Mark D. Cole / Franziska Boehm

EU Data Retention – Finally Abolished?*

– Eight Years in Light of Article 8 –

Zusammenfassung

Neben dem Vorschlag der Europäischen Kommission zu einer Datenschutz-Grundverordnung ist die Vorratsspeicherung von Daten zum Zwecke der Ermittlung und Verfolgung von Straftaten ein weiteres beherrschendes Thema der gegenwärtigen Debatte im Datenschutzrecht. Die Richtlinie, die 2006 verabschiedet wurde, legt den europäischen Rechtsrahmen für die Vorratsdatenspeicherung fest. Die Ermächtigung der Europäischen Union zum Erlass der Richtlinie auf der allgemeinen Rechtsgrundlage zum Binnenmarkt hat der Europäische Gerichtshof in einem Urteil von 2009 bestätigt. Dennoch bleiben viele Fragen, vor allem der Grundrechtskonformität bezüglich der materiellen Bestimmungen der Richtlinie unbeantwortet. Das Recht auf Privatsphäre und der Schutz personenbezogener Daten, wie sie durch Art. 7 und 8 EU-Grundrechtecharta und Art. 8 EGMR normiert sind, scheinen in Zeiten anlassloser und massenhafter Sammlung von Daten massiv gefährdet. Seit Bestehen der Richtlinie haben sich mehrere oberste Gerichte einiger Mitgliedstaaten (darunter auch Deutschland) mit der Vereinbarkeit nationaler Umsetzungsakte mit den in nationalen Verfassungen verankerten Grundrechten auseinandergesetzt und die nationalen Rechtsakte teilweise für verfassungswidrig erklärt. Die Kommission gesteht in ihrem Bewertungsbericht zur Richtlinie vom April 2011 eine uneinheitliche Umsetzung der Richtlinie in den Mitgliedstaaten ein, was sich auf die Effizienz des Regelungswerkes auswirkt. Sie stellt eine Überarbeitung der Richtlinie unter Berücksichtigung der Verhältnismäßigkeit des Speicherungsprozesses und der Verwendung der Daten in Aussicht. Ähnliches ergeht auch aus den Schlussanträgen des Generalanwaltes Cruz Villalón in den verbundenen Rechtssachen Digital Rights Ireland und Seitlinger u.a. vom Dezember 2013, in denen er die Richtlinie in Gänze für unvereinbar mit den europäischen Grundrechten hält. Acht Jahre nach Inkrafttreten der Richtlinie ist der Gerichtshof nun mit drängenden datenschutzsrechtlichen Fragen befasst, die über das Schicksal der Vorratsdatenspeicherung entscheiden werden.

* The author *Cole* is Associate Professor of Law (Law of the New Information Technologies, Media and Communications Law) at the Faculty of Law, Economics and Finance at the University of Luxembourg, the author *Boehm* is Assistant Professor for IT law at the Institut für Informations-, Telekommunikations und Medienrecht at the Faculty of Law of the University of Münster. Previously she worked as Post-Doctoral Researcher at the University of Luxembourg's Interdisciplinary Centre for Security, Reliability and Trust (SnT) and for the Faculty of Law, Economics and Finance, during which she collaborated with *Cole* on a report about the national transposition of the Data Retention Directive in Luxembourg (cf. on this *Roßnagel/Moser-Knierim/Schweda*, Interessenausgleich im Rahmen der Vorratsdatenspeicherung – Analysen und Empfehlungen, Baden-Baden 2013).

Résumé

Outre le projet de règlement relatif à la protection des données personnelles de la Commission européenne, la conservation de données aux fins d'enquêtes et de poursuites de délits constitue un thème dominant de l'actuel débat concernant la législation relative à la protection des données. La directive adoptée en 2006 définit le cadre légal européen de la conservation de données. L'habilitation de l'Union européenne d'adopter un règlement sur base légale et générale du marché intérieur a été confirmée par la Cour de Justice dans un arrêt de 2009. Néanmoins, beaucoup de questions subsistent, surtout quand à la conformité des dispositions matérielles de la directive avec les droits fondamentaux. Le droit au respect de la vie privée et familiale et la protection des données à caractère personnel, consacrés par les articles 7 et 8 de la Charte des droits fondamentaux et par l'article 8 de la CEDH, apparaissent comme compromis dans une phase de collecte massive et non motivée de données. Depuis l'existence de la directive des cours suprêmes de quelques Etats membres (comme l'Allemagne) ont abordé la question de la conformité des actes nationaux de transposition avec les droits fondamentaux consacrés par les constitutions nationales et ont en partie déclaré l'anti constitutionnalité desdits actes nationaux. La Commission admet dans son rapport d'évaluation de la directive d'avril 2011 une transposition non hétérogène de la directive dans les Etats membres, ayant des conséquences sur l'efficacité du cadre règlementaire. Elle prévoit une refonte de la directive en prenant en compte la proportionnalité du processus d'enregistrement et le traitement des données. Une constatation semblable ressort des conclusions de l'Avocat General Cruz Villalón dans les affaires jointes Digital Rights Ireland et Seitlinger e.a de décembre 2013 dans lesquelles il a soutenu la non conformité de l'intégralité de la directive avec les droits fondamentaux européens. Huit ans après l'entrée en vigueur de la directive, la Cour de Justice est préoccupée avec des questions urgentes concernant la protection des données personnelles qui décideront du sort de la conservation des données.

I. Introduction – or: it is finally done

Finally, it has happened: the *German Constitutional Court* with decision of 14 January 2014 has for the first time in its history and after a long tradition of establishing a special relationship on constitutional grounds between itself and the *Court of Justice of the European Union* decided to stay proceedings and ask for a preliminary reference by the *Court in Luxembourg*.[1] Although understandable from the *Court's* perspective why it showed such a long-running reluctance against using the preliminary reference instrument, this article will explore whether it would not have been an equally worthy case to

1 Pending case C-62/14 *Gauweiler and others*. Cf. *German Constitutional Court*, press release no. 9/2014 of 7 February 2014, available in English at http://www.bundesverfassungsgericht.de/en/press/bvg14-009en.html.

do so in the analysis of the German transposition of the so-called EU Data Retention Directive.[2]

The Data Retention Directive of 2006 was mainly a reaction to the terrorist attacks in Madrid of 11 March 2004 and London of 7 July 2005, but was based on the general harmonisation provision of the then EC Treaty in view of reaching a better functioning common market in the telecommunications sector. Whether or not the *German Constitutional Court* regarded the case it had to deal with concerning the national transposition being equally worthwhile a preliminary reference, such a reference would certainly have answered some pressing questions well in advance of 2014. As it stands, eight years after passing of the Directive and five years after the latest deadline for national implementation, the Directive remains to be an extraordinary example of questionable efficiency especially in light of the efforts connected, but more importantly of very doubtful legal validity in view of its fundamental rights issues. This applies even more in light of the recent decision of the *Court of Justice* in the case of *Digital Rights Ireland and Kärnter Landesregierung et al*.[3] according to which "by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter."[4] Certainly, the pressing need for finally settling the fundamental rights issues involved has been articulated by several national constitutional courts (below under III. 2. with a brief evaluation of some of the national retention rules under III. 3.) and the CJEU has responded to this need (III. 4.). To start with, the Article will briefly present the Directive and recall its development (II.) and will end with concluding remarks on the situation eight years after entry into force of the Directive (IV.).

