded in Article 8 ECHR.[33]

---

[28] 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 (COM(2005) 438 final), OJ298/1, 29.11.2005, para. 13.

[29] Case C-301/06, *Ireland v Council and European Parliament*, judgment of February 10, 2009, [2009] E.C.R. I-593.

30 Case C-301/06, Ireland v Council and European Parliament, judgment of February 10, 2009, [2009] E.C.R. I-593.

[31] http://www.vorratsdatenspeicherung.de/images/data_retention_brief_08-04-2008.pdf (accessed 10 Jul 2013)

[32] Case C-301/06, *Ireland v Council and European Parliament*, judgment of February 10, 2009, [2009] E.C.R. I-593.See also joined Cases C-317 and C-318/04, *European Parliament v Council* [2006] E.C.R. I-4721 concerned Council Decision 2004/496/EC of May 17, 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (O.J. 2004 L183/83, and corrigendum at O.J. 2005 L255/168); the Court of Justice held that the transfer of Passenger Name Records ("PNR") data, collected in airlines' computer reservation systems, to the US Customs and Border Protection constituted processing operations concerning public security and the activities of the state in the area of criminal law. The Court considered that the transfer of the PNR data was not within the airline's commercial activities, but was processing for operations concerning public security and the activities of the state in areas of criminal law. Many privacy advocates had hoped that the Court would find that the retained PNR data had been collected by the airlines for commercial purposes and that they should therefore not be further processed for law enforcement purposes.

[33] The amicus curiae brief argued also that blanket data retention was infringing the right to freedom of expression (Art. 10 ECHR) and the protection of property (Art. 1 of the first protocol to the ECHR). It should be remembered at this point that the brief referred only to the ECHR, as the EU Charter had not been yet ratified at that moment. However, the Court of Justice did not examine at all the compatibility of the Directive with human rights and held that the Directive relates predominantly to the functioning of the internal market and was correctly adopted on the basis of Article 95 of the EC Treaty.

4. Data Retention Legislation in Front of National Courts of Member States

Soon after the adoption of the Directive, national courts began to examine the compatibility of data retention with fundamental rights and more specifically with the rights to privacy and data protection. This section will present the national court decisions that have been published on the national implementations of the Data Retention Directive in chronological order. It will examine the points raised by the courts with regard to the compatibility of the national data retention laws implementing the Directive with the rights to privacy and personal data, and it will highlight whether and under which conditions references have been made on the actual compatibility of the Directive itself with fundamental rights.

4.1 Bulgaria

Bulgaria transposed the Data Retention Directive in Regulation 40[34] on the categories of data and the procedure under which they would be retained and disclosed by companies providing publicly available electronic communication networks and/or services for the needs of national security and crime investigation. Soon after the transposition of the Directive in Bulgaria, the NGO "Program Action to Information"[35] filed a complaint at the Bulgarian Supreme Administrative Court claiming that Article 5 of the Regulation that transposed the Directive in Bulgaria was infringing the right to privacy.

Article 5 of the Regulation allowed passive technical access to all retained data for broad purposes through a dedicated computer terminal. It also provided that access to data was allowed "for the needs of the operative investigation activities" and permitted investigation, prosecution and judicial authorities to access the retained data "for the needs of a trial" and security services to access them "for national security needs". These purposes were formulated in a very broad way and the NGO argued that the Regulation did not provide sufficient safeguards for the protection of citizens' private life as required by the Bulgarian Constitution.[36] The Court found that the provisions of Article 5 violated the right to privacy as safeguarded in Article 32(1) of the Bulgarian Constitution and Article 8 ECHR, as it did not provide the necessary safeguards against the violation of citizens' constitutional rights did not make reference to specific laws that would be relevant, such as Article 5, and did not specify any conditions on which interference with the right to private life and personal data of citizens would be allowed.[37] As a result, the Court annulled Article 5 of the Regulation, as it did not provide any limitations or guarantees for the right to privacy.[38]

---

[34] Regulation No.40 of the Ministry of Interior of 7 January 2000, available in Bulgarian at http://lex.bg/laws/ldoc/2135577924 (accessed 10 Jul 2013).

[35] http://www.aip-bg.org

[36] Art.32(1) of the Bulgarian Constitution.

[37] Bulgarian Supreme Administrative Court, No 13627, 11 December 2008, available only in Bulgarian at http://www.capital.bg/getatt.php?filename=o_598746.pdf (accessed 10 Jul 2013).

[38] Bulgarian Supreme Administrative Court, No 13627, 11 December 2008.

The Bulgarian Court did not refer to the Data Retention Directive itself, nor did it criticise blanket data retention. Rather the Court focused on access to the retained data, examining specifically the constitutionality of Article 5 of the Regulation in the light of the broad number of authorities that were granted access to that data for broad purposes. Realistically, the decision of the Bulgarian Supreme Administrative Court therefore deals with the issue of access to data and the conditions under which such access can be in line with the right to privacy of citizens. Nevertheless, the decision is important, as it was the first decision of a national court that examined data retention in relation to the right to privacy of citizens, albeit on an issue that the Directive left to the Member States to regulate. Moreover, the direct reference to Article 8 ECHR rather than merely to the relevant provision of the Bulgarian Constitution illustrates the importance of data retention aspects with regard to the right to privacy.

4.2 Romania

In 2009, the Romanian Constitutional Court was asked to examine the constitutionality of the Romanian transposition of the Data Retention Directive. A Romanian NGO, the Civil Society Commissariat, requested the telecommunications provider Orange to honour its contracts, which guaranteed the confidentiality of telephone conversations.[39] The Commissariat argued that the Romanian law implementing the Data Retention Directive (Romanian data retention legislation)[40] violated fundamental rights, including the right to privacy, freedom of expression and freedom of movement.[41]

The Romanian Court[42] held that although the applicant criticised the Romanian data retention legislation in its entirety, it focused specifically on the provisions of Articles 1 and 15 of the Act. Article 1 of the Act defines the scope of the Romanian data retention legislation,[43] while Article 15 sets out the obligation of providers of

---

[39] A Bannon, "Romania retrenches on data retention" (2010) 24:2 *International Review of Law, Computers and Technology* 145-152 at 150

[40] Romanian law no. 298/2008 regarding the retention of the data generated or processed by the public electronic communications service providers or public network providers, as well as the modification of law 506/2004 regarding the personal data processing and protection of private life in the field of electronic communication area", Official Monitor of Romania, Part I, no. 780, 21 November 2008.

[41] A Bannon, "Romania retrenches on data retention" (2010) 24:2 *International Review of Law, Computers and Technology* 145-152 at 150.

[42] Decision of the Romanian Constitutional Court 1258, 08 October 2009. The original decision in Romanian is available at http://www.legi-internet.ro/fileadmin/editor_folder/pdf/Decizie_curtea_constitutionala_pastrarea_datelor_de_trafic.pdf (accessed 10 July 2013) Unofficial translation by Bogdan Manolea and Anca Argesiu, available at http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf (accessed 10 Jul 2013), upon which the analysis of the author relied.

