Prof. Dr. Franziska Boehm — Assistant Professor, University of Münster, Institute for Information, Telecommunication and Media Law (ITM), Germany

Prof. Dr. Mark D. Cole — Associate Professor, Faculty of Law, Economics and Finance and Interdisciplinary Centre for Security, Reliability and Trust (SnT), at the University of Luxembourg, Luxembourg

Data Retention after the Judgement of the Court of Justice of the European Union

– Münster/Luxembourg, 30 June 2014 –

The Greens | European Free Alliance
in the European Parliament

Contact to the authors:

Prof. Dr. Franziska Boehm
Juniorprofessur für IT-Recht

Westfälische Wilhelms-Universität Münster
ITM – Institut für Informations-,
Telekommunikations- und Medienrecht
Zivilrechtliche Abteilung

Leonardo-Campus 9
D-48149 Münster

T +49 251 83-38615

franziska.boehm@uni-muenster.de
http://www.uni-muenster.de/Jura.itm/hoeren/

Prof. Dr. Mark D. Cole
Associate Professor for the Law of the New Information Technologies, Media and Communications Law at the University of Luxembourg, Faculty of Law, Economics and Finance /
Director for Academic Affairs at the Institute of European Media Law (EMR, Saarbrücken)
4, Rue Alphonse Weicker
L-2721 Luxembourg

T +352 46 66 44 68 24

mark.cole@uni.lu
www.medialaw.lu

Funding for this study was provided by the Greens/EFA Group in the European Parliament.

Abridged Table of Contents

Table of Contents

Abbreviations used in the study

AG = Advocate General

CJEU = Court of Justice of the European Union, also referred to hereinafter as Court

CFR = Charter of Fundamental Rights of the European Union

DRD = Data Retention Directive

DRD Judgement = CJEU Cases C-293/12 and C-594/12

ECHR = European Convention on Human Rights

ECtHR = European Court of Human Rights

EDPS = European Data Protection Supervisor

EES = Entry-Exit-System

LE = law enforcement

PNR = Passenger Name Record

TFTP = Terrorist Finance Tracking Programme

TFTS = Terrorist Finance Tracking System

Other abbreviations relating to specific measures are explained in the text.

Executive Summary

This study analyses the Data Retention Directive Judgement of the Court of Justice of the European Union of 8 April 2014 and evaluates its impact on other data retention measures at Member States as well as at EU level.

Results of the analysis of the Data Retention Judgement

With its decision on the Data Retention Directive, the Court's Grand Chamber has delivered a key judgement.

First, the judgement has major consequences on the relationship between the rights to data protection and privacy on the one hand and law enforcement (LE) measures on the other hand in the EU and its Member States. With the complete and retrospective annulment of the Data Retention Directive (DRD) it emphasizes the seriousness of the violation of fundamental rights by the Directive. It opposes the general and undifferentiated nature of data retention measures foreseen in the Directive and gives important clarifications with regard to the relationship between and scope of Article 7 and 8 CFR.

Second, by referring to the guarantees of the ECHR and its interpretation in the ECtHR case law in the context of data retention measures, the CJEU links irreversibly the two legal orders even closer than in the past and opens the possibility to interpret Article 8 ECHR and Article 7 and 8 CFR in a parallel way. Therefore, the statements of the Court not only refer to the singular case of the DRD, but also establish general principles for similar data retention measures.

These principles encompass the following points:

- The collection, retention and transfer of data each constitute infringements of Article 7 and 8 CFR and require a strict necessity and proportionality test.
- The Court clearly rejects the blanket data retention of unsuspicious persons as well as an indefinite or even lengthy retention period of data retained.
- The Court sees a sensitive problem in data originally collected for other purposes later being used for LE purposes. It requires a link between a threat to public security and the data retained for such purposes.
- The required link significantly influences the relationship between private and public actors. LE is only allowed to access data collected for other purposes in specific cases.
- The Court explicitly demands effective procedural rules such as independent oversight and access control.
- The collection and use of data for LE purpose entails the risk of stigmatization stemming from the inclusion of data in LE databases. This risk needs to be considered and should be taken into account when reviewing other existing or planned data retention measures at EU and Member States level.

Results of the analysis of the impact on data retention measures in the Member States

A further outcome of the analysis shows that national measures transposing the DRD need to be amended if they contain provisions close to those of the now void DRD. There is a close link between the standards of the EU Charter of Fundamental Rights and Member State measures in this field which leads to an equivalent standard for the validity test of the transposing law. If governments and parliaments in the Member States do not change their national data retention systems after the judgement, there are ways to challenge the national laws before courts which likely would lead to similar consequences for the national laws as the CJEU drew for the DRD.

The most promising way to have a national data retention law reviewed in light of its compliance with fundamental rights and compatibility with EU law is the initiation of legal proceedings in front of national courts. This will potentially include a preliminary reference procedure initiated by the national court for further clarification. Alternatively, after exhaustion of domestic remedies individuals could claim that national data retention schemes violate Article 8 ECHR before the European Court of Human Rights.

Results of the analysis of the impact on other data retention measures in the EU

The judgement also impacts other instruments on EU level concerning data retention and access to this data by authorities. The study therefore tested seven exemplary EU measures on compatibility with the standards set by the DRD Judgment, namely the EU-US PNR Agreement, the EU-PNR proposal, the EU-US TFTP Agreement, the EU TFTS proposal, the LE access to Eurodac, the EES proposal and the draft data protection directive in the LE sector.

- All analyzed measures provide for data retention and affect an enormous amount of (unsuspicious) individuals. Some of the measures seem to be even more infringing than the original DRD.
- There are fundamental compatibility problems, in particular when it comes to undifferentiated bulk data collection and transfer of flight passenger and bank data to the US.
- The same problems arise with regard to the respective plans to establish similar systems at EU level. The rationale for these measures contradicts in essential points the findings of the DRD Judgement. The Court requires a link between the data retained and a threat to public security that cannot be established if the data of unsuspicious persons is retained in a bulk.
- The analysed measures show considerable shortcomings when it comes to the compliance with the fundamental rights which is why they need to be reviewed in light of the DRD Judgement.

Conclusion

The study has demonstrated the impact of the DRD Judgement on data protection and privacy in the LE sector and on other data retention measures. Essential is that blanket retention of data of unsuspicious persons for the later use for LE is not in line with Article 7 and 8 CFR since it is not possible to establish a link between the data retained and a threat to public security. Any possible future data retention measure needs to be checked against the requirements of the DRD Judgement. If the EU or the Member States plan to introduce new data retention measures, they are obliged to demonstrate the necessity of the measures in every single case.

A further important outcome for EU policy making is that if the EU enacts measures infringing Articles 7 and 8 CFR, it needs to define key terms that justify the infringement, such as the use of the data for serious crime purposes, to avoid a diverse interpretation of such key terms in the EU Member States. Moreover, the principles of the DRD Judgement also require a review of measures with the same rationale. EU bodies, particularly the Commission, must review the existing and planned data retention measures of Member States and the EU duly considering the DRD Judgement. The principles of the DRD Judgement further require a review and re-negotiation of international agreements (EU-US PNR and EU-US TFTP) since these agreements do not comply with some of the standards set in the DRD Judgement. Finally, the Judgement necessitates a redefinition of the relationship between public and private actors with regard to mutual data access and exchange in the law enforcement context.

A. Background and Scope of Study

In a long-awaited and much discussed decision the Court of Justice of the European Union recently declared the EU Data Retention Directive of 2006 void in its entirety. The judgement as well as previously the Opinion of the Advocate General states very clearly that there is a serious violation of fundamental rights by the DRD. The right to privacy in Article 7 of the Charter of Fundamental Rights of the European Union as well as the right to protection of data in its Article 8 were seriously infringed by the requirement contained in the DRD that Member States have to introduce obligations of electronic communications service providers to collect, store and retain for potential access by competent authorities a large number of communication related data.

In a way the Court's judgement finalized a long "saga".[1] Not only had there been a conflict about the competence of the European Union to legislate on the topic, but also several Member State constitutional and other courts had to deal with the national implementations in challenges brought by individuals and courts. The original competency decision of the CJEU clarified that the EU had the legal basis to pass a data retention obligation for electronic communication means – on the basis of the general harmonisation provision – even though the ultimate objective was the combating of serious crime for which the EU did not have a competency. This decision, however, was not apt to pacify the serious controversies and it does not come as a surprise that several of the challenges initiated at Member States level represented a wide popular demand for review. Although the Court has with its judgement clarified that indeed from the very beginning there was a fundamental rights issue and that the courts of the Member States that had struck down national transpositions were obviously on the right track, there are still a number of questions open.

In this context, the authors of the study were asked by the Greens/EFA Group in the European Parliament to elaborate on the consequences the DRD judgement of the Court has. For that purpose the study initially reminds briefly of the history of the DRD and describes the judgements rendered both by the Court of Justice of the European Union and the Member States courts. The main chapter of the study deals with an in-depth analysis of the judgement of April 2014 with a focus on the general conclusions that can be drawn concerning the application of the fundamental rights of Articles 7 and 8 CFR to comparable situations. In that chapter the relevant case law of the European Court of Human Rights in Strasbourg is included as it is integrated by the CJEU into the interpretation of EU law. The following two chapters deal with the further impact of the judgement. First, the situation for the Member States is analyzed, whereby in one part the general obligations stemming from such a decision are presented and in exemplary cases in the other part the concrete consequences for established national data retention schemes. After that the impact of the judgement on other existing or planned data retention measures on the level of the EU is shown, before a conclusion and recommendations finalize the study.

[1] Cf. extensively also Cole/Boehm, CritQ 2014, pp. 58-78.