II. The EU Data Retention Directive 2006/24/EC and its legal framework

Although not even a decade since the drafting of the Data Retention Directive has passed, it was a somewhat different era then. Data protection and privacy concerns were by far not as prominent as they are (again) today after the advent of big data applications and the general observation of massive data collection by private entities and more recently discussed intensively again in light of the *Snowden*/NSA-revelations by states. Also,

2 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, OJ 2006, L-105/54.

3 Case C-293/12, *Digital Rights Ireland Ltd v The Minister for Communications, Marine and Natural Resources The Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána Ireland and The Attorney General* and in Case C-594/12 *Kärntner Landesregierung, Michael Seitlinger and Christof Tschohl, Andreas Krisch, Albert Steinhauser, Jana Herwig, Sigrid Maurer, Erich Schweighofer, Hannes Tretter, Scheucher Rechtsanwalt GmbH, Maria Wittmann-Tiwald, Philipp Schmuck, Stefan Prochaska and Others*, delivered on 12 December 2013.

4 *Ibid*., para. 69, Advocate General Cruz Villalón had formulated even clearer that the Directive „is as a whole incompatible with Art. 52 (1) of the Charter of Fundamental Rights of the European Union", Opinion of Advocate General Cruz Villalón in Case C-293/12, para 131 and suggested answer part 1, para. 159.

primary EU law was different in this area: although there was a provision in Art. 286 EC Treaty dealing with the application of existing data protection rules to all EC institutions and bodies, there was no general data protection provision as can be found since entry into force of the Treaty of Lisbon in Art. 16 TFEU.[5] According to this provision there is not only a re-statement of the right to data protection, but it also gives the EU a general legal basis to create rules concerning processing of data by the *Union* and the Member States in connection with EU law. And although the equivalence table attached to the Treaty of Lisbon suggests the new Art. 16 TFEU is a replacement of the former Art. 286 TEC, in reality the new provision significantly expands the scope of data protection in the EU context. More importantly, with Lisbon the formerly merely proclaimed Charter of Fundamental Rights of the EU has become binding primary law and with it a specific data protection provision in Art. 8 (in addition to the general provision of Art. 7 CFR concerning private life which resounds Art. 8 ECHR). With this, the previous validity of Art. 8 ECHR via the development of fundamental rights as general principles by the CJEU is expanded.[6]

When the Directive was conceived it could not be based on a data protection provision nor were there sufficient legal bases for a harmonization of investigation instruments in Member States, an area that would have been the most obvious to choose if the Directive was to respond to the terrorist attacks and the idea that tracing the communication schemes of the terrorists involved could have possibly avoided what happened or at least added to finding the suspects or confirming their participation. Therefore, the general harmonization provision in former Art. 95 TEC – now Art. 114 TFEU – was chosen as legal basis to much criticism also from some of the Member States.[7] This eventually led also to a procedure before the CJEU which will be discussed below. But the approach of harmonizing the rules on retention of communications data in the Member States in order to facilitate the provision of (telecommunications) services across the common market was upheld.

The Directive itself establishes the obligation of Member States to introduce a system of retention of telecommunications data for a period of six months until two years. The Directive is rather briefly worded and includes only 17 short articles. However, it lays down in detail the exact categories of data to be retained and gives some basic indications regarding data protection and security requirements. Nonetheless, the Directive merely stipulates the minimum requirements to be respected with regard to the access to data, protection of the data, remedies, liability or the organisation of supervisory authorities. Most of the details are left to the interpretation of the Member States. These had a period of one and a half years for transposition which could be prolonged for internet-related data at the most until March 2009 amounting to three years, an option generally selected. Due to the wide margins left, it was not completely surprising that the transposition of

5 Cf. also Art. 39 TEU concerning data processing by Member States concerning the Common Foreign and Security Policy.

6 Cf. generally on the data protection framework *Boehm*, Information sharing and data protection in the Area of Freedom, Security and Justice – Towards harmonised data protection principles for EU-internal information exchange, Springer 2011.

7 Not last as the first proposal for a legal act concerning data retention came in form of a draft framework decision under the former third pillar which was regarded as more appropriate e.g. by Ireland.

the Directive created opposition from civil society and politics in various Member States. Eventually, even the highest administrative or constitutional courts of *Bulgaria, Romania*, Germany, Cyprus and the *Czech Republic* that had to deal with the respective national transpositions declared parts of the acts transposing the Directive into national law void.[8] None of these, including the *German Constitutional Court*, asked the *Court of Justice of the European Union* on guidance whether the original act itself was possibly in violation of fundamental rights on EU level. In some of the Member States, again for instance *Germany*, the discussion as a result of the judgement is still ongoing as there was no political agreement neither within the past nor within the current government as to whether and how to transpose the Directive. As an effect the Directive has not yet been transposed there into national law[9] and Sweden was fined a lump sum payment of 3 Million Euro for non-transposition.[10]

III. The legal disputes about Directive 2006/24/EC

1. The competency question in the initial ECJ judgement

In 2006, Ireland, joined by *Slovakia*, brought a case before the *European Court of Justice* questioning the legal basis of the Data Retention Directive.[11] More concretely, *Ireland* disputed the choice of Article 95 EC Treaty (now article 114 TFEU) as a first pillar legal basis arguing that Directive 2006/24 should have been better based on a third pillar legal basis, as it regulates the data retention for law enforcement purposes. Article 1 of Directive 2006/24 harmonizes the Member States' provisions concerning the obligation of electronic communication service providers to store the clients' data "in order to ensure that the data are available for the purpose of the investigation, detection and

8 Decision of the *Bulgarian Supreme Administrative Court* of 11 December 2008 available at http://econ.bg/Нормативни-актове/Решение-13627-от-11-12-2008-г-по-адм-дело-11799-от-2008-г-Наредба-40-от-2008-г-за-_l.l_i.156836_at.5.html. English commentary on the Bulgarian case at http://www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention. Unofficial English translation of the *Romanian Constitutional Court* decision of 8 October 2009 available at http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf. Summary translation of the *German Constitutional Court* decision of 2 March 2010 (http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html) available at http://www.bverfg.de/en/press/bvg10-011en.html; for further analysis see *De Vries et al.*, The *German Constitutional Court* Judgement on Data Retention: Proportionality Overrides Unlimited Surveillance (Doesn't It), in Gutwirth et al, Computers, Privacy and Data Protection: An Element of Choice, Springer 2011, p. 3 et seq. More information about the *Cypriot Supreme Court* decision can be found at http://edri.org/edrigram/number9.3/data-retention-un-lawful-cyprus and in *Markou*, The *Cyprus* and other EU court rulings on data retention: The Directive as a privacy bomb, Computer Law & Security Review 28 (2012), 468-475. An English translation of the *Czech Constitutional Court* decision available at http://www.slidilove.cz/en/english/english-translation-czech-constitutional-court-decision-data-retention.