[43] Art.1 – (1) The present law established the obligation of the electronic communication providers of services and public networks to retain certain data produced or processed during their activity of providing electronic communication services, in order to make them available to the competent authorities to use them in activities of enquiry, detection and proceedings against serious crimes.

(2) The present law is applied to traffic and localisation data of the physical and legal persons, as well as to the related data necessary to identify the subscriber or the registered user.

electronic communications networks and services to transfer the data to the competent authorities upon request.[44] The Court was asked to examine the compatibility of the Romanian data retention legislation, and more specifically of article 1 and 15, with the right to freedom of movement[45], the right to family and private life[46], the secrecy of correspondence[47] and the right to freedom of expression.[48]

Within the scope of the paper, we are going to focus on the argumentation of the Court with regard to the right to private life. The Court repeated that the right to privacy and family life is protected under Article 12 of the Universal Declaration of Human Rights, Article 17 of the International Covenant regarding civil and political rights, Article 8 ECHR and Article 26 of the Romanian Constitution. The Romanian Court clarified that the right to privacy and family life also includes the secrecy of correspondence, which can either be encompassed in one Article, as in the case of Article 8 ECHR, or can also exist as a distinct Article, as is the case in the Romanian Constitution, there the secrecy of communications is protected under Article 28.

The Court recognised that the right to privacy (including the secrecy of communications) is not an absolute right and examined whether the Romanian data retention law was fulfilling the necessary requirements in order to establish a justified interference, as specified in Article 8(2) ECHR and Article 53 of the Romanian Constitution. The Court examined Article 20 of the Romanian data retention law, which allows state institutions active in ensuring national security to access the retained data "under the conditions established by the normative acts that regulate the activity of national security". The Court criticised specifically the fact that Article 20 allowed access to data for the prevention and counteracting of "threats to national security". The Court considered the term "threats to national security" as too broad, as it does not provide specific criteria of what could be interpreted as a threat to national security.[49] The Court also criticised that according to Article 20 "the state institutions

---

(3) The present law does not apply to the content of the communication or information accessed while using an electronic communication network.

(4) The enforcement of the present law shall be done by respecting law 677/2001 for people's protection on processing personal data and the free movement of these data, with the subsequent modifications, as well as law 506/2004 regarding the personal data processing and protection of private life in the field of electronic communication area, with the subsequent changes.", as quoted in the decision of the Romanian Constitutional Court.

[44]Article 15 of the Romanian data retention law reads as follows: "The public network communication providers and the electronic communication services providers have the obligation, at the request of the competent authorities, based on the authorization issued according to art 16, to send forthwith the retained data to these authorities according to the present law, with the exception of the force majeure cases.".

[45]Article 25 Romanian Constitution.

[46]Article 26 Romanian Constitution.

[47]Article 28 Romanian Constitution.

[48]Article 30 Romanian Constitution.

[49] C Murphy, "Note on Romanian Constitutional Court, Decision No. 1258 of 8 October 2009 regarding the unconstitutionality exception of the provisions of Law No. 298/2008 regarding the retention of the data generated or processed by the public electronic communications service providers or public network providers, as well as for the modification of Law No. 506/2004 regarding the personal data processing and protection of private life in the field of electronic communication area" (2010) 47 *Common Market Law Review* 933–941 at 935.

with attributions in this field may have access [to the retained data], under the conditions established by the normative acts that regulate the activity of national security". This wording was again considered too broad, as it did not allow access to the retained data only to state authorities that were entrusted with the protection of national security and public order. The national legislator could extend the right to access the retained data to other state institutions, thus broadening considerably the circle of competent national authorities that could get access to the retained data.[50]

Moreover the Court criticised the continuous character of the retention of citizens' data by providers. The Court highlighted that the State has predominantly negative obligations to abstain with regard to the rights to privacy as well as processing of personal data of citizens and reflected on the principle of proportionality with regard to the law at stake. The Court highlighted that the harm in an unacceptable way to the exercise of the right to privacy is:

> …the legal obligation with a **continuous character**, generally applicable, of data retention. This operation equally addresses all the law subjects, regardless of whether they have committed penal crimes or not or whether they are the subject of a penal investigation or not, which is likely to **overturn the presumption of innocence** and to **transform a priori all users** of electronic communication services or public communications networks **into people suspected of committing terrorism crimes** or other serious crimes. Law… has a large applicability – practically to all physical and legal persons that are users of electronic communications services or public communication networks - so, it can't be considered to be in agreement with the provisions in the [Romanian] Constitution and [ECHR] regarding the guaranteeing of the rights to private life [and] secrecy of the correspondence… (emphasis added).[51]

The Court in its ruling made numerous references to the jurisprudence of the European Court of Human Rights and repeated that Court's reasoning in the case of *Klass and others v Germany*[52] that "taking surveillance measures without adequate and sufficient safeguards can lead to 'destroying democracy on the ground of defending it".[53]

Consequently, the Romanian Court went beyond the request of the applicant that was mainly challenging the constitutionality of Article 1 and 15 of the Romanian data retention law and declared the whole law unconstitutional as breaching, among others the right to privacy and the secrecy of correspondence.[54] Although the Romanian Constitutional Court did not refer explicitly to the Data Retention Directive, its criticism went beyond specific provisions of the transposing Romanian law.[55] The

---

[50] Romanian Constitutional Court, decision 1259, 08 October 2009

[51] Romanian Constitutional Court, decision 1259, 08 October 2009

[52] Klass and Others v. Germany, 6.9.1987, no. 5029/71.

[53] Romanian Constitutional Court, decision 1259, 08 October 2009.

[54] Romanian Constitutional Court, decision 1259, 08 October 2009.

[55] C Murphy, "Note on Romanian Constitutional Court, Decision No. 1258 of 8 October 2009 regarding the unconstitutionality exception of the provisions of Law No. 298/2008 regarding the

Romanian Court criticised the spirit of data retention as a whole, including the continuous character of the obligation to retain traffic and location data of citizens, which is undoubtedly a characteristic of the European Data Retention Directive. The argumentation of the Romanian Constitutional Court mainly focused on the concepts of related data and national security.[56] Nevertheless, instead of annulling the relevant provisions of the Romanian law, the Court made a general reasoning and addressed the very nature of data retention as a measure infringing the right to privacy. In its decision the Court did not examine the issue of supremacy or European law and did not make any reference to the Data Protection Directive, so its position towards the supremacy of European over national law "can best be described as ambivalent".[57] This will be an interesting issue on which the Court of Justice will possibly be called upon to comment on, as will be further elaborated in the following section.