B. The EU Data Retention Directive 2006/24/EC

This study concerns the European Union's Data Retention Directive which entered into force in 2006. It was mainly a reaction to the terrorist attacks in Madrid of 11 March 2004 and London of 7 July 2005, but for lack of a competency in criminal law, it was based on the general harmonisation provision of the then EC Treaty. The motivation was to create a better functioning common market in the telecommunications sector by replacing the diverse approaches on national level to data retention by a harmonized framework on EU level. Although the Directive was declared invalid by the Court of Justice in the case of *Digital Rights Ireland and Kärnter Landesregierung et al*.[2] due to its incompatibility with fundamental rights, there were serious doubts raised from the very beginning whether a measure creating such a vast effort was efficient in view of the goals it was supposed to be contributing to. It is necessary to briefly shed light on the developments that led to the passing of the Directive and the events since and up to the judgement of the Court.

I. Brief history and overview of the DRD

1. The relevant legal framework previous to the Lisbon Treaty

One needs to remember that before 2009 primary EU law was different in the area relevant for this study compared to today. Most importantly, although there was a provision in Article 286 EC Treaty concerning the application of the EU data protection framework (also to all EC institutions and bodies) there was no general data protection provision as can now be found in Article 16 TFEU.[3]

The equivalence table attached to the Treaty of Lisbon suggests that this new Article 16 TFEU is a replacement of the former Article 286 TEC, but in actual fact the scope of data protection in the EU context is significantly expanded with the Lisbon Treaty. Not only is it a declaratory restatement of the rights to data protection, it also gives the EU a legal basis to create rules concerning processing of data by the EU and its Member States in connection with EU law. Although the equivalence table attached to the Treaty of Lisbon suggests the new Article 16 TFEU is a replacement of the former Article 286 TEC, in reality the new provision significantly expands the scope of data protection in the EU context.

Further, before the amending Lisbon treaty was passed, fundamental rights on the level of the EU were developed by the CJEU, even as a catalogue style of rights (and limitations) was lacking. Although the Charter of Fundamental Rights of the EU already existed since 2000 it had been merely proclaimed and was not legally binding.

[2] CJEU, Case C-293/12, *Digital Rights Ireland* and in Case C-594/12 *Kärntner Landesregierung and Others*.

[3] Cf. also Article 39 TEU concerning data processing by Member States concerning the Common Foreign and Security Policy.

2. The significance of the e-privacy Directive of 2002

When the European Union prepared the creation of a concise regulatory framework for the telecommunications sector, bringing together existing previous Directives and creating new ones in the regulatory framework for electronic communications networks and services package eventually passed in 2002, it was clear that this would encompass a specific Directive concerning data protection for several reasons. Mainly, the EU Data Protection Directive of 1995 was regarded as being too general and technological. Additionally, market development was so rapid that complementing specific rules were needed.[4]

Some Member States had by then already introduced schemes to collect communications related data. Further, provisions allowing retention of this data for consumer protection reasons, mainly in view of verification of billing already existed. The different measures risked contradicting the general data protection rule according to which processing of data is only allowed under certain conditions and that retention of data is the exception to this rule. Therefore, the communications specific data protection Directive 2002/58/EC – commonly referred to as the "e-privacy Directive" – included a rule regarding the exceptional compatibility of retention instruments by Member States. Based on this provision, several States introduced retention schemes into their national laws, many of them taking into account the terrorist attacks in the US on 11 September 2001 and the resulting introduction of intensive monitoring instruments by the US authorities.

3. Policy considerations in preparation of a legal framework for data retention

This diversity of these national rules was seen as detrimental by some and the Commission was under pressure to propose an instrument on data retention from several sides. Plans to establish an EU-wide data retention regime existed long before the above mentioned terrorist attacks of Madrid and London.[5] These plans however were never officially published, but leaked by NGOs.[6] The terrorist attack in Spain in 2004 then provided the possibility for four Member States (France, Ireland, Sweden and UK) to officially publish a draft for a Framework Decision on the retention of data of electronic communications service providers very shortly after the event.[7]

The proposal was met with criticism relating to a possible infringement of Article 8 ECHR, as well as with regard to the legal basis.[8] The basis foreseen was a (former) third pillar choice because of the connection to LE purposes and this would have resulted in exclusion of the European

[4] Cf. also Directive 97/66/EC as a predecessor of the more comprehensive Directive 2002/58/EC that became the sector-specific data protection Directive for the electronic communications sector.

[5] Cf. the statewatch leak in 2002: http://www.statewatch.org/news/2002/aug/analy11.pdf. A detailed analysis of the history leading to the DRD can be found in Robinson, pp. 3-28, esp. p 16 et seq.

[6] Many documents can be found at statewatch: http://www.statewatch.org/.

[7] Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offence including terrorism, Council doc. 8958/04, Brussels, 28 April 2004.

[8] Cf. inter alia Article 29 Working Group, Opinion 09/2004 of 9 November 2004.

Parliament from the legislative process. The discussions were further sparked by leaked opinions of the legal services of both Commission and Council that indicated that due to pre-existing rules applicable to service providers in the area of electronic communications services the instrument would actually have to be placed under the first pillar (as EC law).[9]

The London bombings of 2005 then accelerated the process and the Commission followed the argument of the Parliament that wanted to be involved in the legislative process. Therefore, the substantively more or less exact copy of what was proposed in the draft framework decision was now proposed in form of a draft Directive.[10] The Parliament, willing to prove its participation in anti-terrorism matters, finally swiftly adopted the DRD, not least because the Council had insisted to adopt a Framework Decision in case the Parliament would refuse to agree to the draft Directive.[11] Within three months of the proposal the Parliament voted in favour (less than a year after having rejected the idea of an equivalent text in a Framework Decision) and in February 2006 the DRD was finally adopted in the quickest legislative process in EU history until then.[12]

4. The final Data Retention Directive of 2006

As a result of the situation described above, preparations were soon underway for a Directive concerning data retention. Because the EU Treaties in the version of the Treaty of Nice did not provide a sufficient legal basis for a harmonization of criminal investigation instruments in Member States and the measure could neither be based on a provision concerning data protection, the general harmonization provision in former Article 95 TEC – now Article 114 TFEU – was chosen as the legal basis. This was subject to much criticism from some of the Member States, as the Directive itself mentions as a main goal the prevention and combating of crime and the original approach was consequently a proposal for a framework decision under the former third pillar as mentioned above.[13] This eventually led to a procedure before the CJEU initiated by Ireland which will be discussed below. Irrespective of the criticism, 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 established the obligation of Member States to introduce a system of retention of telecommunications data for a period of six months to two years. The Directive is includes only 17 short articles, but details the exact categories of data to be retained and gives some basic indications regarding data protection and security requirements. However, and this is an early flaw of the Directive, measured against the extensive coverage of data to be retained, there are only very basic requirements that the Member States' rules have to include with regard to the access to data, protection of the data, remedies, liability or the organisation of

[9] Cf. with further references Robinson, p. 18 et seq.

[10] For the change in the legal basis, compare: Roßnagel/Moser-Knierim/Schweda, pp. 13-16.

[11] Roßnagel/Moser-Knierim/Schweda, p. 14.

[12] Cf. Robinson, p. 18.

[13] On this change of approach in order to make the proposal "fit" the constraints of the legal bases available in the Treaty then Robinson, p. 18 et seq.

supervisory authorities. Unsurprisingly, because these wide margins were left, the transposition of the Directive in the Member States was diverse. The original transposition period was one and a half years but this could be prolonged for internet-related data until latest March 2009 (amounting then to three years), an option which Member States generally used.

The national provisions resulted in strong opposition from civil society and politicians in several Member States. As a result many of the laws were challenged before courts. The highest administrative or constitutional courts of Bulgaria, Romania, Germany, Cyprus and the Czech Republic that were confronted with cases about the conformity of national laws transposing the DRD with national administrative or constitutional order declared parts of the or the whole acts void.[14] Although some of these decisions briefly presented below were very severe in the statement of non-conformity with fundamental rights, none of these courts made a reference to the Court of Justice of the European Union for guidance on whether the original DRD itself was possibly itself the violating act and not in conformity with EU fundamental rights. In Germany there was a specific case, because the Constitutional Court's judgement removed in total the existing transposition act, but left open the possibility of creating a new act within the confines of national fundamental rights law. This possibility was never realized due to political controversies in the governments concerned, so there was no transposition in Germany after 2010 and until the DRD judgement of the CJEU was handed down.[15] Sweden had been very late in transposition and was therefore fined a lump sum payment of 3 Million Euro for non-transposition in an infringement procedure before the CJEU.[16]

II. Transposition of the DRD and Related Case Law

1. First Judgement of the ECJ concerning EU Competence in 2009

As mentioned above, due to a conflict over the competence of the EU to pass a Directive concerning data retention in view of criminal investigations, the CJEU already at an earlier stage was confronted with the DRD. After the Directive was passed by majority in 2006, Ireland, joined by Slovakia, brought a case before the European Court of Justice questioning the legal basis of the Data Retention Directive.[17] Ireland argued that the DRD should have been based on a third pillar legal basis, as it was originally planned because it regulates in actual fact the data

[14] Decision of the Bulgarian Supreme Administrative Court of 11 December 2008; Decision of the Romanian Constitutional Court of 8 October 2009; Decision of the German Constitutional Court of 2 March 2010; Decision of the Czech Constitutional Court of 22 March 2011; Decision of the Cypriote Supreme Court of 1 February 2011; for further analysis see De Vries et al., 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, Law & Security Review 28 (2012), 468-475.

[15] Cf. also Commission infringement procedure at the Court, Case C-329/12 *Commission v Germany*, which was withdrawn after the DRD Judgement.