9 Cf. also *Commission* infringement procedure pending at the Court, Case C-329/12 *Commission v Germany*.

10 CJEU, Case C-270/11 *Commission v Sweden.*

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

prosecution of serious crime".[12] *Ireland* assumed therefore that the main purpose of the Directive is not the harmonisation of the internal market, as was the purpose of former Article 95 EC Treaty[13], but rather the storing of client data to have them available for later use for law enforcement purposes.

Notwithstanding the wording of Article 1 of Directive 2006/24 mentioned above, the *Court* ruled that Directive 2006/24 regulates operations which "are independent of the implementation of any police and judicial cooperation in criminal matters".[14] Thus, the goal of the Directive concerns solely the harmonization of the activities of service providers in the EU internal market and does not relate to police purposes.[15] As a result, the *Court* approved the first pillar choice of Article 95 EC Treaty as the correct legal basis for the Directive.

While it is correct that the retention of the data does not directly involve police related activities, the reason for the storing is nonetheless the later use of the client data for law enforcement purposes. That the *Court* did not further consider this argument may be related to the consequences the annulment of the first pillar legal basis would have had. If the *Court* had annulled the first pillar choice, the Directive would have needed an alternative legal basis, which would have been most likely a third pillar option. This option would have excluded both the *European Parliament* and the *European Data Protection Supervisor* from the legislative process and the Directive from democratic control. Whereas thus the reasons for the decision may have been to a certain extent of political nature at that time, the entry into force of the Lisbon Treaty abolished the pillar structure and, even if this may be highly speculative, the same context could be decided differently under the new legal framework. It is to be expected that this will be seen in a new proposal of the *Commission* if it takes the consequence from the evaluation report concerning the Directive and/or the outcome of the case at the CJEU.

2. The national law related court decisions in the Member States

As the Directive regulates the storing of huge amounts of data of unsuspicious persons, the main criticism relates to the infringing effect the Directive has on the fundamental rights of privacy and free correspondence. Data protection issues and the "diffusely threatening feeling of being watched" play also an important role.[16] As mentioned above, these questions were left unanswered by the initial judgement of the *Court of Justice* as it did not touch upon the topic of fundamental rights which were regarded as crucial by many of the observers. The *Court* focussed on the choice of the legal basis and completely avoided to rule on the fundamental rights problem thereby limiting its answer

12 Article 1 (1) and (2) Directive 2006/24/EC.

13 Former Article 95 EC Treaty could be invoked "when disparities exist between national rules which are such as to obstruct the fundamental freedoms or to create distortions of competition and thus have a direct effect on the functioning of the internal market", cf. also case C-301/06 *Ireland v. Parliament and Council* [2009] ECR I-593, para 63.

14 Case C-301/06 *Ireland v. Parliament and Council* [2009] ECR I-593, para 83.

15 Case C-301/06 *Ireland v. Parliament and Council* [2009] ECR I-593, para 84.

16 Cf. the argument of the *German Constitutional Court* in the data retention case of 2 March 2010, point 3 of the English summary translation of the judgment (http://www.bverfg.de/pressemitteilungen/bvg10-011en.html).

purely to the question brought up by *Ireland*. National courts however were less reluctant in this regard and discussed in detail the implications for fundamental rights. Nonetheless, none of them referred the fundamental rights questions to the CJEU before their decisions. On the contrary, national courts restricted their judgements to questions of compliance of the national act transposing the Directive with national constitutional law leaving the EU instrument itself untouched. This only changed with the preliminary reference procedure initiated by *Ireland* in 2012 which will be discussed further below.

In several Member States, complaints against the national act transposing the Data Retention Directive into national law were subject to court rulings. The national supreme courts of *Bulgaria, Romania, Germany, Cyprus* and the *Czech Republic* passed judgements on this issue and in other Member States, cases are still pending.[17]

a) Bulgaria

An early decision regarding a national act transposing the Data Retention Directive was the Decision of the *Bulgarian Supreme Administrative Court* in December 2008.[18] The *Court* annulled a part of the national data retention act due to missing privacy guarantees as well as limitations regarding the access to the retained data. In addition, the justifications for getting access as well as the procedure for the actual retention were regarded as not specific enough and there were no limitations provided for against violations of the rights which are granted by the Bulgarian Constitution. Therefore, a number of articles of the Bulgarian data retention act were declared void. As a reaction to this judgement, the Bulgarian legislator carried out the changes requested by the *Court* and a new data retention act has since been in force.[19]

b) Romania

The Decision of the *Romanian Constitutional Court* was published in December 2009. The *Court* annulled the Romanian data retention law and declared it as unconstitutional. The *Court* criticized the unclear wording of the provisions restricting the right to private life, the secrecy of correspondence and the freedom of expression. Moreover, it stipulated that "[…] the continuous limitation of the privacy right and the secrecy of correspondence makes the essence of the right disappear by removing the safeguards regarding its execution. The physical and legal persons, mass users of the public electronic

17 In *Hungary* a case was lodged before the *Constitutional Court* (cf. http://tasz.hu/en/data-protection/constitutional-complaint-filed-hclu-against-hungarian-telecom-data-retention), however after the constitutional reform that also affected procedural aspects before the *Court* open cases were removed from the docket. Cf. on this specifically concerning the procedure *Kosta*, The Way to *Luxemburg*: *National Court* Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection, (2013) 10:3 SCRIPTed 339 http://script-ed.org/?p=1163, also with an overview of further pending cases.

18 Compare http://edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention and http://www.aip-bg.org/documents/data_retention_campaign_11122008eng.htm.

19 Cf. for details: http://eur-lex.europa.eu/search.html?or0=DN%3D72006L0024*%2CDN-old%3D72006L0024*&qid=1397661364500&type=advanced&AU_CODED=BGR.

communication services or networks, are permanent subjects to this intrusion into their exercise of their private rights to correspondence and freedom of expression, without the possibility of a free, uncensored manifestation, except for direct communication, thus excluding the main communication means used nowadays."[20] It compared the rules on data retention with the rules on audio and video surveillance in criminal investigations and was astonished to see that the latter rules are regulated in a much stricter way than the rules on data retention although the data retention rules target persons not being suspected of having committed a crime. Further, the *Court* explained that this intrusion "into the free exercise of the right takes place continuously and independently of the occurrence of a justifying fact […]".[21] These aspects, among others, led to the unconstitutionality of the Romanian act transposing the Data Retention Directive. As in the Bulgarian case, the legislator reacted and the *Romanian Parliament* passed a new law on data retention which was promulgated by the President in June 2012.[22] However, the blanket unconstitutionality as the *Constitutional Court* saw it indicates that the massive and long-term retention of everyone's data is per se problematic and not only the details of the way it is regulated. The wording used resounds the German Constitution's "Wesensgehaltsgarantie" which guarantees that the essence of each fundamental right has to be respected and cannot be completely reduced even by in themselves constitutionally valid limitations/justifications and which can now also be found in Art. 52.1 first sentence of the Charter of Fundamental Rights of the EU ("respect the essence").

c) Germany

In March 2010, the *German Constitutional Court – Bundesverfassungsgericht* annulled essential parts of the German provisions implementing the EU Data Retention Directive.[23] The *Court* restricted its criticism to the German provisions transposing the Directive and did not criticize the EU Directive itself, but it issued fundamental disapproval with the German interpretation of the EU Directive. The *Court* declared the way in which the German legislator transposed the Directive as not proportionate to the aims that were to be achieved by the measure. More precisely, Article 10 of the German Constitution (protecting the secrecy of telecommunications) was violated in the *Court's* view. While

20 Quote of the English translation of the *Romanian Constitutional Court* decision on data retention, accessible at http://www.legi-internet.ro/en/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html, cf. also *De Vries et al.*, The *German Constitutional Court* Judgement on Data Retention: Proportionality Overrides Unlimited Surveillance (Doesn't It), in Gutwirth et al, Computers, Privacy and Data Protection: An Element of Choice, Springer 2011, p. 3 et seq.