4.3 Germany

The adoption of a law implementing the Data Retention Directive in Germany faced immense public outcry. After the transposition of the Directive into German law, the German Constitutional Court was called upon to decide on the compatibility of specific provisions of the legislation with the right to the secrecy of communications[58] and the right to informational self-determination[59] protected in the German Basic Law (Constitution). The complaint was launched before the German Constitutional Court by 34000 citizens via an initiative of the Working Group on Data Retention (Arbeitskreis Vorratsdatenspeicherung). It challenged sections 113a, 113b of the Telecommunications Act[60] and section 100g of the Criminal Procedure Act (the latter to the extent that it allowed the collection of data that were stored in accordance with section 113a). Section 113a of the Telecommunications Act stated that the providers of publicly available communications services have a duty to store any kind of traffic data, excluding content data, for six months.[61] After that period, the retained data

---

retention of the data generated or processed by the public electronic communications service providers or public network providers, as well as for the modification of Law No. 506/2004 regarding the personal data processing and protection of private life in the field of electronic communication area" (2010) 47 *Common Market Law Review* 933–941 at 939.

[56] C Murphy, "Note on Romanian Constitutional Court, Decision No. 1258 of 8 October 2009 regarding the unconstitutionality exception of the provisions of Law No. 298/2008 regarding the retention of the data generated or processed by the public electronic communications service providers or public network providers, as well as for the modification of Law No. 506/2004 regarding the personal data processing and protection of private life in the field of electronic communication area" (2010) 47 *Common Market Law Review* 933–941 at 940.

[57] C Murphy, "Note on Romanian Constitutional Court, Decision No. 1258 of 8 October 2009 regarding the unconstitutionality exception of the provisions of Law No. 298/2008 regarding the retention of the data generated or processed by the public electronic communications service providers or public network providers, as well as for the modification of Law No. 506/2004 regarding the personal data processing and protection of private life in the field of electronic communication area" (2010) 47 *Common Market Law Review* 933–941 at 941.

[58] Article 10 German Basic Law.

[59] Article 2(1) in conjunction with Article 1 German Basic Law.

[60] Telekommunikationsgesetz (TKG)

[61] Section 113a German Telecommunications Act

must be deleted. Section 113b of the Telecommunications Act specified the purposes for which the retained data can be accessed and used, in some case allowing access without an order from a judicial authority or a duty to notify the citizens concerned[62]. Finally, section 100g of the Criminal Procedure Act dealt with access to and use of the data for the purpose of criminal prosecution. Section 100g required prior judicial authorisation and provided for duties of notification and subsequent judicial relief.[63]This provision did not cover only data that were retained under the data retention regime, it also allowed access for the purpose of prosecuting all types of criminal offences, not just serious crime. This is despite the fact that section 100a(2) of the Act includes an exhaustive list of offences considered to be serious. If retained data is accessed to prosecute criminal offences that are committed by the means of telecommunications, such access must be proportionate to the aim pursued. In all other cases, no proportionality requirement was included in the relevant legislation.

The German Federal Constitutional Court highlighted that the issue of access to the retained data falls outside the scope of the Data Retention Directive and is left to the Member States to decide upon. In its settled case law the Court had developed the so-called *Solange* doctrine. According to this doctrine as long as (*solange*) the European Communities, especially via the case law of the European Court, generally ensure the effective protection of fundamental rights, and as long as such protection is considered substantially similar to the protection offered by the German Basic Law, the Court will no longer exercise its power to examine the compatibility of secondary Community legislation with the fundamental rights contained in the Basic Law[64]. In accordance with this doctrine, the Court therefore did not question the adequate protection of fundamental rights in the European legal order. Questioning whether the Data Retention Directive adequately protects fundamental rights of citizens, may very well have opened a Pandora's box of fundamental rights protection in Europe: the Court could on the one hand have questioned the role and the value of the EU Charter within the European legal system, while on the other hand, this could have opened the door for other national courts to start evaluating European legislation under the norms and standards of their national constitutions. In short, if the German Court had deviated from its *Solange* doctrine and had questioned the compatibility of the Data Retention Directive with fundamental rights protected by the European legal order, it could have initiated a "supranational legal crisis"[65] with severe impact on the relationship between European and national legislation.

However, the Court showed no appetite for such drastic measures. Instead, it found that the contested provisions are not compatible with Article 10(1) of the German Basic Law, which protects the privacy of correspondence, post and telecommunications, and decided their annulment. The German Constitutional Court did not examine the Data Retention Directive, as such an action would fall outside its

---

[62] Section 113b German Telecommunications Act

[63] Section 100g of the Code of Criminal Procedure

[64] Solange II – Wünsche Handelsgesellschaft, 22 October 1986, BVerfGE 73, 339, 2 BvR 197/83. An unofficial translation of the case in English can be found at Wünsche Handelsgesellschaft [1987] 3 CMLR 225.

[65] C DeSimone, "Pitting Karlsruhe against Luxembourg? German data protection and the contested implementation of the EU Data Retention Directive" (2010) 11:3 *German Law Journal* 291-317 at 316

competences. However the Court adopted a "rigorous proportionality check"[66] and came to the conclusion that the retention of data is only allowed in clearly specified situations and that access to and use of the retained data must be "under judicial oversight".[67] Encroachments are allowed only when they are carried out for a legitimate purpose, if they are necessary for the fulfilment of this purpose and if the means used to achieve this purpose are proportionate to it.[68]

Despite the fact that an obligation to retain telecommunications data is not unconstitutional in itself, the Court found that data retention constitutes a serious restriction of the right to privacy and therefore it has to be laid down in the legislation only for limited circumstances and pursuant to the principle of proportionality.[69] The Court found that the six-month retention period that was provided for in the German legislation is a retention period that can still be justified under the German Constitution[70], but it is a period that is close to the maximum limit that can be justified under proportionality considerations.[71] In its decision the Court implied that although the retention period of six months can be justified, an eventually longer retention period might not be acceptable under the German Constitution. The Court divided the need for proportionality as arising from the constitutional court into the following four criteria: (i) proportional security standards, (ii) proportional purpose limitation, (iii) transparency and (iv) judicial control and effective legal remedies.[72]

The Court found that "the challenged provisions guarantee neither adequate data security nor an adequate restriction of the purposes of use of the data. Nor do they in every respect satisfy the constitutional requirements of transparency and legal protection. The provision is therefore as a whole unconstitutional and void".[73]

---

[66] T Konstadinides, "Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem" (2011) 36 *European Law Review* 722-736 at 731.

[67] C DeSimone, "Pitting Karlsruhe against Luxembourg? German data protection and the contested implementation of the EU Data Retention Directive" (2010) 11:3 *German Law Journal* 291-317 at 314.

[68] German Constitutional Court (Bundesverfassungsgericht), Decision of 02 March 2010, *NJW* 2010, 833, para. 204; A-B 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* 503-517 at 512.

[69] European Commission, Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), Brussels, 18.4.2011, COM(2011) 225 final at 20.

[70] German Constitutional Court (Bundesverfassungsgericht), Decision of 02 March 2010, *NJW* 2010, 833, para. 270.

[71] German Constitutional Court (Bundesverfassungsgericht), Decision of 02 March 2010, *NJW* 2010, 833, para. 215.

[72] K de Vries, R Bellanova, P De Hert and S Gutwirth, "The German Constitutional Court judgement on data retention: Proportionality overrides unlimited surveillance (Doesn't it?)" in S Gutwirth, Y Poullet, P De Hert and R Leenes (eds.), *Computers, Privacy and Data Protection: an Element of Choice* (Springer Dordrecht Heidelberg London New York: Springer Science+Business Media B.V, 2011), 3-23 at 7-8.