[16] CJEU, Case C-270/11 *Commission v Sweden.* In the EP plenary session of 16 April 2014 Commissioner Malmström confirmed that as a consequence of the Court's DRD Judgement Sweden would be paid back the fine, cf. www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20140416+ITEM-017+DOC+XML+V0//EN&language=EN.

[17] CJEU Case C-301/06 *Ireland v. Parliament and Council*. Cf. further on this section Cole/Boehm, CritQ (2014), p.71 et seq.

retention for law enforcement purposes. This aim is indeed mentioned in Article 1 (1) and (2) DRD according to which the Directive harmonized 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 prosecution of serious crime". From the viewpoint of Ireland the reasoning that the main purpose of the Directive was the harmonisation of the internal market under former Article 95 EC Treaty[18] was misleading, because the real reason was not to facilitate the service providers' cross-border activity in the EU but to have the data available for later use by LE.

Notwithstanding the wording of Article 1 DRD, the Court ruled that Directive 2006/24 regulates operations which "are independent of the implementation of any police and judicial cooperation in criminal matters".[19] With this the Court could conclude that the DRD did actually have the harmonization of the rules concerning activities of service providers in the EU internal market in mind and did not directly concern police purposes.[20] As a result, the Court approved the first pillar choice of Article 95 EC Treaty as the correct legal basis for the DRD and dismissed the case of Ireland and Slovakia.

One possible explanation that the CJEU did not enter into a further discussion of was whether there was at least a second function of the Directive concerning LE purposes and what consequence such a ruling would have had. If the Court had annulled the first pillar choice, any measure concerning data retention on the EU level which was used for LE purposes would have had to be based on a different provision and that would most likely have been a third pillar option. This in turn would have meant that both European Parliament and European Data Protection Supervisor would have been excluded from the legislative process. Politically speaking, this lack of more direct control of the measure by the Parliament in a matter concerning the everyday life of EU citizens was possibly seen as more negative. With the abolition of the pillar structure by the Treaty of Lisbon a competency case concerning the DRD after 2009 may have ended differently, although this is speculative.

2. Member States Courts' Decisions concerning National Transposition Acts

As the DRD resulted in the storing of huge amounts of data of unsuspicious persons, the main criticism uttered in Member States was related to the infringing effect the DRD had on the fundamental rights of privacy and free correspondence. In addition, specific data protection issues and – as one Court put it – the "diffusely threatening feeling of being watched" as a consequence of mass data retention were further important aspects in the judicial evaluation.[21] As mentioned above, these questions were left unanswered by the initial judgement of the

[18] 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*, para 63.

[19] CJEU Case C-301/06 *Ireland v. Parliament and Council*, para 83.

[20] CJEU Case C-301/06 *Ireland v. Parliament and Council*, para 84.

[21] 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 judgement.

Court. Although the CJEU had in its above-mentioned decision underlined that it had not dealt with the issue of conformity with fundamental rights, national courts dealing with the transposition acts obviously had to focus on this question and decided to conclude without a further guidance by the Court of Justice. Instead, national courts restricted their judgements to questions of compliance of the national act transposing the DRD with national constitutional law leaving the EU instrument itself untouched until the cases initiated by Irish and Austrian courts reached the CJEU in 2012. These cases are discussed in detail below. In addition, to the hereinafter briefly mentioned decisions of national supreme courts of Bulgaria, Romania, Germany, Cyprus and the Czech Republic there were other cases in Member States still pending when the CJEU gave its DRD judgement in 2014.[22]

a) The Decision of the Bulgarian Supreme Administrative Court

The Bulgarian Supreme Administrative Court decided on validity of the national transposition act of the DRD already in December 2008.[23] It annulled a part of the act, because there was a lack of privacy guarantees and because there were no sufficient limitations concerning access to the retained data. The court identified the procedure for receiving access to the retained data as crucial and because the national act did not specify these sufficiently, the court declared the act to be in breach of the Bulgarian Constitution. Lack of such rules and even on the actual retention procedure could lead to violations against which there were no safeguards. As a result, a number of articles of the Bulgarian data retention act were declared void, but not the act in its entirety. The Bulgarian legislature amended the act according to the court's requests and an amended data retention act has since been in force.[24]

b) The Decision of the Romanian Constitutional Court

A more fundamental reaction could be seen in the Decision of the Romanian Constitutional Court in October 2009.[25] The Court annulled in total the national transposition act[26] due to its unconstitutionality. The Court severely criticized the act and found a number of reasons why it did not conform with the constitutional order, namely the rights of privacy (Article 26 of the Constitution), inviolability of domicile (Article 27), secrecy of communications (Article 28) and generally the right to free development of human personality (according to Article 1 (3)).

As a starting point, in view of the restrictions the act had concerning the right to private life, the secrecy of correspondence and the freedom of expression. The court underlined that the wording was imprecise and not clear, thereby violating Article 53 which sets the requirements

---

[22] 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, (2013) 10:3 SCRIPTed 339.

[23] Cf. http://edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention and http://www.aip-bg.org/documents/data_retention_campaign_11122008eng.htm.

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

[25] Decision No. 1258 of 8 October 2009, published in December 2009.

[26] Law No. 298/2008, published in the Official Monitor No. 780 of 21 November 2008.

for provisions restricting fundamental rights. This criticism related *inter alia* to the provisions about access of "state bodies" which could be interpreted as encompassing any security or intelligence authority. It went further in saying 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 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."[27]

The Romanian court compared the rules on data retention with other LE rules and expressed deep concern that the framework for audio and video surveillance in criminal investigations was much stricter than for data retention although that measure is only used against persons suspected of a crime. In the court's view this was especially problematic because the intrusion in the fundamental right by data retention happened continuously and without being justified by a specific reason such as a suspicion. In that way the exceptional admissibility of retention became the rule and reversed the rule/exception as foreseen by privacy laws. Also problematic was the fact that the secondary legislation that was supposed to give more precise rules on the implementation of the act, was never passed. As a consequence of the judgement and even though the criticism had been fundamental[28], the Romanian Parliament passed a new law under turbulent circumstances. The initial draft for this new law which was prepared under pressure of the Commission to follow-up the obligation of transposition, was rejected by the Senate, but in May of 2012 finally adopted by the Parliament and promulgated by the President in June 2012.[29] The amended law was criticized by many even more intensively as it actually s a near copy of the original law with only few amendments and does not respond to the different points criticized by the court.[30] Especially the refusal to insert specific procedural safeguards, but to rely instead completely on the procedures contained in the Criminal Procedure Code seems to be in contradiction to the requirements set by the court. However, no new case has been brought before the court concerning the law of 2012.

c) The Decision of the German Federal Constitutional Court

Maybe the most debated judgement concerning the DRD transpositions was handed down in March 2010 by the German Constitutional Court. It annulled essential parts of the German

---

[27] 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 (emphasis added); cf. also De Vries et al., p. 3 et seq.

[28] Cf. for further details also country report update on Romania in Invodas-study, available at http://www.emr-sb.de/tl_files/EMR-SB/content/PDF/Gutachten%20Abgeschlossene/INVODAS_Country%20Report%20Romania.pdf.

[29] Act no. 82/2012 published in the Official Monitor No. 406 of 18 June 2014 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.

[30] Cf. e.g. country report update on Romania in Invodas-study, available at http://www.emr-sb.de/tl_files/EMR-SB/content/PDF/Gutachten%20Abgeschlossene/INVODAS_Country%20Report%20Romania.pdf.

telecommunications law amendments concerning the provisions implementing the EU DRD[31]. As a result of that judgement there was a lack of transposition until the final DRD judgement of the CJEU. As already mentioned, the Federal Constitutional Court restricted its criticism to the German provisions transposing the Directive and even though that criticism was severe, it did not consider asking the CJEU for a review of the EU Directive itself, but instead showed a fundamental disapproval with the German legislature's interpretation of the EU Directive when preparing the transposition. The court declared the manner of transposition to violate the principle of proportionality in view of the aims the DRD sought to achieve, meaning that the court saw room for an interpretation of the DRD implementation obligation that would possibly not be in violation of the Constitution.

The act under scrutiny, however, was regarded to violate Article 10 of the Grundgesetz which protects the secrecy of telecommunications. Data retention for LE purposes is not per se incompatible with this provision of the Constitution in view of the Court[32], but the measures to protect citizens against massive infringement of their fundamental rights were seen to be insufficient. The Federal Constitutional Court emphasized that the collected data could be used to establish "meaningful personality profiles of virtually all citizens and track their movements".[33] This would necessitate very high standards for data security, transparency of the processing and legal protection against violations including the possibility of effective sanctions. A central element of the decision was that the use of retained data for investigation and prosecution of crimes requires that "there must at least be the suspicion of a criminal offence, based on specific facts, that is serious even in an individual case".[34] The lack of a precision of which types of criminal offences justify requesting access to the data was seen as a violation in itself, because this left too much room for interpretation.[35] The German Parliament could not agree on whether and how to re-introduce data retention measures to transpose of the DRD in the years after the judgement and this situation remained until the DRD Judgement of the CJEU, which is why the Commission initiated the above mentioned infringement procedure against Germany.

d) The Decision of the Cypriot Supreme Court

A further decision on data retention was issued in February 2011 by the Cypriot Supreme Court.[36] Interesting in this case was that the national court pointed out, that parts of the transposition went even beyond the requirements of the DRD and it declared those parts void. In Cyprus, too, the rights to privacy and secrecy of correspondence and communication (guaranteed by Articles 15 and 17 of the Cypriot Constitution) were regarded to be violated due to the access of the police to the retained data. The court required a limitation of the cases in

[31] Judgement of the Bundesverfassungsgericht of 2 March 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08.

[32] Compare point 3 of the English summary translation of the judgement.

[33] Compare point 3 of the English summary translation of the judgement.