21 Quote of the English translation of the *Romanian Constitutional Court* decision on data retention, see above.

22 Act no. 82/2012 on the retention of data generated or processed by electronic communications public networks providers and by the electronic communication services for the public; available in Romanian at http://www.legi-internet.ro/legislatie-itc/date-cu-caracter-personal/legea-nr822012-privind-retinerea-datelor.html.

23 Judgment of the *Bundesverfassungsgericht* of 2 March 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08.

the precautionary storage of telecommunications traffic data for the possible later use in criminal proceedings was found to be not in itself incompatible with this provision of the Constitution[24], the measures to protect citizens against such a massive infringement of their rights were not regarded as sufficient. The *Court* emphasized that the collected data could be used to establish "meaningful personality profiles of virtually all citizens and track their movements".[25] For this reason the *Court* demanded high standards with regard to data security, transparency, legal protection as well as effective sanctions against violations. The *Court* insisted that if the data are used for the prosecution of crimes, "there must at least be the suspicion of a criminal offence, based on specific facts, that is serious even in an individual case".[26] As a minimum, a specific list of the criminal offences that entitle to access the data is needed to comply with this requirement of the *Court*. Regarding transparency and the use of the data for criminal prosecution, the *Court* demanded an "open use" of the data. Data should only be used in secret if this kind of use is ordered by a judge in an individual case and therefore it should be exceptional. The *Court* also required that the retained data must be subjected to judicial authority. On the other hand, less strict requirements were applied to the indirect use of the data by private actors to identify IP addresses for example in proceedings about rights infringements. All in all, as the conditions mentioned above were not complied with in the German transposing act, the violation of the secrecy of telecommunication led to the respective provisions being void.

The conflicting interests at stake resulted in intense political discussions after the judgement and not last due to a change in government and the prospect of the upcoming CJEU judgement[27], until today no compromise could be reached. As a result, four years after the judgement of the *Bundesverfassungsgericht* (and eight years after passing of the Directive), *Germany* has still no valid transposition of the Data Retention Directive. As mentioned above and was also the case against Sweden, in May 2012 the EU *Commission* initiated proceedings against *Germany* before the *Court of Justice of the European Union* and requested a daily penalty payment of over 300 000 € for non-compliance with the Directive.[28] Now, after the CJEU decision, the German government has decided to abandon plans to introduce a data retention law.[29]

24 Compare point 3 of the English summary translation of the judgment.
25 Compare point 3 of the English summary translation of the judgment.
26 Compare point 4 of the English summary translation.
27 Although this argument was not regarded as a valid reason for delay by the *Commission* in the infringement proceedings initiated by the *Commission* against *Germany* for non-transposition.
28 Cf. pending Case C-329/12 *Commission v. Germany*. On the problem of pushing transposition of a Directive whose fundamental rights validity seems at least questionable in view of the amount of national courts reacting negatively to the national transpositions *Konstadinides*, Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem, European Current Law Issue 1/2012, xi, xxi, at http://epubs.surrey.ac.uk/282571/.
29 Compare recent press articles: e.g. http://www.spiegel.de/netzwelt/netzpolitik/vorratsdatenspeicherung-regierung-verzichtet-auf-neues-gesetz-a-964155.html.

d) Cyprus

A further decision on data retention was issued in February 2011 by the *Cypriot Supreme Court.*[30] The *Court* annulled part of the Cypriot data retention act and stipulated that the criticized part went beyond the requirements of the EU Data Retention Directive. Provisions concerning the access of the police to the retained data violated Article 15 and 17 (Right to privacy and secrecy of correspondence and communication) of the Cypriot Constitution. The *Court* limited access to the data to fewer cases than initially provided for in the Cypriot data retention act. The *Court* emphasized that Article 17 of the Cypriot Constitution does not allow an interference with the exercise of the right to secret correspondence and other communication, apart from situations, which are "in accordance with the law" and relate to "cases of convicted and unconvicted prisoners and business correspondence and communication of bankrupts during the bankruptcy administration".[31] So far, the effects of the court ruling on the practical application of the concerned act are not fully clear, but other than some of the *Courts* mentioned above the *Cypriot Supreme Court* did not criticize data retention as such and only ruled on the provisions providing access to the data.[32]

e) Czech Republic

In March 2011, the *Czech Constitutional Court* raised doubts about the necessity and proportionality of data retention in general[33] and declared some national provisions void which required the storing of more data than the Directive demands.[34] The *Court* also criticized that the national legislation did not entail a right to inform the persons about the fact that their data had been requested.[35] Further, the spectrum of public authorities entitled to access the data as well as the definition of the purpose for which the data could be accessed was found as being not specific enough to satisfy requirements established by the *Constitutional Court*.[36] Additionally, the Court demanded that "the legislator must limit the possibility to use retained data for purposes of criminal proceeding concerning very serious crimes only and only in case the pursued purpose cannot be reached otherwise".[37] These requirements clearly restrict the scope of data retention and

30 More information can be found at: http://edri.org/edrigramnumber9-3data-retention-un-lawful-cyprus/ and *Markou*, The Cyprus and other EU court rulings on data retention: The Directive as a privacy bomb, Computer Law & Security Review 28 (2012), 468-475.

31 English translation of the Cypriot Constitution available at: http://www.kypros.org/Constitution/English/appendix_d_part_ii.html.

32 Compare also *Markou*, The *Cyprus* and other EU court rulings on data retention: The Directive as a privacy bomb, Computer Law & Security Review 28 (2012), 468-475, in particular p. 472.

33 *Czech Republic Constitutional Court,* Pl. ÚS 24/10, 22 March 2011, paras 55-57; for an English translation of the *Czech Constitutional Court* see above fn.8.

34 For more information cf. *Czech Constitutional Court* rejects data retention law, EDRi, 31 March 2011, available at http://edri.org/czech-decision-data-retention.

35 Para 47 of the judgement.

36 Para 48 of the judgement.

37 Para 48 of the judgement.

leave room for doubts whether it is at all possible to implement the data retention obligation in a legally valid way in the EU Member States. Irrespective of this observation, a new Data Retention Act has in the meanwhile been passed by the *Parliament* and entered into force.[38]

3. The evaluation of data retention rules in the Member States

The cases discussed above show that a number of Member States were struggling to implement the Data Retention Directive in a way that is compatible with fundamental rights as guaranteed by their national constitutions. As the Directive only regulates the storing of the data, but not the access of law enforcement to this data, the Member States are far away from following the same rules with regard to this question. The organisation of the access to the data obviously creates further potential problems and makes it even more complicated to find a way that is compliant with fundamental rights. It is therefore interesting to analyze how Member States have implemented the Directive.