[73] German Federal Constitutional Court, Press release no. 11/2010 of 2 March 2010, Judgment of 2 March 2010, Cases 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, available at http://www.bverfg.de/pressemitteilungen/bvg10-011en.html (accessed 10 Jul 2013).

The contested provisions related to the purposes for using the retained data and to data security. The Court found that the provisions infringed the privacy of telecommunications and annulled the relevant section of the relevant law.[74] The Court did not annul the legislation entirely but suspended it, asking for the immediate deletion of the data already collected and for the massive modification of the law in order to provide stricter conditions for the use and storage of the data.

4.4 Cyprus

In February 2011, the Supreme Court of Cyprus dealt with a case relevant to data retention. The Court ruled jointly on a number of civil applications[75] for certiorari, "i.e., a writ annulling the orders issued by several District Courts ordering the disclosure of telecommunication data concerning several persons who were relevant to criminal investigations to the Cyprus police".[76] The Court was asked to decide on the validity of orders for access to retained data based on Articles 4 and 5 of the Cypriot law 183(1)/2007 on the retention of telecommunications data for the investigation of serious penal crimes. The applicants questioned the compatibility of Articles 4 and 5 of the aforementioned law with the fundamental right to private and family life (protected under Article 15(1) of the Constitution of Cyprus) and the right to protection of secrecy of correspondence (protected under 17(1) of the Constitution of Cyprus). The police issued the orders to retained data and got access to the telephone calls from and to the telephones of the applicants by the providers. The Court admitted that this action was in principle an interference with the secrecy of communications and examined further whether this interference was justified under the Constitution. The Court examined the individual cases and decided that for three of them the interference was not justified, while in the fourth case the interference was justified, as the applicant was a prisoner and different legal rules were applicable.

What makes this case interesting is, on the one hand, the justification of the Supreme Court explaining why they were not allowed to question the spirit and the provisions of the Data Retention Directive and, on the other hand, the reasoning of the Court on what falls outside the scope of the Data Retention Directive.

The Cypriot law 183(1)/2007 on the retention of telecommunications data for the investigation of serious penal crimes was adopted in order to transpose the Data Retention Directive into the national legislation of Cyprus. The Court focused on the legal provisions that were put in place with the adoption of the aforementioned law, and the transposition of the Directive in the national legislation of Cyprus. The Court in its reasoning said that it would have to examine to what extent these provisions have led to a modification of the legislation relating to the constitutionally protected right to secrecy of communications of citizens, in such a way that would lift the

---

[74] German Constitutional Court (Bundesverfassungsgericht), Decision of 02 March 2010, *NJW* 2010, 833

[75] Supreme Court of Cyprus, Decision of civil applications 65/2009, 78/2009, 82/2009 & 15/2010-22/2010, 01 February 2011, available in Greek at http://www.supremecourt.gov.cy/judicial/sc.nsf/0/5B67A764B86AA78EC225782F004F6D28/$file/65-09.pdf (accessed 08 Jul 2013).

[76] C Markou, "The Cyprus and other EU court rulings on data retention: the Directive as a privacy bomb" (2012) 28 *Computer Law & Security Review* 468-475

secrecy of communications and would allow the access to communications data.[77] Article 1A of the Constitution of Cyprus was amended in 2006 and provides that

> [n]o provision of the Constitution shall be deemed as overriding any legislation, acts or measures enacted or taken by the Republic that are deemed necessary due to its obligations as a Member State of the European Union, neither does it prevent Regulations, Directives or other Acts or binding measures of a legislative character, adopted by the European Union or the European Communities or by their institutions or competent bodies thereof on the basis of the Treaties establishing the European Communities or the Treaty of the European Union, from having legal effect in the Republic.[78]

Therefore and with respect to Article 1 of the Constitution, the Court stated that, apparently, the adoption of the Cypriot law on data retention was a necessary measure deriving from the obligations of Cyprus towards the European Union. The Court had to examine to what extent this law overreaches what is necessary and proportionate to the obligations of the democratic state of Cyprus, so that the legal provision is considered prevailing of the constitutional provision that safeguards the secrecy of communications.[79] The Court found that the Directive does not impose any obligation of the Member States to set down provisions on the access to the retained telecommunications data of the citizens or on their transmission to the competent authorities. The issues of access to the retained data, as well as the transfer of these data to the competent authorities, fell outside the scope of the Data Retention Directive and were left to the Member States to regulate in their national legislation.[80] Therefore, the provisions of Article 4 and 5 of the Cypriot data retention law were not covered by Article 1A of the Constitution of Cyprus.

In this decision the Supreme Court of Cyprus clarified that it did not have the competence to question the validity of the Data Retention Directive and the Cypriot law that was adopted to implement it. It further clarified that the cases at stake related only to the access to the retained data and the transfer to law enforcement authorities, issues that fell outside the scope of the Data Retention Directive. However, the Court examined whether the orders for access to retained data based on Articles 4 and 5 of the Cypriot data retention law were compatible with the rights to privacy and secrecy of communications, as protected under the Constitution of Cyprus. The Court found

---

[77] Supreme Court of Cyprus, Decision of civil applications 65/2009, 78/2009, 82/2009 & 15/2010-22/2010, 01 February 2011, available in Greek at http://www.supremecourt.gov.cy/judicial/sc.nsf/0/5B67A764B86AA78EC225782F004F6D28/$file/65-09.pdf (accessed 08 Jul 2013).

[78] Article 1A of the Constitution of the Republic of Cyprus.

[79] Supreme Court of Cyprus, Decision of civil applications 65/2009, 78/2009, 82/2009 & 15/2010-22/2010, 01 February 2011, available in Greek at http://www.supremecourt.gov.cy/judicial/sc.nsf/0/5B67A764B86AA78EC225782F004F6D28/$file/65-09.pdf (accessed 08 Jul 2013).

[80] Supreme Court of Cyprus, Decision of civil applications 65/2009, 78/2009, 82/2009 & 15/2010-22/2010, 01 February 2011, available in Greek at http://www.supremecourt.gov.cy/judicial/sc.nsf/0/5B67A764B86AA78EC225782F004F6D28/$file/65-09.pdf (accessed 08 July 2013); C Markou, "The Cyprus and other EU court rulings on data retention: the Directive as a privacy bomb" (2012) 28 *Computer Law & Security Review* 468-475 at 472.

that there was actually an interference with these rights in three out of the four examined cases and annulled the relevant order for access to retained data. In the fourth case, the Court found that there was interference, but the interference was justified on the grounds foreseen in the Constitution.