[34] Compare point 4 of the English summary translation.

[35] For further points of criticism cf. Cole/Boehm, CritQ (2014), p.58-78.

[36] More information can be found at http://edri.org/edrigramnumber9-3data-retention-un-lawful-cyprus/ and Markou, Computer Law & Security Review 28 (2012), 468-475.

which access to the data stored would be possible, especially since Article 17 of the Cypriot Constitution expressly limits interferences with the right to secret correspondence to cases of "convicted and unconvicted prisoners and business correspondence and communication of bankrupts during the bankruptcy administration".[37] The decision of the Cypriot Supreme Court was narrower than the ones mentioned above as it limited its criticism to the access and use rules which could be rectified.[38]

e) The Decision of the Czech Constitutional Court

Another constitutional challenge in a Member State was decided in March 2011 by the Czech Constitutional Court resulting in some of the provisions of the national transposition act of the DRD to be held void. The court raised doubts about the necessity and proportionality of data retention especially as the national rules went beyond the fight against serious crime and terrorism.[39] In the view of the court a major drawback from the perspective of the fundamental rights holders was that the law did not oblige the authorities to subsequently inform the persons concerned that their data had been requested.[40] Again, as in some of the cases above, the wide range of authorities that were in principle entitled to access the data and the lack of limitation of purposes was subject to criticism by the Czech Constitutional Court.[41] Not only did the court criticize that the national act went beyond the aims of the DRD, but it explicitly demanded from the legislature that the use of the retained data was only allowed if the aim could not be reached by other instruments.[42] The decision of the court left serious doubts as to whether or not it was at all possible to implement the DRD in conformity with national constitutional provisions, but the Parliament passed a new Data Retention Act taking into consideration the criticism conveyed.[43]

III. Focus of Criticism on the DRD and Transposition

The national courts which dealt with the transposition acts of the DRD criticized similar points. Most of them regarded blanket data retention measures as such, already to be problematic in view of fundamental rights guarantees and only exceptionally admissible with a robust set of guarantees and safeguards. In most cases, the vagueness of the provisions in national law, especially concerning who could access the retained data for which purposes, was seen as

---

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

[38] Cf. Markou, Computer Law & Security Review 28 (2012), 468, 472.

[39] Decision of the Czech Republic Constitutional Court of 22 March 2011, paras 55-57; for an unofficial English translation of cf. http://www.slidilove.cz/en/english/english-translation-czech-constitutional-court-decision-data-retention; cf. also Czech Constitutional Court rejects data retention law, EDRi, 31 March 2011, available at http://edri.org/czech-decision-data-retention.

[40] Para 47 of the judgement.

[41] Para 48 of the judgement.

[42] Para 48 of the judgement.

[43] 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, IRIS 2012-9:1/15.

reason for incompatibility with constitutional requirements. Further, the fact that the retention could take place without a specific cause, and was applied to everyone using electronic communications was identified as a significant and problematic difference to other LE instruments. Some of the courts went into great detail about the incompatibility of specific provisions of the national acts. From the judgements it becomes clear that the retention schemes were questionable in total as the balancing between aim and seriousness of infringement had not been done in view of the rights of the persons concerned. Therefore, it is surprising – although politically understandable – that none of these courts initiated a preliminary reference procedure questioning the original source instead of trying to find in the detail of the national transposition act errors that could be "repaired". This had been criticized[44] and therefore the decisions – albeit after lengthy considerations – of first the Irish High Court and subsequently the Austrian Constitutional Court were welcomed with relief as they gave the Court of Justice of the European Union the chance to revisit the fundamental rights questions left open in its initial (competency) judgement on the DRD. In view of the fact that the Court clearly and without room for interpretation stated that "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"[45] it is, retrospectively speaking, an even stronger disappointment that the national courts did not act earlier and thereby contributed to a more swift clarification of the validity (or actually invalidity) of this important piece of EU secondary law.

[44] Cf. e.g. for the German Federal Constitutional Court: Giegerich, ZEuS 1/2014, p.3-17.

[45] Ibid., para. 69, Advocate General Cruz Villalón had formulated even clearer that the Directive „is as a whole incompatible with Article 52 (1) of the Charter of Fundamental Rights of the European Union", AG Opinion, para 131 and suggested answer part 1, para. 159.

C. The CJEU Judgement in Cases C-293/12 and 594/12 Annulling the Data Retention Directive

I. Background of the Judgement

With its judgement on the 8th of April 2014[46] (DRD Judgement) the CJEU has taken a landmark decision.[47] It has annulled the so called Data Retention Directive 2006/24/EC, which laid down rules concerning the storing of the entire traffic and location data arising from usage of electronic communications systems by the service providers. The data retention requirement needed to be transposed into Member States law whereby certain aspects of the DRD left ample space for Member States implementation, such as e.g. the period of retention foreseen which was to be within the range of minimum 6 months and maximum two years. The DRD was declared invalid by the Court in its entirety and with immediate effect, based on a violation of Articles 7 and 8 CFR.

The Court's judgement concerned two joined cases which were references for a preliminary ruling by the Irish High Court and the Austrian Constitutional Court.[48] The applicant in the Irish case was the NGO "Digital Rights Ireland" and the referring High Court asked a series of questions relating to the fundamental rights compatibility. It also requested to clarify "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 implementing measures for Directive 2006/24/EC with the protections afforded by the Charter of Fundamental Rights [...]".[49] This latter question was not answered specifically by the Court but will be dealt with here under part D. The Austrian case originates in a "class action" brought by more than 11.000 Austrian Citizens[50] (as well as further actions) against parts of the national telecommunications law transposing the DRD.[51] The Court joined the two references for the hearing in July 2013 and for the sake of the final decision; the Opinion by AG *Villalón Cruz* was delivered on 12th of December 2013.

The judgement concentrates on the scope, interference and possible justification of infringements of the fundamental rights concerning the right to private life and data protection. Therefore, the Court, beyond analysing the relevant provisions in the CFR, focuses also on the

---

[46] CJEU, C-293/12 *Digital Rights Ireland* and 594/12 *Seitlinger and Others*.

[47] Compare in this sense also view expressed in Information Note by the General Secretariat for the Council of the European Union, 5 May 2014, para. 19.

[48] Further details on the originating cases can be found in Cole/Boehm, CritQ (2014), 58, 71 et seq.

[49] Cf. the questions referred in the Case C-293/12 *Digital Rights Ireland*.

[50] The above mentioned German Constitutional Court's decision about the national implementing Act 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.

[51] CJEU, C-594/12 *Seitlinger and Others*.

respective Article 8 of the European Convention on Human Rights (ECHR) and its interpretation by the European Court of Human Rights (ECtHR) in Strasbourg.

II. Impact of ECHR and ECtHR Jurisprudence

1. Relevance of ECtHR jurisprudence in general

The general relevance of the ECHR and the respective ECtHR case law in the context of European Union law is based on several factors. Before the EU Treaties contained an explicit reference to Fundamental Rights, the CJEU had developed EU (or originally EEC/EC)-specific fundamental rights as so-called "general principles" which have the same validity as primary law. In doing so, the Court used Member States constitutional traditions as source of inspiration and more frequently the ECHR due to the fact that all EU Member States are also bound by this international convention as signatory States. Since the Treaty of Maastricht there have been references to this methodology as well as an explicit reference to the ECHR.

Today this is Article 6 TEU, which firstly declares the CFR to have the same value as the Treaties and requests an accession of the EU to the ECHR. Finally, it also points out that the Charter rights are to be interpreted according to the horizontal provisions in Title VII. One of these provisions concerns the interpretation of Charter rights which resemble the provisions of the ECHR. Namely, Article 52 (3) CFR states that for rights which correspond to the rights of the ECHR "the meaning and scope of those rights shall be the same as those laid down in the Convention". Consequently, the ECtHR case law is not only a general source of inspiration when creating general principles but more specifically a guiding authority for the interpretation of certain Charter provisions.

2. Specific relevance in the case of DRD

One of the provisions which is nearly identical, is Article 7 CFR that resembles Article 8 ECHR with the respect for private and family life.[52] In addition, the Charter contains a specific provision (Article 8 CFR) that relates to the protection of personal data which is not explicitly contained in the ECHR but has been acknowledged by the ECtHR as an integral part of Article 8 ECHR since a long time.[53] As there is only a limited amount of judgements of the CJEU concerning data protection before the Charter entered into force as binding law with the Treaty of Lisbon in 2009, the Court referred to both the ECHR provision as well as corresponding case law.[54] Consequently, the CJEU explicitly mentions several relevant decisions of the ECtHR also in its DRD judgement.[55] These cases deal with different types of data retention schemes that were

[52] The only difference in wording being the replacement of "correspondence" and "communications" which is not intended to have a different meaning in substance.

[53] 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.

[54] Compare e.g. CJEU, joined Cases C-465/00, C-138/01 und C-139/01, *ORF,* paras. 72 et seq.

[55] Compare DRD Judgement, paras 35, 47, 54, 55.

evaluated in light of Article 8 ECHR. Irrespective of the differences in the underlying cases, the ECtHR has developed some generally applicable standards that it mentions throughout the cases. The CJEU refers to these repeatedly which underlines the relevance for the reasoning in the DRD judgement. This is especially noteworthy, as the AG had widely refrained from doing so in his opinion and especially did not mention the cases concerning retention measures. By picking up the ECtHR arguments and integrating them extensively into the judgement which concerns a specific type of data retention – in this case for communication data – the CJEU judgement must be read in a way that allows general conclusions for any type of retention measure.