In that sense, the *Commission's* first evaluation report on the implementation of the Data Retention Directive published in April 2011 proves insightful. The report on the outset repeats the argument of the *Commission* that the diversity of existing provisions on the retention of telecommunication data in the Member States before passing of the Directive led to the risk of competitive distortions in the internal market for service providers. To counter this risk the Data Retention Directive was introduced which provided for harmonised rules in this industrial sector. Despite this statement, the report nonetheless clearly focuses on how the Member States now regulate the use of the data for law enforcement purposes and shows in this regard how the Member States have transposed the EU requirements from the Directive.[39]

a) General remarks

From the report, it is visible that at that time some Member States had only partially transposed the Directive (*Belgium*), others had drafted legislation (*Sweden* and *Austria*) and still others had not transposed (or revoked their transposition of) the Directive (*Germany, Czech Republic, Romania*).[40] Although the amount of Member States which

38 Cf. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:72006L0024:EN:NOT #FIELD_CZ; *Czech Republic*: Data retention – almost back in business, EDRi, 1 August 2012, available at http://edri.org/edrigramnumber10-15czech-republic-new-data-retention-law/; *Fučík*, *Czech Republic*: New Regulation on Data Retention, IRIS 2012-9:1/15.

39 Cf. also *Jones/Hayes*, SECILE D2.4 The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy, esp. p. 34 et seq., http://www.statewatch.org/news/2013/nov/Data-Retention-Directive-in-Europe-A-Case-Study.pdf.

40 Cf. p. 5 et seq. the report. Apart from the official source of Eur-Lex (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:72006L0024:EN:NOT) several organisations provide information and overview on national transpositions online, cf. e.g. the wiki on www.vorratsdatenspeicherung.de or https://wiki.openrightsgroup.org/wiki/Data_Retention_Directive.

had not yet implemented the Directive or which were forced to annul the national act transposing the Directive due to court decisions is remarkable, the reasons for these circumstances are not the subject of the report. Instead, it focuses on what it regards as main aspects of the Directive and how they were concretely transposed in the other States.

b) Purpose limitation, access and retention period

Six tables illustrate the transposition of the Directive's essential points.[41] The tables show that the purpose for which the data are used, the access to the retained data as well as the retention periods (according to the Directive at least for 6 months and up to two years) vary quite considerably.

With regard to the purposes for which the data can be used, eight Member States (*Belgium, Denmark, France, Italy, Latvia, Poland, Slovakia, Slovenia*) went beyond the requirements of the Directive and allow not only for the use of the retained data in the context of serious crimes, but also for all other criminal offences and for crime prevention or on general grounds or national state and/or public security.[42] Other Member States (*Cyprus, Malta, Portugal, United Kingdom*) do not see the need to define the term "serious crime", which allows in fact for the use of the data for very different purposes as long as they are related to a crime. The list of authorities allowed to access the retained data includes – in addition to police forces and prosecutors – security and intelligence services as well as tax and/or customs authorities and four Member States (*Estonia, Poland, Portugal, Finland*) list additionally border authorities.

Regularly, judicial authorisation is required for access requests, but there are Member States in which there is no such protection measure and the only condition for access is that the requests must be in writing.[43] A (EU-)harmonised procedure for authorities to organise and limit the access to the retained data does not exist. Regarding the types of data to be retained, in most of the cases, the Member States follow the categories described in the Directive. Only *Belgium* does not define the categories of telephony data to be retained, it also does not provide for provisions for internet-related data.[44]

The retention period varies and is regulated in a diverse way. At the time of the report, fifteen Member States had introduced one single data retention period for all categories of data and five Member States provided for different retention periods for different types of data.[45] Some Member States make a distinction between telephone and internet

41 There are six tables showing the purpose for which the data are used, the access to the retained data, the retention periods, the data protection requirements, the age of the retained data accessed and an overview of the Member States reimbursing costs, cf. Report from the *Commission* to the *Council* and the *European Parliament* of 18 April 2011, Evaluation on the Data Retention Directive (Directive 2006/24/EC), COM(2011), 225 final.

42 Point 4.1., p. 6 of the Report from the *Commission*, COM(2011), 225 final.

43 In Finland for instance, subscriber data may be accessed without judicial authorisation; in *Malta* and *Ireland*, the only condition is that the requests must be in writing; cf. table 2, pp. 10-12 of the Report from the *Commission*, COM(2011), 225 final.

44 Point 4.4., p. 13 of the Report from the *Commission*, COM(2011), 225 final.

45 Point 4.5., pp. 13-14 of the Report from the *Commission*, COM(2011), 225 final.

data, others differentiate between unsuccessful call attempts and other data or between fixed, mobile and Internet telephony and internet access and e-mail data.

c) Data Protection and security

Another revealing information of the evaluation report relates to the outcome of the analysis of the data protection and data security requirements. Only 15 of the 23 Member States which had transposed the Directive implemented the required data protection and security principles. In particular the requirement to destroy the data after the retention period has ended did not seem to be addressed by certain Member States (*Belgium, Estonia, Spain*). The report also evaluates the use of the data for law enforcement purposes. The volume of the data accessed by law enforcement varies between 100 (*Cyprus*) and over 1 million (*Poland*) requests per year.[46] The *Commission* does not find an explanation for these discrepancies. Statistics on the actual result of the access requests in relation to the convictions, which were achieved due to the information of the service providers are not mentioned. However, it seems unlikely that such significant differences in the access requests result in an equivalent amount of convictions. Statistics from *Germany* show no noteworthy change in the resolution of crime cases during the time in which data retention in *Germany* was allowed according to the Directive and the period when it was not. A comparison of the crime resolution rate before and after the introduction of data retention between the EU Member States carried out by the *German Parliament* shows no significant change.[47] Only in one (*Latvia*) of 19 countries analyzed, the percentage of cases resolved grew in a statistically significant amount, but even there it is more likely due to the introduction of a new criminal procedure law and not mainly due to the rules concerning data retention.[48]

d) Age of the accessed data

Concerning the age of the accessed data, the report shows clearly that the vast majority of access requests concern the time period of the first six months of the retention of the data, it was actually around 90 % of the requests. After one year of storage only a very small number of requests are still made, concerning mobile phones only 1 %, concerning internet data up to 7 %. This result supports the arguments of critics demanding a shorter retention period and a strict limitation of the time period during which data are maintained for potential access requests.

46 Point 5.1., p. 21 of the Report from the *Commission*, COM(2011), 225 final.

47 Cf. also Analysis by *Max-Planck-Institut für ausländisches und internationales Strafrecht*, Schutzlücken durch Wegfall der Vorratsdatenspeicherung?“, 2nd. version of Juli 2011, available at www.mpg.de/5000721/vorratsdatenspeicherung.pdf.