4.5 Czech Republic

A group of fifty-one Members of the Czech Parliament filed an application before the Czech Constitutional Court in order to have annulled specific provisions of the law that transposed the Data Retention Directive in the Czech Republic[81]. The Parliamentarians contested the Act *in abstracto* and not its specific application by state bodies.[82] The Czech Constitutional Court commenced its decision commenting on the admissibility of the application and criticising the fact that several of the applicants that were seeking the annulment of specific provisions of the law transposing the Directive had voted in favour of the adoption of the same law. Nevertheless, although the Court warned that in the future it would dismiss submissions filed under such circumstances, it did go into the substance of the case.[83]

The applicants invited the Czech Constitution Court to file a request for a preliminary ruling at the Court of Justice on whether the Data Retention Directive was consistent with Community law. However, the Court took the position that as Community law was not part of the Czech constitutional order, the Court was not competent to interpret it. Moreover it found that the Data Retention Directive allowed sufficient space for implementation in compliance with the Czech constitutional order.[84]

The Constitutional Court examined the compatibility of the contested provisions with the Czech Constitution and made extensive reference to the jurisprudence of the German Constitutional Court and the European Court of Human Rights. It also referred to the court decisions on data retention in Bulgaria, Romania and Cyprus. More specifically the Court focused on the right to privacy and informational self-determination. The Court acknowledged the fact that the Czech Charter of Fundamental Rights (hereafter 'Charter')[85] does not guarantee the right to respect of

---

[81] More specifically the applicants sought the annulment of Section 97, Paragraphs 3 and 4 of the Czech Act No. 127/2005 Coll., on Electronic Communications and Amendment of related Acts (Act on Electronic Communications), as well as Decree No. 485/2005 Coll. on the types of traffic and location data that are collected, the period of retention of the aforementioned data and the way in which they are transferred to the competent authorities in order to use the retained data.

[82] P Molek, "Czech Constitutional Court – Unconstitutionality of the Czech implementation of the Data Retention Directive; Decision of 22 March 2011, PI. ÚS 24/10" (2012) 8 *European Constitutional Law Review* 338-353, at 346.

[83] Czech Constitutional Court, Decision of 22 March 2011 on petition Pl. ÚS 24/10, available online in Czech at http://www.usoud.cz/fileadmin/user_upload/ustavni_soud_www/Aktualne_prilohy/2011_03_31b.pdf. Translation by the Constitutional Court in English, available online at http://www.usoud.cz/en/decisions/?tx_ttnews%5Btt_news%5D=40&cHash=bbaa1c5b1a7d6704af6370fdfce5d34c (accessed 08 Jul 2013), para. 2.

[84] Czech Constitutional Court, Decision of 22 March 2011 on petition Pl. ÚS 24/10, para. 26.

[85] Resolution of the Presidium of the Czech National Council of 16 December 1992 on the declaration of the Charter of Fundamental Rights and Basic Freedoms, as a part of the constitutional order of the Czech Republic, available at http://www.psp.cz/docs/laws/listina.html. Unofficial translation in English available at http://www.wipo.int/wipolex/en/text.jsp?file_id=190580(accessed 10 Jul 2013).

private life in a single Article, similar to Article 8 ECHR. Nevertheless the Court clarified that the right to privacy and the right to informational self-determination are sufficiently protected by the Czech Charter under a matrix of articles protecting private life, personal liberty, human dignity, undisturbed private life and the confidentiality of correspondence[86] and carried out an assessment of the contested provisions with the Czech Charter of Fundamental Rights.

The Court found that the wording of the contested provisions that referred to the duties and obligations of the providers with regard to the retained data was vague.[87] Moreover, the Czech law did not define clearly and precisely the purposes for which the retained data are provided to the competent authorities[88] and the access to data did not rely on "well-founded" suspicions.[89] In addition the Court found that the range of authorities that could have access to the retained data was not defined in a sufficient way.[90] With regard to the security of the retained data, the Court found that the relevant provisions did not offer "sufficient, unambiguous, detailed and appropriate"[91] safeguards on the minimum security requirements that had to be put in place by the providers.[92] It also criticised the retention period that was included in the Czech law as ambiguous and insufficient because it required that data should be retained for a period between 6 and 12 months.[93] For those reasons the Czech Constitutional Court found that the Czech law was in violation with "the right to privacy in the form of the right to informational self-determination…, based on the proportionality principle"[94] and ordered the abolishment of the contested provisions.

Perhaps one of the most interesting parts of the Court decision was the remark made by the Court as *obiter dictum*. The Court had clarified from the very beginning of its decision that it was not allowed to examine the compatibility of the Data Retention Directive with Community law, and human rights in particular. However, in the form of an *obiter dictum*, the Court:

> expresses its doubts whether the very instrument of global and preventive retention of location and traffic data on almost all electronic communications may be deemed necessary and adequate from the perspective of the intensity of the intervention to the

---

[86] Czech Constitutional Court, Decision of 22 March 2011 on petition Pl. ÚS 24/10, para. 31.

[87] Czech Constitutional Court, Decision of 22 March 2011 on petition Pl. ÚS 24/10, para. 46.

[88] Czech Constitutional Court, Decision of 22 March 2011 on petition Pl. ÚS 24/10, para. 47.

[89] J Kudrna, "Human rights – real of just formal rights? Example of the (un)constitutionality of data retention in the Czech Republic" (2012) 19:4 *Jurisprudence* 1289-1300 at 1297.

[90] Czech Constitutional Court, Decision of 22 March 2011 on petition Pl. ÚS 24/10, para. 48.

[91] P Molek, "Czech Constitutional Court – Unconstitutionality of the Czech implementation of the Data Retention Directive; Decision of 22 March 2011, PI. ÚS 24/10" (2012) 8 *European Constitutional Law Review* 338-353 at 348, quoting the decision of the Czech Constitutional Court.

[92] Czech Constitutional Court, Decision of 22 March 2011 on petition Pl. ÚS 24/10, para. 50.

[93] Czech Constitutional Court, Decision of 22 March 2011 on petition Pl. ÚS 24/10, para. 51.

[94] Czech Constitutional Court, Decision of 22 March 2011 on petition Pl. ÚS 24/10, para. 53.

> private sphere of an indefinite number of participants to electronic communications.[95]

The Court highlighted the criticism that the Data Retention Directive has received in several European Member States and questioned the overall use of data retention as an effective tool offering protection against security threats and the prosecution of serious crime.[96] Moreover, the Court questioned the role of private entities in the collection and retention of data for the purposes of data retention and criticised the lack of specific requirements relating to the security of the retained data, potential review mechanisms and procedures for the destruction of the retained data.[97]

4.6 Relevant Terminated and Pending National Court Cases

Besides the decisions that have already been adopted by the aforementioned national courts, there are a number of cases on data retention that are currently pending and are still to be discussed by national courts.

The Hungarian Constitution previously allowed a so called *actio popularis,*[98] which enables any interested entity to request a constitutionality assessment by the Hungarian Constitutional Court of any legal norm of the Hungarian legal system, without requiring applicants to prove personal interest or harm.[99] In 2008 the Hungarian Civil Liberties Union (HCLU) filed such an *actio popularis* before the Hungarian Constitutional Court requesting the examination of the constitutionality of the relevant provisions of the Hungarian Act C of 2003 on electronic communications that were amended in order to transpose the Data Retention Directive into Hungarian law. The complaint mainly challenged the blanket retention of personal data without previously defined purposes and questioned the compliance of the data retention related provisions with privacy, as well as with other fundamental rights, such as freedom of information, freedom of the press, freedom of religion, freedom of assembly and freedom of petition.[100] However, Hungary adopted a new Constitution, the Fundamental Law, which entered into force in January 2012 and abolished the

---

[95] Czech Constitutional Court, Decision of 22 March 2011 on petition Pl. ÚS 24/10, para. 55.