3. Applicable ECtHR case law

The cases mentioned by the CJEU in the DRD judgement relate to several landmark decisions of the ECtHR involving the balance of rights in the context of data collection and retention measures. Particularly mentioned are *Leander v. Sweden*, *Rotaru v. Romania, Weber and Saravia v. Germany, Liberty and Others v. United Kingdom*, *S. and Marper v. United Kingdom* and *M.K. v. France*.[56] While all cases include essential general principles in the context of data storage, *S. and Marper v. United Kingdom* and *M.K. v. France,* are of specific importance since the facts and circumstances of these cases are similar to the DRD situation and concern also the mass collection and storage of data for LE purposes. The key statements of these cases are briefly recalled here.

a) The case of S. and Marper v. United Kingdom

The main question of the *S. and Marper v. United Kingdom*[57] case concerned the conformity of the UK national DNA database with the guarantees of Article 8 ECHR. More specifically, the Strasbourg Court had to answer the question whether the continuous retention of fingerprints and DNA data of persons who had once been suspected, but not convicted of criminal offences was in accordance with Article 8 ECHR.[58]

Since its early case-law on data retention measures in the 1970s, the ECtHR proceeds on the assumption that the storage of data constitutes an interference with Article 8 ECHR.[59] Throughout the course of its case law, the ECtHR gradually expanded this assumption to various categories of data.[60] In *S. and Marper v. UK*, the ECtHR confirmed this understanding with regard to fingerprint and DNA data.[61] Fingerprints, for instance, contain "unique information

[56] Compare DRD Judgement, paras 35, 47, 54 and 55.

[57] ECtHR, S. and Marper v. UK (in the following S. and Marper), no. 30562/04 and 30566/04, judgement of 4 December 2008 (Grand Chamber).

[58] ECtHR, S. and Marper, para 106.

[59] ECtHR, Klass v. Germany, no. 5029/71.

[60] For instance in Klass v. Germany, the ECtHR held that interception of telephone communications by State bodies constitutes an interference, later this was expanded to video footage or telephone calls.

[61] ECtHR, S. and Marper, para 67.

about the individual concerned" and allow the "person's identification with precision in a wide range of circumstances".[62]

The retention of data not only constitutes one interference, the access of authorities to data stored in a governmental or non-governmental database also amounts to a separate interference with Article 8 ECHR. The CJEU in its DRD judgement, as will be shown below, refers to this interpretation of interference in the DRD judgement and concludes that the access of LE to data stored at the service providers needs therefore to be justified in light of Article 7 CFR.[63]

The *S. and Marper v. UK* case is relevant not only with regard to the interference, the ECtHR also stipulates important general principles with regard to the justification of data retention measures in light of Article 8 ECHR. The ECtHR recognized the detection and prevention of crimes as being a legitimate aim for the interference[64], but also stated that the margin of appreciation granted to the Member States when enacting data retention legislation would narrow "where the right at stake is crucial to the individual's effective enjoyment of intimate or key rights", such as Article 8 ECHR.[65] Taking this general statement as a basis, the ECtHR further detailed its argumentation.

The Strasbourg Court criticised the possibility of indefinite retention of fingerprint and DNA data. It was "struck by the blanket and indiscriminate nature of the power of retention in England and Wales" and pointed to a special risk with regard to the use of new technologies in a LE context[66]:

> "The Court observes that the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests."[67]

The ECtHR criticised the way the database had been established by the British government. Emphasizing that the retention of data must always be proportionate in relation to the purpose of collection, the ECtHR required as a minimum criterion a limited period of storage. Additionally, it clarified that retaining data irrespective of the nature or gravity of the offence or the age of the suspected person was not in line with the guarantees of the ECHR.

> "The Court further considers that the retention of the unconvicted persons' data may be especially harmful in the case of minors such as the first applicant, given their special situation and the importance of their development and integration in society."[68]

---

[62] ECtHR, S. and Marper, para 84.
[63] DRD Judgement, para.35.
[64] ECtHR, S. and Marper, para100.
[65] ECtHR, S. and Marper, para 103.
[66] ECtHR, S. and Marper, para 119.
[67] ECtHR, S. and Marper, para 112.
[68] ECtHR, S. and Marper, para 124.

The Court found that the presumption of innocence and the risk of stigmatisation demanded a different treatment (of data) of convicted and not convicted persons.

> "Of particular concern in the present context is the risk of stigmatization, stemming from the fact that persons in the position of the applicants, who have not been convicted of any offence and are entitled to the presumption of innocence, are treated in the same way as convicted persons."[69]

The "the blanket and indiscriminate nature" of the powers of retention of persons suspected but not convicted of offences constituted an arbitrary form of retention and failed therefore to strike a fair balance between the competing public and private interests.[70]

Moreover, law makers need to distinguish between different types of offences (serious and less serious) and have to establish possibilities to have the data removed from the database when balancing the rights of individuals against the interest of the state in a data retention context. Independent review mechanisms have to be in place to monitor and assess the reasons for the retention. Pre-defined criteria, such as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances need to be taken into account when assessing the justification for retention. Finally, retention has to be always limited in time as already pointed out above.[71] In this case, the UK "overstepped any acceptable margin of appreciation" and violated Article 8 ECHR.

Due to the clear criteria developed by the ECtHR in this decision, important general principles with regard the minimum protection standards in context with the storage of data in LE databases can be derived. Certainly, one key element is the distinction between suspicious and unsuspicious persons in data retention cases. Time limitations, the distinction between different types of offences, effective deletion possibilities and independent review mechanism are further important principles. These principles are referred to by the CJEU in the DRD judgement. This should be borne in mind when later analysing the impact of the DRD judgement on other data retention measures.

b) The case of M.K. v. France

The general principles developed in the *S. and Marper v. UK* case were recently confirmed by the ECtHR in *M.K. v. France*.[72] Similar facts and circumstances caused the ECtHR to repeat its reasoning with regard to the retention of data of innocent persons in LE databases, giving these principles a more general value. The facts of this case can briefly be summarized as follows.

In *M.K. v. France*, the applicant's fingerprints were stored in the French national fingerprint database due to two allegations of book theft. The fingerprints were taken on both occasions and stored twice in the database although in the first set of proceedings he was acquitted and the second set of proceedings was discontinued. In addition to the fingerprints, the database

[69] ECtHR, S. and Marper, para 122.

[70] ECtHR, S. and Marper, para 125.

[71] ECtHR, S. and Marper, para 103 et seq.

[72] ECtHR, M.K v. France, no. 19522/09, judgement of 18 April 2013.

contained the person's name, sex, date and place of birth as well as the applicant's parents' names. While successfully requesting the deletion of the data related to the first proceedings, the applicant failed to achieve the deletion of the data related to the second proceedings. The French government forwarded an interesting reason for the refusal. The deletion of *M.K.'s* data related to the interest in the government to rule out identity theft, in case someone else should try to use *M.K.'s* identity in a possible criminal context. Approving this reasoning would have paved the way for indiscriminate storage of biometric data of an indefinite number of persons. Therefore the ECtHR clearly opposes these arguments:

> "Besides the fact that such a reason is not explicitly mentioned in the provisions […] of the impugned decree, […] the Court considers that accepting the argument based on an alleged guarantee of protection against potential identity theft would in practice be tantamount to justifying the storage of information on the whole population of France, which would most definitely be excessive and irrelevant."[73]

Further, the ECtHR dealt with the question whether the practice of retaining fingerprints in a LE database of a person who was never found guilty violates Article 8 ECHR. As already seen in *S. and Marper v. UK*, the ECtHR regarded the mere retention of fingerprints as interference and examined the necessity and proportionality of the measure.[74] While the detection and prevention of crimes was considered being a legitimate aim, the Strasbourg Court emphasized the fundamental importance of Article 8 ECHR for the enjoyment of key rights. It repeated that the margin of appreciation considerably decreases, if the affected rights were crucial for the exercise of such key rights. Effective safeguards needed to be in place, in particular where "the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes."[75]

Against the backdrop of these general statements the Strasbourg Court referred to the case of *S. and Marper v. UK* and based its criticism on similar reasoning. As in *S. and Marper v. UK*, the French database barely made a distinction between minor and serious offences.[76] This indiscriminate retention requirement contradicts the established purpose limitation principle which requires that the domestic law should ensure that the stored "data are relevant and not excessive in relation to the purposes for which they are stored".[77]

The ECtHR further referred to the risk of stigmatization stemming from the fact that there was no distinction made about whether or not the person concerned had been convicted by a court or had been even prosecuted.[78] France therefore violated the presumption of innocence by treating convicted and not convicted persons the same.

---

[73] ECtHR, M.K v. France, para 37.

[74] ECtHR, M.K v. France, para 26 et seq.

[75] ECtHR, M.K v. France, para 32.

[76] The circumstances that book theft leads to an entry in this database proved this finding.

[77] ECtHR, M.K v. France, para 32.

[78] ECtHR, M.K v. France, para 39.

In addition to the principles already mentioned in *S. and Marper v. UK*, the ECtHR debated another crucial point constantly subject to discussion in a LE context. The data in the French database could be stored for a long retention period of 25 years. Moreover, as in many LE contexts, the French law only provided for the deletion of data if the data became unnecessary for the purpose of the database. The purpose of the database, according to the ECtHR, is, however, to collect as much data as possible.[79] This purpose has to be seen in light of the deletion provision and was regarded by the Strasbourg Court as a contradiction in itself making the safeguard of deletion ineffective. Therefore, it considered the data retention period as excessive and referred to the requirement of deletion as an essential safeguard against abuse. It concludes:

> As the chances of "deletion requests succeeding are at best hypothetical, a twenty-five-year time-limit is in practice tantamount to indefinite retention".[80]

The ECtHR considered deletion in this case as being "theoretical and illusory" rather than "practical and effective".[81]

This reasoning is crucial in LE contexts. It means that even if States limit the retention of data to a specific period of time, the deletion of data must be constantly possible to guarantee effective safeguards against abuse. The argument that data are only deleted if they are not necessary for the purpose of the database anymore is not regarded as a valid argument, if there is not a practical and effective possibility of deletion during the retention period. Against this background, the storage of data in the French database violated Article 8 ECHR.