48 WD 7 – 3000 – 036/11, Sachstand, Die praktischen Auswirkungen der Vorratsdatenspeicherung auf die Entwicklung der Aufklärungsquoten in den EU-Mitgliedsstaaten, Wissenschaftlicher Dienst, Deutscher Bundestag, Autor: Johannes Becher.

e) Interim conclusion

The report concludes with a rather irritating summary. The *Commission* underlines that the EU should "regulate data retention as a security measure" and that Member States' "transposition has been uneven" as well as that "the Directive has not fully harmonised the approach to data retention and has not created a level-playing field for operators".[49] Therefore, the *Commission* considers a review of the Directive, obviously in view to respond to these issues. However, in the meantime, it is clearly stated by the *Commission* that it requires the transposition of the Directive in all Member States including those that have not yet implemented the Directive or which – in view of constitutional doubts by courts – do not plan to implement it. The *Commission* threatens to bring them to the *Court of Justice* for having failed their obligations. This threat seems to have resolved itself after the clear decision of the CJEU against the Directive.

The analysis of the transposition in the Member States shows that the provisions of the Directive have been interpreted in a diverse way. Essential points such as the purpose limitation, access conditions, the retention period or the data protection and security requirements are regulated differently, leading to a very diverse picture of data retention obligations in the Member States and thereby to the opposite result of why the Directive was foreseen. The report of the *Commission* clearly acknowledges this negative result concerning the harmonisation of the retention of telecommunication data in the Member States.

4. The finally initiated preliminary reference questions concerning fundamental rights

a) The referring courts

As mentioned, although a majority of courts dealing with the national transpositions of the Directive refrained from posing a question concerning the actual Directive to the CJEU, the *High Court of Ireland* after the unsuccessful attempt of *Ireland* to bring the Directive to a halt based on the wrongful legal basis action for annulment was planning to introduce a preliminary reference to the *Court*. However, it took a long while after the initial announcements until the *High Court of Ireland* eventually introduced in June 2012 a reference for a preliminary ruling.[50] The applicant in the case is the Irish NGO *Digital Rights Ireland* and the questions the *High Court* referred to the *Court of Justice* are precise and relate to the compliance of the Directive with fundamental rights. More concretely, they refer for instance to the question whether Directive 2006/24/EC is compatible with the rights of privacy of the citizens and the protection of personal data, with the right to freedom of expression and the right to good administration as well as with the right to move and reside freely. The *High Court* additionally asks another interesting question regarding "the extent the Treaties – and specifically the principle of loyal cooperation laid down in Article 4.3 of the Treaty on *European Union* – require a national court to inquire into, and assess, the compatibility of the national implemen-

49 Point 8, pp. 30-33 of the Report from the *Commission*, COM(2011), 225 final.
50 Case C-293/12 *Digital Rights Ireland*.

ting measures for Directive 2006/24/EC with the protections afforded by the Charter of Fundamental Rights [...]".[51]

Soon after the case was lodged at the *Court*, in November 2012 the *Austrian Constitutional Court* in a "class action" case brought by more than 11.000 Austrian Citizens[52] (as well as further actions) against parts of the national telecommunications law transposing the Directive decided to stay proceedings and also refer questions to the *Court of Justice of the European Union*.[53] The *Austrian Constitutional Court* combined the questions concerning the Data Retention Directive with a series of general interpretation questions concerning the Charter of Fundamental Rights.[54] The *Court* joined the two references for the hearing in July 2013 and for the sake of the final decision; the Opinion by Advocate General *Villalón Cruz* was delivered on 12 December 2013 and will be discussed below.

In addition to these joined Cases C-293/12 and C-594/12 for which the judgement was delivered in April 2014 there is a further case pending concerning the validity (and interpretation) of the Data Retention Directive[55]: the Austrian Data Protection *Commission* has asked the *Court* with decision of 28 January 2013 mainly about the rights of later access to the retained data by the individual whose communications data have been retained and again about the fundamental rights compliance of the Directive.[56]

b) The Advocate General's Opinion

Although the *Court* recently decided in the data retention case[57], the Opinion of Advocate General *Villalón Cruz* is worthwhile to look more detailed into as it reveals some fundamental flaws in the way the Directive was conceived, which will remain to be

51 Cf. the questions referred in the Case C-293/12 *Digital Rights Ireland*. The AG does not deal with the last question in detail, but clearly indicates that in view of the CJEU judgement in case C-617/10 *Akerberg Fransson* there is no doubt about the obligation of national courts also to measure the transposition act against the standards of the CFR, Opinion of AG *Cruz Villalón,* para. 153.

52 Noteworthy, the *German Constitutional Court's* decision was also about a joint «Verfassungsbeschwerde» (constitutional complaint), one of which was backed by nearly 35.000 citizens (although technically the final decision did not concern their application which was identical to one of the successful claims). The *Austrian Constitutional Court* was dealing with two further actions in the same line as the class action and all of them are joined for the preliminary reference procedure.

53 Case C-594/12 *Seitlinger and Others*.

54 Cf. for details the questions, to be found in Opinion of AG *Cruz Villalón*, see above fn. 3, para. 17.

55 There was an additional reference request concerning the interpretation of Directive 2006/24/EC by the Administrative Court of Wiesbaden (VG Wiesbaden; *Germany*) that dated back to a decision already in February 2009 and which ended in the ruling in joined cases C-92 and 93/09 *Volker und Markus Schecke and und Harmut Eifert v. Land Hessen*. However, the questions concerning the Directive were declared hypothetical and therefore remained unanswered by the *Court*, cf. para. 38 et. seq.

56 Case C-46/13 *H v. E.*

57 The judgment in the data retention case was delivered shortly before printing of this text. The main points of the decision are summarized in III. 4. c).

problematic even after the final judgement. Also, the questions the *Court* had put forward to the parties and the way they were discussed during the hearing last July indicate a very critical perspective on the validity of the Directive by the CJEU Judges and namely the Juge Rapporteur. One of the points mentioned in the hearing concerned the original intention that the retention of data was ultimately to be useful for resolving "serious crime" and not for the clearing of minor crimes such as theft (which a number of the cases actually concerned according to the Austrian statistics that were requested for the hearing), another the duration of retention. The opinion is also interesting as it proposes some general approaches to the Charter of Fundamental Rights in the area of privacy and data protection that will certainly be discussed controversially in future.

The AG does not answer all questions posed and focuses on the key elements of both references, thereby differentiating between the question of proportionality of the *European Union* taking into account the Data Retention Directive as a measure generally (and using Art. 5.4 TEU as standard), the question about proportionality of the Directive's provisions themselves in view of an infringement of the fundamental rights guaranteed in the Charter (and therefore using Art. 52.1 CFR as standard) and in that connection also whether at all the limitations on the exercise of the fundamental rights were provided for by law as is required by Art. 52.1. CFR. Ultimately, as mentioned above, the AG proposes to strike down the Directive as being in violation of the principle of proportionality without, however, saying that Data Retention as such (and in the form of a EU Directive) is incompatible with fundamental rights. The *Court* followed this Opinion. In consequence, this means that the concept of data retention continues to exist and a different Directive could be prepared, although with due respect of the conditions of the *Court*.

aa) The proportionality test under Art. 5.4 TEU

At first, the Opinion deals with the outcome of the original *Ireland v. Parliament and Council* judgement in which the *Court* rejected the view that the Directive was based on the wrong legal basis. The AG underlines that before the Data Retention Directive was passed, the relevant Directives[58] allowed Member States to introduce a system of retention as an exception to the general principle of secrecy of communications as established by those Directives. The Data Retention Directive then imposed an obligation on Member States to introduce such a scheme even though a number of the exact elements were left to them to complete. Therefore, in the view of the AG, the Directive went beyond merely harmonising (pre-existing and differing) national rules in a specific area to actually creating them via an obligation on the EU level.[59] This observation is decisive for the AG's later conclusion that the Directive necessarily should have included guarantees already at EU level that the introduction of the retention system does not violate fundamental rights and that the fact that the Directive left the design of the retention system in a way that is in accordance with fundamental rights to the national level, was a violation from its inception onwards.