[96] Czech Constitutional Court, Decision of 22 March 2011 on petition Pl. ÚS 24/10, para. 56. The Court actually referred to the "prevention" of serious crime, while this purpose was not included in the final adopted text of the Directive, where data retention is aimed at the "investigation, detection and prosecution" of serious crime.

[97] Czech Constitutional Court, Decision of 22 March 2011 on petition Pl. ÚS 24/10, para. 57. P Molek, "Czech Constitutional Court – Unconstitutionality of the Czech implementation of the Data Retention Directive; Decision of 22 March 2011, PI. ÚS 24/10" (2012) 8 *European Constitutional Law Review* 338-353 at 349.

[98] Art 32A(3) of the old Hungarian Constitution.

[99] K. Kelemen, "The Hungarian Constitutional Court in the new constitutional framework" (2012) Paper presented at the III Colloquio biennale dei giovani comparatisti, Aosta (Italy) on 28-29 June 2012, organised by the Italian Association of Comparative Law, available at < http://academia.edu/1760644/The_Hungarian_Constitutional_Court_in_the_new_constitutional_framework> (accessed 08 Jul 2013).

[100] Constitutional complaint filed by HCLU against Hungarian telecom data retention regulations, 02 June 2008, available at http://tasz.hu/en/data-protection/constitutional-complaint-filed-hclu-against-hungarian-telecom-data-retention (accessed 08 Jul 2013)

actio popularis.[101] Under the new rules, the Constitutional Court is allowed to review the general conformity of rules of law with the Fundamental Law upon the initiative of the Government, of one fourth of the MPs, or of the Commissioner for Fundamental Rights.[102] It is maybe surprising that all pending cases that were submitted by entities that are not entitled to submit a constitutional complaint under the new provisions were automatically terminated.[103] The *actio popularis* of HCLU against data retention was among terminated pending cases. The Hungarian Parliamentary Commissioner for fundamental rights, Máté Szabó, contested the constitutional amendment, but the Hungarian Constitutional Court rejected his appeal.[104]

In 2011 a case was filed at the Polish Constitutional Tribunal questioning the powers of law enforcement agencies to access transmission and location data that are retained under the Polish data retention legislation.[105] At the time of writing, the case is still pending.

In October 2012, a group of Members of the Slovak Parliament challenged the Slovak data retention law before the Slovak Constitutional Court, on the initiative of a Slovak non-profit organisation, the European Information Society Institute (EISi).[106] The MPs asked the Slovak Constitutional Court to examine the national implementation of the Data Retention Directive in Slovakia and its conformity with the Slovak Constitution. If the Court deemed it necessary, the applicants also requested the Slovak court to send a request for a preliminary ruling to the Court of Justice on the

---

[101] K. Kelemen, "The Hungarian Constitutional Court in the new constitutional framework" (2012) Paper presented at the III Colloquio biennale dei giovani comparatisti, Aosta (Italy) on 28-29 June 2012, organised by the Italian Association of Comparative Law, available at <http://academia.edu/1760644/The_Hungarian_Constitutional_Court_in_the_new_constitutional_framework> (accessed 08 Jul 2013).

[102] According to the 4th amendment of the Fundamental Law in force from 1 April 2013, the Attorney General and the president of the Supreme Court is added to the list.

[103] K Kelemen, "Hungary: The Constitutional Court annulled some provisions of the media laws" (16 January 2012) available at http://www.medialaws.eu/hungary-the-constitutional-court-annulled-some-provisions-of-the-media-laws/ (accessed 08 Jul 2013).

[104] The Constitutional Court of Hungary (2013.05.23) Press release regarding the constitutional review of the Fourth Amendment of the Fundamental Law of Hungary, available at http://mkab.hu/sajto/news/press-release-regarding-the-constitutional-review-of-the-fourth-amendment-of-the-fundamental-law-of-hungary (accessed 08 July 2013). Constitutional Court of Hungary, Case II/648/2013, Ex post review of conformity with the Fundamental Law on the petition of the Commissioner for Fundamental Rights regarding certain provisions of the Fourth Amendment to the Fundamental Law of Hungary, available in Hungarian at http://public.mkab.hu/dev/dontesek.nsf/0/1E09722E15EB5DA0C1257B5D001B9851?OpenDocument (accessed 08 Jul 2013).

[105] The documents on the file of the case in front of the Polish Constitutional Tribunal are available only in Polish at http://www.trybunal.gov.pl/OTK/ezd/sprawa_lista_plikow.asp?syg=K%2023/11 (accessed 30 Jul 2013).

[106] http://www.eisionline.org/. EISi prepared a sample submission against data retention that could be used by the Slovak MPs that were interested, available at http://www.eisionline.org/index.php/projekty-m/data-retention-m/28-vzorove-podanie-na-ustavny-sud-sr-vo-veci-plosneho-sledovania-obcanov (accessed 08 Jul 2013). The submission in front of the Slovak Constitutional Court is available in Slovak at http://portal.concourt.sk/SearchRozhodnutia/podanie.do?id_spisu=458285 (accessed 08 Jul 2013).

validity of the Data Retention Directive.[107] At the time of writing, the case is still pending.

A similar case is pending in Slovenia, which implemented the Data Retention Directive in 2007 with regard to telephony data and in 2009 with regard to data relating to the internet transposing the relevant provisions in its Act on Electronic Communications.[108] This act was amended in 2012 and the new provisions entered in force on 15 January 2013. In March 2013 the Information Commissioner of Slovenia challenged the constitutionality of the data retention provisions as contained in the Act on Electronic Communications before the Slovenian Constitutional Court[109], claiming that the provisions of the Slovenian law implementing the Data Retention Directive did not respect the principle of proportionality.[110] The Slovenian Information Commissioner claimed that the Slovenian legislation allows the use of the retained data for a broad scope of criminal offences and purposes going beyond the Data Retention Directive; according to the investigations of the Commissioner the retained data had been used even in civil cases and labour law disputes.[111] The Commissioner claimed that the Slovenian data retention legislation is not compatible with human rights, such as the right to secrecy of communications, freedom of speech and freedom of movement and that the Slovenian government should have carried out an impact assessment in order to illustrate the necessity of data retention measures in the form that they were adopted.[112]

5. An important decision anticipated from the Court of Justice

Unlike the national courts referred to above, who decided to take a position on the compatibility of the national laws implementing the Data Retention Directive with the rights to data protection and to privacy, the Irish High Court decided to make a reference for a preliminary ruling to the Court of Justice on the compatibility of the Data Retention Directive with fundamental rights. The civil and human rights advocacy group Digital Rights Ireland challenged the Data Retention Directive, as well as the relevant Irish legislation transposing it, in front of the Irish High Court. The Court granted relief for a preliminary ruling[113] to the Court of Justice on the

---

[107] European Information Society Institute, Data retention in front of the Slovak Constitutional Court, 11 November 2012, available at http://www.eisionline.org/index.php/projekty-m/data-retention-m/49-slovak-case-on-data-retention (accessed 10 Jul 2013).