The *M.K. v. France* case confirmed the general principles developed in *S. and Marper v. UK* concerning the balancing of rights in data retention cases. As already mentioned, these principles were repeatedly referred to by the CJEU in the DRD judgement. This allows general deductions for other types of data retention measures.

c) Interim Conclusion

Analysing the outcome of these cases makes it possible to draw some general conclusions with regard to data retention schemes. In cases of collection, storage and use of data relating to the private life of an individual, there is always an infringement of Article 8 ECHR. As applies for other rights as well, while States enjoy a margin of appreciation when implementing rules that affect Article 8 ECHR, the more the fundamental right is adversely affected by a measure, the narrower the margin of discretion becomes. The ECtHR further underlines that measures infringing data related aspects necessitate at least safeguards preventing excessive and unlimited collection, storage and use.

In general, there are four main principles the ECtHR refers to in its analysis of these cases:

---

[79] ECtHR, M.K v. France, para 36.

[80] ECtHR, M.K v. France, para 41.

[81] ECtHR, M.K v. France, para 42.

- Firstly, it demands at least that the legislature defines different types of offences and limits access and retention obligations to particular cases. From this, one can conclude that retention measures must be limited to the more serious categories of crimes. Evidently, the ECtHR in its cases always only measured (and declared as violating the fundamental right) a concrete retention scheme against the ECHR standard without indicating under what circumstances data retention measures *as such* are at all acceptable.
- Secondly, the ECtHR stresses that there is a risk of stigmatization if data of unsuspicious persons are treated in the same way as data of criminals. Already this statement clarifies that any type of indiscriminate data retention regime risks violating fundamental rights as it can lead to discriminatory effects.
- Thirdly, the ECtHR highlights the importance of effective procedural rules in cases of data retention measures. Examples are that persons concerned by the retention need to have information, access and deletion rights in order to be able to effectively remedy infringements that occurred. A rather theoretical possibility to have the data deleted is not sufficient to comply with Article 8 ECHR.
- Fourthly, the period of any retention measure needs to be limited in time by the legislature, taking into consideration the seriousness of the interference.

These principles, as mentioned above, are integrated via the case law of the ECtHR that the CJEU refers to in its DRD judgement. Because the principles point beyond the specific case circumstances they are to be interpreted as not just having impact on the form of data retention as it was subject of the case. Instead, they reflect fundamental principles which need to be considered for any type of data retention – and comparable measure – that is foreseen in EU law.

III. Impact of the EU Charter of Fundamental Rights

The Court's judgement – as well as the Opinion of the AG – centres around the fundamental rights compatibility test. It identifies the (obviously) relevant provisions and then applies them by defining their scope, analyzing whether and what level of interference the DRD constitutes. It finally undertakes a detailed proportionality test in view of the possible justifications for the DRD measures; in doing so it identifies special requirements that interferences with Articles 7 and 8 CFR have to satisfy compared to the general fundamental rights compatibility test.

1. Relevant provisions of the Charter for the judgement

The judgement concerns mainly Article 7 CFR which, as mentioned above, resembles Article 8 ECHR with its right to privacy. Further Article 8 CFR, the data protection-specific rights provision of the Charter (compared to the lack of an explicit mention in the ECHR), is taken into detailed consideration. These two provisions read as follows:

Article 7: Respect for private and family life

> Everyone has the right to respect for his or her private and family life, home and communications.

Article 8: Protection of personal data

> (1) Everyone has the right to the protection of personal data concerning him or her.
>
> (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> (3) Compliance with these rules shall be subject to control by an independent authority.

The relevance of these two provisions in the context of a scrutiny of data retention measures is not only obvious from the wording of the Charter provisions, but also because the DRD itself mentions in recital 22 that it "seeks to ensure full compliance with citizens' fundamental rights to respect for private life and communications and to the protection of their personal data, as enshrined in Articles 7 and 8 of the Charter".[82] The Court confirms that the retention of data for the purpose of possible later access by the competent national authorities directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 CFR.[83] Moreover, data retention constitutes a form of processing of personal data within the meaning of Article 8 CFR and therefore must satisfy the data protection requirements of that article.[84] In his opinion, the AG considers how Article 7 and 8 CFR are related to each other and differentiates which one is applicable and to what context.[85] The Court does not rely on this section in its judgement but rather lists the different types of infringements that take place as a consequence of the DRD (see below) and assigns each of these as falling into the domain of either the one or the other Charter right.

Additionally, because one of the referring courts addressed the issue, the AG and the Court briefly mention the possibility of an infringement of Article 11 CFR, which protects the freedom of expression and information. This is worth noting as the AG made some interesting remarks with regard to a possible infringement of Article 11 through data retention measures. He confirmed a link between the fact that a general retention of data may lead to a "vague feeling of surveillance"[86] which could in turn have an important influence on the way citizens use their

---

[82] The DRD pre-dates the entry into force of the Treaty of Lisbon and thereby the legally binding character of the CFR. However, since the first proclamation of the Charter in 2000 – expressed by the signing of the document by the representatives of the three main (and legislative) bodies Commission, Parliament and Council – the EU bodies made an assessment of the validity of any proposed legislative act in view of the rights as laid down in the Charter and expressed this typically in the recitals or reasoning for proposing the legislative act. Whether this assessment is, however, correct, is ultimately to the Court to decide.

[83] DRD Judgement, para 29.

[84] DRD Judgement, para29.

[85] AG Opinion, para 60 et seq.

[86] The Court, para 52, uses this notion in its arguments, too, but not as the AG in order to explain a possible applicability of Article 11 CFR, but to underline the seriousness of the infringement with Articles 7 and 8 CFR (see below).

freedom of expression.[87] In that sense restrictions or potential sanctions not only could have a chilling effect on the use of the freedom, but also the fear of what might happen with data stored which allows the recognition of communication patterns. In the view of the AG, albeit this consequence might be very likely, such a limitation would only be a further "collateral consequence" of the interference with Article 7 CFR. For this reason and the lack of a sufficient basis at hand for the Court to support such a conclusion, the AG proposed to examine the DRD only on basis of the privacy and data protection provisions.[88]

It is noteworthy, however, that the AG at least indicated this further possible line of argument, as he refrained from doing so with other points raised by the referring court. Likewise, the CJEU in its ruling also briefly discusses Article 11 CFR, although it declares that an additional conclusion concerning Article 11 is unnecessary at the end of the very extensive analysis of Articles 7 and 8 CFR.[89] At the very beginning of the analysis the Court leaves no doubt that the sum of data retained is the problem in view of a potential impact on the behaviour of the service users whose data is retained. In the Court's view, the potential conclusion that can be drawn from the set of data is wide-spread and concerns habits of persons, their residence, their movements, their activities, their connection to other persons and the surroundings they go to. This "profiling" effect[90] can have a negative consequence in view of Article 11 CFR irrespective of the fact that the actual content of the communications is excluded from being stored.[91] Even though it turned out unnecessary due to the result concerning Articles 7 and 8 CFR, it needs to be remembered that a review of data retention measures in view of the freedom of expression would also be critical of the DRD.

2. Interference of the DRD with Articles 7 and 8 CFR

Focussing in the section on interference on Articles 7 and 8 CFR, the Court gives a brief but precise explanation of the interference including a qualification of the type of the interference.

a) Conditions for an infringement

Concerning Article 7 CFR, the Court points out that the general rule on processing of personal data in the electronic communications sector set by Directives 95/46/EC and 2002/58/EC is that these communications and traffic data are treated confidentially and that they are erased or at

---

[87] AG Opinion, para 52, in fn. 45 he expressly relates his argument to the chilling effects-doctrine in U.S. First Amendment law.

[88] AG Opinion, para 52.

[89] DRD Judgement, para 70.

[90] This effect, although in a different context, was also starting point for the Court to demand in its even more recent Google Spain Judgement (Case C-131/12 *Google Spain and Google v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*) that individuals have the possibility to request removal of links in search engines to information, if this – even though possibly truthful – information accumulation in the search engine result list is capable to draw a misleading "profile" of a person and there is a justified interest that this does not happen (possibly: any longer), cf. mainly paras. 93-94, 96-97. Although the decision was based mainly on an intensive analysis of the relevant provisions of the Data Protection Directive 95/46/EC the Court applies Articles 7 and 8 CFR as underlying standard when balancing the interests of the concerned individuals with other interests.

[91] DRD Judgement, para 27 et. seq.

least anonymised when no longer needed.[92] In this way, the DRD derogates from the right to privacy protecting system of these basic directives. The obligation of the providers to retain the data for a certain period and, under certain circumstances, make it accessible to competent national authorities already constitutes an interference pursuant to the relevant judgements of the ECtHR as discussed above.

The Court also underlines that the threshold of an infringement of these rights is rather low:

> "It does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way."[93]

Therefore when analysing the possible interference it is irrelevant whether or not individuals have been affected or whether they regard the retention of the data as "disturbing". Furthermore, any type of information that can be derived is sufficient to constitute an infringement, such infringements are not limited to any specific category of information or data.