58 The General Data Protection Directive 95/46/EC and the E-Communications Privacy Directive 2002/58/EC.

59 Cf. Opinion of AG *Cruz Villalón,* paras. 35 et seq.; the AG speaks of a « functional duality ».

The way the AG reads the CJEU judgement on the legal basis means that the reliance on the harmonising provision of former Art. 95 TEC would not have been possible if there would not have been such a divergence in existing retention rules, namely that a number of Member States did not have any such obligations at all. This situation made it possible for the *Court* to accept the legal basis as it had been chosen by the *Commission* to be correct. Since the Directive harmonised the (differing) rules applicable to service providers in the sector across *Europe* and thereby avoided distortions and a lesser functioning of the common market, it fulfilled the requirement of the harmonisation provision. In the analysis of the AG this is, however, why the lack of safeguarding provisions in the Directive, which should have accompanied the obligation for Member States to introduce data retention schemes, puts the Directive in violation of fundamental rights even though it is based on the correct legal basis in principle.[60]

The AG points out that his approach may be questioned, but he states that in the legal basis-judgement the *Court* strictly limited itself to answer whether or not Art. 95 TEC was the correct basis without answering whether the instrument chosen is – in view of the aims pursued – disproportionate as measure per se under Art. 5.4 TEU.[61] He goes on mentioning that the standards applied for scrutiny of a measure are different under the general proportionality principle of Art. 5.4 TEU – relating to whether it was at all correct that the EU took action and how it did so – and the proportionality test for infringements of fundamental rights by concrete provisions of such instruments.[62] Even though the EU legislator has a wide discretion when making choices in complex situations, the *Court* can still review whether the motivation of the legislator was "based on objective factors and is not manifestly inappropriate in relation to the objective pursued".[63] Simply said: Introducing a significantly infringing measure (in view of the right to privacy), such as data retention, simply in order to harmonise national rules for improving the functioning of the internal market is on the face (or in the words of *Cruz Villalón*: manifestly) disproportionate.[64] The Directive's second objective – in addition to the harmonization of rules concerning service providers, the availability of the retained data for investigation and prosecution of serious crimes – would be a more valid legitimate aim to limit the fundamental rights, however would not have been sufficient to save the Directive based on former Art. 95 TEC. But this very existence of a second (the "ultimate") aim making the Directive potentially valid under the proportionality test of Art. 5.4 TEU, leads the AG to leave the question open and focus fully on the proportionality test of Art. 52.1 CFR concerning the limitation of the fundamental rights therein.[65]

60 Cf. Opinion of AG *Cruz Villalón,* esp. paras. 46, 102, 118, 123.
61 Opinion of AG *Cruz Villalón,* paras. 85, 88.
62 Opinion of AG *Cruz Villalón,* para. 89.
63 Opinion of AG *Cruz Villalón,* para. 96 (footnote ommitted).
64 Opinion of AG *Cruz Villalón,* para. 100.
65 Opinion of AG *Cruz Villalón,* paras. 103 et seq.

bb) The proportionality test under Art. 52.1 CFR

Of all fundamental rights potentially affected by the Data Retention Directive according to the referring courts, the AG limits the analysis to Articles 7 and 8 of the Charter.[66] In doing so, he puts an emphasis on Art. 7 (the equivalent to Art. 8 ECHR guaranteeing respect for private and family life, home and communications) as the more general privacy-related provision and regards Art. 8 CFR (concerning protection of personal data) as being more specific to the processing of data (an observation which he bases on the explicit provisions of paras. 2 and 3). Although his distinction might not be necessary because Art. 8.1 CFR actually also contains a more "general statement" according to which (more specifically than the general provision of Art. 7) "personal data concerning him or her" are protected as a fundamental right, he makes a refreshing clarification which many involved parties in the discussion of the Data Retention Directive seem to have forgotten in their observation of details and defence of its necessity: Introducing a general scheme of data retention concerning all citizens goes well beyond a simple processing of data. Further, the communications data concerned is – due to its revealing nature, if put together to profile an individual and his behaviour – very private, if not intimate, and therefore the Directive touches the very core of the right to privacy. This he sees as mainly protected by Art. 7 CFR which could, generally spoken, be violated by a measure that in itself is totally compatible with Art. 8 CFR.[67]

Not only is the collected data very private due to its profiling potential, even though this profiling is only realized in a case of actual access to the data, the type of interference with the fundamental rights is particularly serious in the view of the AG. He strongly relies on the observations of the *German Constitutional Court* in its own decision concerning the German law and quotes it several times. Namely he points out that the complete and lengthy retention of all communications data amounts to a "vague feeling of surveillance"[68] which is made worse by the fact that the data is retained by service providers and not the States themselves. The latter have to foresee certain security obligations for providers concerning the data according to the Directive, but the Directive does not detail these. In view of cloud storage options chosen nowadays this entails a significant threat whether the data concerned are actually at all times in a secure environment.

In view of these general observations the AG concludes that the first requirement of Art. 52.1 CFR concerning limitations to the fundamental rights guaranteed by the Charter is not met: All limitations need to be prescribed by law. In line with ECHR case law this does not only mean a formal requirement of existence of a law, but the law additionally needs to have a certain quality.[69] This question has so far not been treated in a case of the *Court of Justice of the European Union*[70] and it is connected to the question of proportionality because the preciseness of the limiting legal act depends on the con-

66 Although his observation concerning a likely violation of Art. 11 CFR's freedom of expression and information is noteworthy, cf. Opinion of AG *Cruz Villalón,* para. 52.
67 Cf. Opinion of AG *Cruz Villalón,* paras. 58 et seq. and 65 et seq., 74.
68 Opinion of AG *Cruz Villalón,* paras. 72 quoting BVerfG, above fn. 8.
69 E.g. recently judgment of the ECtHR in *Yildirim v. Turkey*, Application no. 3111/10, 18 December 2012, paras. 57 et seq.
70 Cf. observation of the AG *Cruz Villalón* in his opinion in fn. 86.

crete extent of the infringement on the right, too. As the Directive of the EU itself introduces an obligation for Member States to limit the fundamental right to privacy, that very Directive at the same time must also foresee in precise terms the guarantees against a too massive infringement.[71] In limiting the fundamental right itself, the EU is to be held responsible for ensuring a justified limitation. This very valuable observation of the AG holds especially true, if one considers the variations of national transpositions e.g. concerning the types of access and the remedies foreseen as was visible from the evaluation report of the *Commission* discussed above. In addition, this very true statement supports the position that Member States' courts at an earlier point could have and possibly should have questioned the validity of the originating Directive and not only the national transposing act, as the potential principal violation of fundamental rights was created already by the Directive irrespective of the margin it left to the Member States in the transposition. That margin served as an argument for most courts to limit their criticism to the national legislator not having used the margin in a more "fundamental rights-friendly manner" and thus avoiding the discussion of the Directive itself.