[108] ZEKom-1

[109] The text of the complaint can be found in Slovenian at https://www.ip-rs.si/fileadmin/user_upload/Pdf/ocene_ustavnosti/ZEKom_-_Zahteva_za_oceno_ustavnosti__data_retention_.pdf(accessed 10 Jul 2013)

[110] Information Commissioner of the Republic of Slovenia challenges data retention before Constitutional Court, https://www.ip-rs.si/index.php?id=272&tx_ttnews[tt_news]=1155(accessed 10 Jul 2013)

[111] Ibid.

[112] Ibid.

[113] Irish High Court, Digital Rights Ireland, 5 May 2010, available at http://www.scribd.com/doc/30950035/Data-Retention-Challenge-Judgment-re-Preliminary-Reference-Standing-Security-for-Costs (accessed 10 Jul 2013)

validity of the Data Retention Directive, which was submitted in June 2012.[114] Among other questions, the Court of Justice was asked to decide on the compatibility of the Directive with the right to privacy, as protected in the EU Charter and in the European Convention on Human Rights, and with the right to the protection of personal data that was recognised in the EU Charter as a separate fundamental right. A few months later, a similar decision was issued by the Austrian Constitutional Court[115] seeking a preliminary ruling by the Court of Justice on whether data retention is compatible with, among other rights, the rights to privacy and to data protection, as specifically protected in the EU Charter.[116] The Court of Justice joined the two cases and the hearing took place on 9 July 2013. The opinion of the Advocate General is expected in November 2013 and the decision of the Court at the beginning of 2014.

The majority of the national court decisions, with the exception of the Romanian one, focused on the national provisions on the access of the retained data by competent authorities and the purposes for which those authorities could access the data. The fact that the national courts did not examine the compatibility of data retention as a measure in its entirety or the compatibility of the Data Retention Directive with fundamental rights, and in particular the rights to privacy and processing of personal data, should not be interpreted as admittance that data retention does not violate fundamental rights.

The Supreme Court of Cyprus clearly stated that it was not allowed, bound by Article 1A of the Constitution of Cyprus, to examine the constitutionality of a European legal instrument. Similarly, the German Constitutional Court abided by its *Solange* doctrine[117], the main point of which was that as long as (*solange*) the European Communities ensured an effective protection of fundamental rights that were substantially similar to that of the fundamental rights of the German Constitution, the German Constitutional Court would no longer exercise its jurisdiction to decide on the compatibility of secondary Community legislation with those fundamental rights.

The Romanian Constitutional Court also focused on specific provisions of the Romanian data retention legislation in its analysis. However, and contrary to the approach taken by the other national courts, instead of annulling the relevant provisions of the national legislation, the Court made a general reasoning and addressed the very nature of blanket data retention as a measure infringing the right to privacy.

---

[114] Reference for a preliminary ruling from High Court of Ireland made on 11 June 2012 — Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, Case C-293/12, O.J. C258/11 (25.08.2012).

[115] Austrian Constitutional Court, Decision of 28 November 2012, G47/12, G59/12, G62,70,21/12, available in German at http://www.vfgh.at/cms/vfgh-site/attachments/5/9/4/CH0007/CMS1363700023224/vorratdatenspeicherung_vorlage_eugh_g47-12.pdf. The text of the decision is available in English at http://www.vfgh.gv.at/cms/vfgh-site/attachments/1/4/5/CH0007/CMS1363699922389/vorlage_vorratsdatenspeicherung_english.pdf (accessed 10 Jul 2013).

[116] Request for a preliminary ruling from the Verfassungsgerichtshof (Austria) lodged on 19 December 2012 — Kärntner Landesregierung and Others, Case C-594/12, O.J. C79/7 (16.03.2013).

[117] Solange II – Wünsche Handelsgesellschaft, 22 October 1986, BVerfGE 73, 339, 2 BvR 197/83. An unofficial translation of the case in English can be found at Wünsche Handelsgesellschaft [1987] 3 CMLR 225.

Nevertheless, the remaining national courts examined the compatibility of specific provisions of their data retention legislation with fundamental rights – and mainly the rights to privacy and data protection - to the extent that their national legislation allowed them. The Czech Constitutional Court emphasised the importance of providing guarantees and instruments for protecting fundamental rights of citizens when handing their personal data in the electronic communications sector, as expressed by the Court of Justice in the *Schecke* case, where an extensive proportionality balance was carried out.[118] Although the Czech Court, in the context of the specific case that it was discussing, based its analysis on the Czech data retention legislation, it actually questioned the compatibility of data retention in general, and of the Data Retention Directive in particular, with fundamental rights and more specifically with the right to privacy, in its *obiter dictum*. The Bulgarian, the German and the Cyprus courts first delineated the frame in which they were allowed to decide in the given cases and then ruled on the compatibility of specific provisions of the national data retention legislations. The Cyprus and the German courts, especially, were very concrete in specifying the limits within which they were allowed to take a decision.

In all the countries where the national courts annulled specific provisions of the national data retention laws (or the law in its entirety, as in the case of Romania), new provisions or laws were adopted in an attempt to avoid heavy fines from the European Commission for failing to transpose the Data Retention Directive. Especially in the case of Romania, where the blanket retention of data was considered unconstitutional, it would be interesting to see whether a challenge of the new data retention law in front of the Romanian Constitutional Court could have a different outcome. In this context, it is questionable whether "domestic legislators still have some 'margin of appreciation' between the Scylla of the Directive and the Charybdis of domestic constitutions".[119]

The Court of Justice in its decision on the requests for preliminary rulings is called to examine the compatibility of the Data Retention Directive with fundamental rights. The Court can take either of the approaches taken by the national courts: it can follow the reasoning of the Romanian Constitutional Court and reject the blanket retention of identification and communications data; or it can follow the more "conservative" approach of the rest of the courts, which has been more extensively elaborated and documented in the decision of the German Constitutional Court, and require the enhancement of the Data Retention Directive with more safeguards for the protection of fundamental rights. A third option would be that the Court decides that the Data Retention Directive does not infringe fundamental rights and does not recommend any additional safeguards for their protection. However this third option seems unlikely to be followed by the court, especially in view of the numerous national court decisions that have, in one way or another, raised issues with regard to the compatibility of data retention with fundamental rights.

---

[118] Czech Constitutional Court, Decision of 22 March 2011 on petition Pl. ÚS 24/10, para. 52; joint case of Volker und Markus Schecke GbR GbR and Hartmut Eifert v. Land Hessen (C-92/09 and C-93/09).