Both, the storing of the data and the possibility of access by the competent authorities constitute separate infringements of Article 7 CFR. The Court draws this conclusion from the established case law of the ECtHR.[94]

The infringement of Article 8 CFR lays in the fact that the DRD required the processing of personal data, which is the scope of this data protection-specific right.[95] The Court does not discuss the differentiation and specific relationship between Articles 7 and 8 CFR in the way the AG does, but it does point out that the protection of personal data resulting from the explicit obligation laid down in Article 8 CFR is an especially important element for safeguarding the (more general) right to privacy as it is enshrined in Article 7 CFR.[96] Consequently, in the later discussion regarding the justification the Court combines the two provisions whilst the AG in his opinion puts a clear emphasis on Article 7 CFR which, in his view, encompasses a wider protection with relation to data processing. The AG opined that this needed to be analysed because the problem is primarily the original retention of the data irrespective of whether and how it is processed later.[97]

b) Seriousness of the infringement

With remarkable clarity, both the AG and Court make clear that the retention of data as foreseen by the DRD is not only an infringement in Articles 7 and 8 CFR, but that this infringement has a particularly significant weight and therefore needs to be classified as a "particularly serious" and "wide-ranging".[98] The AG spent some time in his opinion explaining

[92] DRD Judgement, para 32.
[93] DRD Judgement, para 33.
[94] DRD Judgement, para 35.
[95] DRD Judgement, para 36.
[96] DRD Judgement, para 53.
[97] DRD Judgement paras 36 and 39 et seq., 53 on the one hand; on the other hand AG Opinion, paras 58 et seq., 67.
[98] DRD Judgement, para 37, AG Opinion para 70 et seq.

this classification, whereas the Court agrees with the result in one paragraph and simply refers to parts of the section in which the AG elaborated on this position.

The seriousness of the infringement derives from the amount of the retained data. The data emanates largely from EU citizens' everyday electronic communications and due to the large amount of such data created daily, needs to be stored in "huge databases".[99] Although the potential use of the data by authorities takes place retroactively, the fact that this (wide-ranging) data is stored for long periods of time subjects every person to the constant feeling of threat that their personal and professional activities are under scrutiny, especially as the concerned persons are not informed in case of actual use of the data.[100]

Additionally, since the DRD applies to all means of electronic communications, the use of which is common and of growing importance in people's everyday lives, the adverse effects of the retention increase constantly with the growth and enlargement of electronic communications.[101]

Further, the AG suggested in his opinion a further argument for the seriousness of the interference. He applied the notion that the retained data have a "special" nature which in his view goes beyond usual personal data. Such personal data in the traditional sense relates to specific information concerning the identity of individuals such as e.g. in passports. The data stored in application of the DRD are not this type of data, but in the view of the AG are especially relevant, because their use makes it "possible to create a both faithful and exhaustive map of a large portion of a person's conduct strictly forming part of his private life, or even a complete and accurate picture of his private identity".[102] The Court itself is well aware of the "profiling" danger that exists in connection with the data under the DRD[103] but nonetheless rightly and only applies this when scrutinising the level of infringement which is necessary to be able to do a balancing test in the context of analysing possible justifications. On the contrary, introducing a category of "special" data is unnecessary and misleading, because the significance of the data mostly depends on the context in which it is used rather than the different categories of data. Distinguishing different forms of data beyond what is foreseen by the law – e.g. in Article 8 Directive 95/46/EC – always leads to the assumption that certain categories of data are "more important" than others. This distinction can prove to be dangerous, especially in the context of profiling measures, because the processing context makes the use of the data problematic, even if the data by itself seemingly may not have a very significant impact.

The seriousness of the infringement already stems from the amount and broadness of the data collected without the necessity of referring to a special weight that the data itself has.

---

[99] AG Opinion, para 72; the German version of the Opinion uses the even more drastic word "in gigantischen Datenbanken".

[100] DRD Judgement, para 37.

[101] AG Opinion, para 73.

[102] AG Opinion, para 74.

[103] see above discussion concerning Article 11, DRD Judgement, para 27 et seq.

Lastly, the AG argued that the lack of sufficient safeguards against abuse of the retained data contributes to the seriousness of the interference.[104] Although the Court is again in full agreement concerning this risk, it uses this argument in the context of the scrutiny of Article 8 CFR and declares that the lack of sufficient safeguards constitutes a further element of the violation of that provision (see below).

To sum, both AG and the Court express serious concerns with regard to quantity, quality and level of security of the retained data. Underlining that the DRD amounts to an especially high level of interference, the Court emphasises that any form of justification would have to meet highest standards due to the gravity of the infringement.

3. Justification of the Interference

Having established an interference with the rights enshrined in Article 7 and 8 CFR, the Court proceeds in its analysis to examine whether the interferences could be justified under Article 52(1) CFR.

Following this provision, limitations on the exercise of the rights and freedoms enshrined in the Charter must fulfil the strict conditions of being provided for by law and of respecting the essence of those rights and freedoms. Additionally they must comply with the principle of proportionality in the sense that any limitation must be strictly necessary and genuinely meet the objectives of general interest of the Union or the need to protect the rights and freedoms of others.[105] This follows the reasoning of the ECtHR in applying the standards of Article 8 ECHR (and the other Convention rights) which in the article's section 2 requires for justifications of measures by States that they are "in accordance with the law and […] necessary in a democratic society in the interests" listed therein. It does, however, additionally lay an emphasis on the respect for the essence of each of the rights contained in the Charter. The DRD was thus submitted by the Court to a three-fold test: whether the essence of the rights are respected, whether it meets the objective of general interest and foremost whether it respects the boundaries of proportionality, namely appropriateness and necessity. The Court focuses on the aspect of necessity and in doing so applies standards developed by the ECtHR.

The question of whether the interference is provided for by law is simply answered by referring to the DRD itself as legislative act of the European Union.[106] The AG reiterated the ECtHR's interpretation of the equivalent provision in the ECHR according to which "must go beyond a purely formal requirement" and also concern the "quality of the law". In that sense the AG established that the precision of the law requires that the limitation to the exercise of fundamental rights must be accompanied by the necessary degree of detail of the guarantees

[104] AG Opinion, para 75.

[105] Article 52(1) CFR.

[106] Since it is so obvious the Court does not expressly mention this but simply refers to the relevant provisions of the DRD directly (para 38 et seq.). The AG stated that the interference "must be regarded as being formally provided for by the law", because of the DRD and says himself it is "hardly worth pointing out", AG Opinion, para 108.

that must accompany such limitations.[107] In the case of DRD the AG criticized that neither access, nor use of the retained data was accompanied by sufficient safeguards, at least in the form of principles which "must govern the definition, establishment, application and review of observance of those guarantees".[108] As a consequence, the AG suggested that the DRD be declared incompatible with Article 52(1) already on the grounds of lack of prescription by (a sufficiently detailed) law.[109] The Court refers to these arguments of the AG at a later stage of the judgment in the context of the strict necessity test but again shares the AG's opinion in substance.

a) The criterion of "essence of the rights"

As previously shown, the analysis of the Court focused firstly on the question of whether the interference respected the essence of the right to privacy and the right to the protection of personal data, as enshrined in Articles 7 and 8 CFR. This absolute limitation for interferences that Article 52(1) CFR establishes has the aim of avoiding the complete erosion of a fundamental right by reserving a certain space against any form of interference. The essence of the rights covers only a limited scope as any form of proportionality and balancing test is not possible at all in that area. Therefore, the application of this criterion is limited to extreme cases of severe infringements and it does not come as a surprise that the Court rejects an infringement of the essence of both rights. Concerning Article 7 CFR it did so, because the DRD does not foresee any storage of or access to the content of the communications.[110] Concerning Article 8 CFR the Court argues that the prescription of at least some principles concerning the protection and security by technical and organizational measures of the data collected would have been sufficient to respect the essence.[111]

Irrespective of the fact that in result the Court did not find a violation of the essence of the rights it is very critical because of the large infringement. As far as Article 7 CFR is concerned, the Court recognizes the danger that although the actual content is not retained, the sum of data collected allows authorities to draw similarly clear conclusions by observing the pattern of behaviour of individuals.[112] Certainly, the data allows interpretation that could result in conclusions about the private lives of individuals as if the actual communication content would have been known. As far as Article 8 CFR is concerned, as will be further detailed below, the Court concludes in the last step of the compatibility test that the rules relating to the security and protection of the retained data as provided for by the DRD are not sufficient "to ensure effective protection against the risk of abuse, unlawful access and use".[113] This means even as provisions are in place they are nonetheless insufficient for safeguarding the standards which Article 8 CFR requires.

---

[107] AG Opinion, para 111.
[108] AG Opinion, para 120.
[109] AG Opinion, para 131.
[110] DRD Judgement, para 39.
[111] DRD Judgement, para 40.
[112] DRD Judgement, para 26.
[113] DRD Judgement, para 66.

Although in principle the retention of data "per se" is not a violation of the essence of the two mainly concerned rights, with these observations by the Court it is questionable how much space – taking the proportionality test into consideration – is left for any legitimate retention of data, especially if it happens for a comparable objective (which will be discussed below) such as LE purposes.

b) Objective of general interest

In order to be potentially justified, the measure infringing fundamental rights must satisfy an objective of general interest. According to Article 1(1) the DRD "aims *to harmonise* Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the *investigation, detection and prosecution of serious crime*, as defined by each Member State in its national law".[114]

These two objectives – one of a more general nature which aims to safeguard the harmonization of rules improving the functioning of the internal market, the other being more specific and ensuring the availability of data in the fight against serious crime – are closely linked to each other. The ultimate goal is the combating of serious crime for which purpose the Member States rules are harmonized. In this sense the AG identified in his opinion a "functional duality" of the DRD. On the one hand, there is the unquestioned harmonization purpose, which he saw as the "primary objective".[115] On the other hand he pointed to what he called a "creating effect" by the DRD. He underlined that it is the DRD itself that actually "seeks to establish, where appropriate, obligations – in particular data retention obligations"[116] and thereby introduce them to those Member States that until then did not have any provisions that could have been harmonized. Thus he demanded that the analysis of the DRD must take into account this "second function"[117], because it creates provisions that are critical in view of their fundamental rights impact and should have been considered much more carefully. The Court also focuses on this second aspect, the "material object" of the DRD as it calls it. The DRD contributes "to the fight against serious crime and thus, ultimately, to public security", which the Court also sees reflected in the quoted conclusions of the Justice and Home Affairs Council of 2002 that underlined the particular importance of the data relating to the use of electronic communications and their value in the prevention of offences and the fight against organized crime.[118]

More importantly, however, a legitimate objective attained is not sufficient, the actual proportionality of the measure in view of this objective is what is needed.