With this lack of precision in the originating legal act, it is evident that the AG had to declare it as completely incompatible with the horizontally applicable provision of Art. 52.1 CFR in his opinion. However, the AG also indicates which minimum requirements the Directive should fulfil in order to avoid this conclusion. He concretely mentions the guarantees that should be included, such as a definition of "serious crime", regulation of (strictly limited) access, obligation of erasure after the data is no more useful and of information of the data subjects concerned.[72]

In addition to criticizing the insufficient quality of the Directive, the AG also states a violation of the proportionality principle and even though he only analyzes one aspect of the Directive in this respect he indicates that further points could also have amounted to this violation. He criticizes briefly for example that the demonstrated lack or at least doubt of efficiency of the Directive's mechanism due to the relatively easy way of circumventing the retention as well as the low numbers of actually successfully used retained data for purposes of combating serious crimes such as terrorism may lead to the conclusion of making it a disproportionate if not an inappropriate means.[73] The AG recalls that the legitimate aim concerned here is not the harmonization of provisions of Member States for the functioning of the common market but the ultimate goal of "investigation, detection and prosecution of serious crime".[74]

The only element he actually analyzes in detail and regards as violation of proportionality in a strict sense, is the temporal scope of the data retention obligation. As the retention happens in advance of a possible use of the data and not as would be the case in a "quick freeze-system" after the data has occurred and the need for its use is established, the time frame concerned is important in view of the length of the infringement. In a somewhat philosophical analysis – which *Villalón Cruz* admits to being purely subjective – he distinguishes what period of time for retention would be acceptable[75] and concludes that this certainly must be below a year which is why the two year

71 Opinion of AG *Cruz Villalón,* paras. 117 and 118.
72 Opinion of AG *Cruz Villalón,* paras. 125 et seq.
73 Opinion of AG *Cruz Villalón,* para. 137.
74 Opinion of AG *Cruz Villalón,* para. 136.
75 Opinion of AG *Cruz Villalón,* paras. 144 et seq.

possibility for maximum length in the Member States' rules on retention already makes the Directive disproportionate. This seems to be in line with the criticism uttered by some of the Judges in the hearing which is why it came as no surprise that the violation of the fundamental rights in the final judgement is also based on the temporal aspect.[76]

c) The final judgement

In line with the AG, the *Court* in its final decision considered "the interference caused by Directive 2006/24 with the fundamental rights laid down in Art. 7 and 8 of the Charter […] wide-ranging, and […] particularly serious" but did not find the essence of these rights adversely affected, since the content of the retained data is not revealed to the authorities receiving them.[77] All in all, the *Court* mainly follows the arguments of the AG. Whereas the goal of the Directive, namely the retention of data for the later use for crime prevention purposes, is still found to be in accordance with EU law, the requirements of the comprehensive retention provided for in the Directive go beyond what is necessary to protect the mentioned goal. In particular what is *not* regulated in the Directive seems to disturb the *Court*. There are no provisions controlling the access to the data for the authorities, no distinction is made between the data or persons concerned, there is no link between the retained data and a threat to public security or serious crime, there are no provisions limiting the access to the retained data or rules that provide for a storing of the data within the EU, essential notions, such as "serious crime" are not defined and the time limit for retention is too broad.[78] The criticism is extensive and this results in the invalidity of the Directive. The *Court* clearly rejects the whole instrument but it is not entirely obvious whether it gives up the idea of data retention for law enforcement purposes as such. Interestingly, although the *Court* followed the AG in substance, in contrast to his Opinion there is no clause that gives the legislator time to rectify the Directive. This could be understood as a total rejection of data retention as such.

Questions such as for example what consequence the decision has for the national acts transposing the now invalid EU Directive, follow from the judgement and are not yet answered. However, in view of the reasoning in the judgement, it is quite likely that cases against the national acts brought before courts would be successful. The decision is also a clear rejection of the use of unspecified terms, such as "protection of serious crimes", used in many EU instruments to justify interferences with Art. 7 and 8 Charter of Fundamental Rights. Apart from the very specific criticism relating to the retention period or the access conditions, this is a more general statement, essential for the evaluation and drafting of other instruments in this area.

IV. Conclusion: The way forward after the judgment

One consequence from the decision of the CJEU is that the Data Retention Directive in its current form is too vague and at the same time too broad. In view of not only the

76 Case C-293/12 *Digital Rights Ireland*, paras. 63 and 64.
77 *Ibid*, paras. 37-39.
78 *Ibid*, paras. 51-71.

strict safeguards the *Court* demands, but more so considering its general observation in para. 51 that even an overwhelmingly important legitimate aim such as the fight against serious crime including terrorism (and the fact that a right of individuals to security is also inherent, cf. para. 42) by itself cannot justify a measure as far-reaching as the now void Directive, and even more so in para. 52 that infringements to the right to privacy have to be limited to the strictly necessary, it seems possible that the *Court* actually completely rejects the idea of preventive data retention for law enforcement purposes. At least a general and all-encompassing solution seems impossible now. However, further clarification, including a more explicit statement for or against the idea of preventive data retention as such, would have avoided future discussions regarding this question, especially if a new attempt for a revised Data Retention Directive is initiated.

However, in addition to the existing national retention mechanisms introduced across *Europe*, data protection today also faces the challenge of continuous technological development with expanded storing and usage capacities for data and international cross-border exchange and use of data, all of this in light of strongly differing legal regimes.[79] In addition, the data retention initiated by the Directive is in many cases outweighed by at least seemingly consented collection of data by online service providers through acceptance by users. There is a large amount of data collected and exchanged within the EU's agencies and between law enforcement units in the Member States.[80] Therefore, the data retention judgment only closes one open issue, but it has a signal value also for other areas.

A further effect of the decision is related to a harmonizing aspect: the judgment brings the case-law of the EU in line with the decisions regarding Art. 8 ECHR of the *European Court of Human Rights*.[81] In view of a future accession of the EU to the ECHR it was time to end the "data retention saga" at this point and not delay a clarification any further.

For the EU, the hope remains that the *Commission* and the EU legislator will not again in future do the mistake of reacting too fast and with too broad instruments to what was regarded as a pressing need in order to avoid what seems evident many years later: that a significant infringement of very fundamental rights was tolerated in view of a measure that turns out to have somewhat limited efficiency. This seems a general problem of more recent security measures even though many citizens may not currently view this individually as problem, but it should not only be a legally prescribed rule but a politically respected guideline that legal acts are considered and weighed more intensively in their preparation, the more they potentially infringe fundamental rights.

79 Cf. on this e.g. *Weaver/Partlett/Cole*, Protecting Privacy in a Digital Age, in: Dörr/Weaver (eds.), The Right to Privacy in the Light of Media Convergence – Perspectives from Three Continents, Cologne 2012, p. 1 et seq.

80 Cf. e.g. *Boehm*, Data processing and law enforcement access to information systems at EU level – no consistent framework in spite of the data protection reform, DuD 2012, p. 339 et seq.

81 Cf. e.g. the judgment of the ECtHR in *S. and Marper v. the United Kingdom*, Application nos. 30562/04 and 30566/04, 4 December 2008, para. 107.