[119] P Molek, "Czech Constitutional Court – Unconstitutionality of the Czech implementation of the Data Retention Directive; Decision of 22 March 2011, PI. ÚS 24/10" (2012) 8 *European Constitutional Law Review* 338-353 at 353.

If the Court of Justice followed the reasoning of the Romanian Constitutional Court and rejected data retention as a measure in its entirety as infringing fundamental rights, and more specifically the rights to privacy and personal data, then this would be considered as a true victory of fundamental rights in Europe. However, one needs to keep in mind that the Data Retention Directive was adopted as a common market measure aiming at the harmonisation of the obligations of providers with regard to the collection of traffic and location data for law enforcement purposes. The Court of Justice has already confirmed the function of the Directive as a common market measure.[120] To the extent that the questions of compatibility touch on the access to retained data, the purposes for which they can be used and the authorities that can have access to them, the Court of Justice is likely to decide that these issues are deliberately left to the Member States to regulate. The Court of Justice may provide safeguards in order to "guide" Member States in the carrying out of a proportionality test between the goals of the Directive and the protection of fundamental rights of citizens. It would be very useful, though, to see that the Court of Justice exercises such a proportionality test also with regard to specific provisions of the Directive, such as Article 4, in specifying what types of authorities, and under which safeguards, may have access to the retained data.

6. Conclusions

The analysis of the national court decisions on data retention showed that nearly all of the relevant national courts - either Supreme Administrative Courts, as in the case of Bulgaria, the Supreme Court in Cyprus or Constitutional Courts in the rest of the cases examined - focused only on the national provisions relating to the access to the retained data and the purposes for which their use is allowed. The only exception is the Romanian Constitutional Court, which in a concise but breakthrough decision condemned data retention in its entirety. Nevertheless, the reluctance of the remaining national courts to criticise data retention should not be interpreted as accepting its compatibility with fundamental rights and the right to privacy in particular. Most of those Courts did not examine the compatibility of the Data Retention Directive itself with their constitutions and with fundamental rights because by their own assessment their competence to do so was limited by the supremacy of EU law in this area. The Constitution of Cyprus contains an explicit relevant provision on the primacy of European legislation that was claimed by the Supreme Court of Cyprus in order to delineate the relevant cases upon which it was asked to decide. The German Federal Constitutional Court was bound by its *Solange* doctrine, while the Czech Constitutional Court criticised data retention in its *obiter dictum*.

Meanwhile, the implementation of the Data Retention Directive in the national legislation of the Member States and the different decisions taken by the national courts has shown the difficulties in creating a harmonised framework on data retention throughout Europe. It has also highlighted the difficulties that national courts face when evaluating the compatibility of national laws transposing EU law with their own countries' fundamental rights framework. What the case law

[120] Case C-301/06 *Ireland v European Parliament and Council of the European Union* [2009] ECR I-00593.

surrounding data retention shows, therefore, is that while those national frameworks may in many cases be similar or identical to the one set out in the Charter, fundamental rights protection within the EU still grapples with a number of procedural issues that have the potential to result in delay and conflicts of competence. Those problems need to be tackled, headed both by the Court of Justice and by the EU's legislative bodies, if comprehensive fundamental rights protection at EU level is to be guaranteed.

The current uncertainty also makes it difficult for the legislative bodies of the Member States that have not yet implemented the Data Retention Directive to decide on how to proceed. They are, in a way, caught between the requirements set out by their own courts and the enforcement capability of the European Commission. The example of Sweden is illustrative in this context. In 2010 the Court of Justice found that Sweden had failed to transpose the Directive.[121] While Sweden adopted data retention legislation in 2012, the Court of Justice ordered it to pay a lump sum payment of EUR 3.000.000 in May 2013 for late implementation.[122] By the same token, the Commission has taken Germany to court for failing to re-implement the Directive – required by the 2010 decision by its Constitutional Court - because of a political impasse. The argument put forward by some German politicians, that enforcement should be delayed pending the decision of the Court of Justice in the Irish and Austrian challenge, has been officially rebuked.[123] Member States are therefore adopting data retention laws, but it is "hazardous for the Commission to rule with an iron fist by forcing Member States to adopt data retention legislation that is incompatible with their constitutions".[124]

At the time of writing the Irish and Austrian requests for a preliminary ruling on the compatibility of the Data Retention Directive with fundamental rights, and specifically with the right to privacy and to data protection, are pending before the Court of Justice and were joined by it. In 2009 the Court of Justice did not examine the issue of compatibility of the Data Retention Directive with fundamental rights, in a case when the legal basis of the Directive was questioned. However, these two preliminary rulings raise exactly the issue of compatibility of the Directive with fundamental rights. In 2010 the European Commission carried out an evaluation of the Data Retention Directive.[125] Even if the EU Commissioner for Home Affairs, Cecilia Malmström, admitted that "data retention raises sensitive issues about privacy

---

[121] Judgement of 4 February 2010, Commission / Sweden (C-185/09, ECR 2010 p. I-14*, Summ.pub.)

[122] Judgement of 30 May 2013, Commission / Sweden (C-270/11).

[123] Interview with Cecilia Malmström, "Wir waren sehr geduldig mit Deutschland", Frankfurter Allgemeine Zeitung, 3 July 2012; available at http://www.faz.net/aktuell/politik/europaeische-union/eu-innenkommissarin-cecilia-malmstroem-wir-waren-sehr-geduldig-mit-deutschland-11808962.html (accessed 30 Aug 2013).

[124] T Konstadinides, "Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem" (2011) 36 *European Law Review* 722-736 at 733.

[125] European Commission, Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), Brussels, 18.4.2011, COM(2011) 225 final

and the protection of personal data"[126], the Commission evaluation did not reveal "any concrete cases of law enforcement abusing their powers to access retained data and violate the right to privacy".[127] If the Court of Justice follows the reasoning of the European Commission in the evaluation report of the Directive, then it will be conservative in its findings. It may be difficult for the Court of Justice to follow a reasoning similar to the Romanian Constitutional Court and reject data retention in its entirety as a measure infringing fundamental rights, and more specifically the rights to privacy and personal data. Nevertheless it is to be hoped that the Court will at least provide guidance to the EU legislator and the Member States on the minimum safeguards that must be observed in the context of the mere retention of communications data to ensure the adequate protection of the fundamental rights of EU citizens under the Charter. In addition, it would be useful to see how the Court of Justice views the distinction currently contained in the Directive between retention and access. Arguably, it is this distinction – where EU law regulates the former while national law is left to regulate the latter – that is the source of many of the substantive and procedural issues that have arisen in the context of this legislative project. It is likely that guidance on a more comprehensive approach dealing not just with the types of data to be retained but also with the types of authorities that should have to access them and for what purpose, would be welcomed by citizens, law enforcement authorities and communications service providers alike. It is to be hoped that the Court will rise to that challenge when it finally gets to hand down its decision.

---

[126] Cecilia Malmström,"Taking on the Data Retention Directive" European Commission conference, Brussels, 3 December 2010, Speech/10/723, available at http://europa.eu/rapid/press-release_SPEECH-10-723_en.htm (accessed 10 Jul 2013).

[127] Ibid.