---

[114] Emphasis added.

[115] AG Opinion, para 38.

[116] AG Opinion, para 46.

[117] AG Opinion, para 47.

[118] DRD Judgement, para 43.

c) Proportionality in view of the objective

In order to verify whether the "serious interference" with Articles 7 and 8 CFR can be justified under Article 52(1) CFR, the Court of Justice refers to the general proportionality test developed in its case law as mentioned above. The Court refers to the relevant ECtHR case law – analysed here under C. II. – and the general principles developed therein. By emphasising the importance of the right to data protection, the Court recalls that – due to the significant nature of this right and the seriousness of the interference – the margin of discretion for the EU legislator which is only subject to a limited review by the Court, is significantly reduced.[119] Especially in accordance with the ECtHR's *S. and Marper v. United Kingdom* decision the Court applies a strict scrutiny standard concerning the compatibility of the DRD with Articles 7 and 8 CFR.[120] The reference to the ECtHR case law in this context could prove to be of special importance, because the confirmation of the special meaning of the right to data protection and the risks of data retention can be interpreted in a broader sense. In this sense these principles would globally apply in the context of data retention measures in a LE environment.

aa) The criterion of appropriateness

Against the background of the increasing use of electronic communications, the Court very briefly deals with the appropriateness of the DRD for use in criminal investigations. It considers that the retention of communications data as such can indeed be appropriate to obtain this aim of the DRD to contribute to more successful investigations.[121]

Although there are means to circumvent the retention of communications data, this alone does not amount to making the DRD inappropriate. The Court in that context rejects the argument of some of the opponents of data retention schemes that argue because persons with criminal intentions have alternative means of achieving their goal of unmonitored communication, for example by using methods of anonymous communication such as pre-paid SIM cards or free wireless networks, the whole scheme is worthless. Even if the objective pursued by the Directive is limited by such factors and the goal may not be achieved to the same extent as it would be with a measure that gives no alternative for persons trying to avoid the retention of their data, this does not lead to this lesser efficient measure being inappropriate.[122]

bb) The criterion of necessity

After having established the general appropriateness of the DRD, the Court dedicates a considerable part of its judgement to the analysis of the necessity of the measure. Even though, as the Court declared initially (see above), the essence of the rights deriving from Articles 7 and 8 CFR have been respected, the measure at stake can still be found disproportionate. Although the general interest of fighting serious forms of crime may be of "utmost importance", this

[119] DRD Judgement, paras 47 and 48.

[120] DRD Judgement, para 47 and 48.

[121] DRD Judgement, para 49. The Court does not separately investigate the appropriateness to attain the harmonisation of rules for improving the functioning of the internal market as does the AG, Opinion para. 98 et seq.

[122] DRD Jugement, para 50; also AG Opinion, para. 137.

objective "does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight".[123] Even with such an objective of general interest, any interference with or limitation of the right to private life are only permitted in the case of *strict* necessity. As far as data are concerned, the Court regards the safeguards required for by Article 8 (1) CFR as establishing a close link to Article 7 CFR whereby the existence of provisions securing Article 8 CFR is a necessary (but not sufficient) prerequisite for the proportionality test under Article 7 CFR. In order to satisfy this requirement, the limitations to these rights always need to be accompanied by effective safeguards against abuse, unlawful access and use of the retained data. Legislation restricting Articles 7 and 8 CFR must lay down clear and precise rules regarding the scope and application of the limitations.[124] By referring to the ECtHR cases *S. and Marper v. UK* and *M.K. v. France*, the Court insists that these limitations are even more important in view of the automatic processing of data that is taking place in LE environments nowadays.[125]

A further point that at first glance the provisions seem problematic in light of the strict necessity-criterion is mentioned next by the Court. The indefinite scope of application of the DRD is often in the focus of criticism. Because the DRD requires the retention of all traffic data concerning all means of electronic communications which are commonly used today in people's everyday lives, it "therefore entails an interference with the fundamental rights of practically the entire European population".[126] The generalising and indiscriminate manner in which the DRD applies to the entire EU population builds the basis for the following findings of the Court. The wording used by the CJEU is similar to the wording of the ECtHR in the above mentioned case law.[127] Although the Court does not directly draw the parallel in this paragraph of the judgement, it uses very similar terms as the ECtHR in the *S. and Marper v. UK* case, in which e.g. the ECtHR was struck by the blanket and indiscriminate nature of the interference.[128]

The Court then divides its analysis into three main points to underpin the non-compliance of the DRD with the necessity requirement.

(1) Scope of retention obligation

Firstly, it criticizes that "all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime" are concerned.[129] Thus, the Court clearly opposes the general indiscriminate mass collection of data. This point was already mentioned in strong

[123] DRD Judgement, para 51.
[124] DRD Judgement, para 54.
[125] DRD Judgement, para 55.
[126] DRD Judgement, para 56.
[127] ECtHR, S. and Marper and M.K. v. France.
[128] ECtHR, S. and Marper, para 119.
[129] DRD Judgement, para 57.

words by the AG, who sees in the accumulation of data, concerning "actual and particular persons" an "anomaly" and concluded that such retention requirements "should never exist".[130]

Another very important element of this criticism involves the retention of data of unsuspicious persons for LE purposes. According to the Court, applying the storage requirement to data of persons with absolutely no link to serious crimes cannot be regarded as "necessary" in terms of Articles 7 and 8 CFR:

> "Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions."[131]

As there are no exceptions included in the DRD, for instance for persons that are subject to professional secrecy and therefore specially protected by law, the blanket retention – the German Constitutional Court uses the very appropriate expression of "anlasslos"[132], which could be translated as "without cause" or "without occasion" or "without specific reason"[133] – cannot fulfil the requirements of the CFR.

The Court further requires a link between the data retained and the use for LE purposes. Retaining data in absence of "any relationship between the data whose retention is provided for and a threat to public security" is not in line with the guarantees of the CFR. This link is of utmost importance not only with regard to the DRD, but also for any other data retention scheme that involves the storage of data of unsuspicious persons.

Other limitations of the retention such as restrictions "in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences" are equally not provided for in the DRD and result in harsh criticism from the Court.[134] This can also be interpreted as meaning that any "anlasslose" data retention measure is impossible as these by definition lack a specific link or connection to the crimes concerned.

(2) Lack of Limits

The second argument was focused around the purpose limitation principle as the DRD neither contains limits itself nor provides for objective criteria to determine the limits of access of national authorities to the retained data or their subsequent use.[135] A general reference to "serious crimes" is considered insufficient by the Court as this is not at all defined in EU Law but

---

[130] AG Opinion, para 144.

[131] DRD Judgement, para 58.

[132] Bundesverfassungsgericht (German Federal Constitutional Court), joint cases 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, first maxim.

[133] The German Federal Constitutional Court uses the term "without occassion, by way of precaution" in the English press release (available at: http://www.bverfg.de/pressemitteilungen/bvg10-011en.html).

[134] DRD Judgement, para 59.

[135] DRD Judgement, para 60.

left to the Member States. Along these lines, the Court also criticizes the lack of substantive or procedural conditions concerning who, to what extent and under which circumstances can access and use the retained data. Leaving this decision to the Member States without laying down any conditions risks an unacceptably extensive access regime. The Court suggest for example that there should have been rules concerning that the use of data would be made dependent on a prior review by a court or at least independent administrative body.[136]

(3) Lack of precision concerning retention period

Several aspects concerning the retention period are subject to criticism by the Court. On the one hand the Court considers that the 6 to 24 month period of obligation for retention does not provide any form of differentiation, e.g. by establishing different categories of data and their value for achieving the purpose and the consequence this has for the length of retention. The provisions do not require Member States to include this differentiation in their transposition either. Also, the determination of the time period according to the DRD needs not be based on objective criteria so as to be limited to what is strictly necessary[137]. The AG considered the provision of a retention period ranging from at least 6 months up to 24 months to give data retention a "dimension of temporal continuity" which confirmed the seriousness of such interference.[138] In his view, the retention period would have at least needed to be limited to a period of less than a year.[139] The Court gives no indications whatsoever, but instead clearly states that any such form of undifferentiated and insufficiently precise time aspect cannot pass the necessity test.

With a different emphasis on which of the elements is lacking, both Court and AG in a remarkably direct and unequivocal manner, conclude that the DRD established a wide-ranging and particularly serious interference with the fundamental rights deriving from Article 7 and 8 CFR which could not be justified under the necessity test.

cc) The additional criterion of "sufficient safeguards to ensure effective protection"

In the analysis of possible justifications of the DRD the Court adds a further criterion beyond the proportionality test. Irrespective of the fact that the Court declares void the DRD already due to the failure of the necessity test, it points out that additionally the DRD would also have failed due to the lack of safety precautions – the already above mentioned "sufficient safeguards". These safeguards according to the Court's reasoning are required by Article 8 CFR which protects generally data of persons and concerns, in section 2, the processing of that data. Consequently, any legislation providing for data retention must not only be limited to what is strictly necessary but also has to establish rules guaranteeing effective protection of the data.[140] These rules are of a more formal, procedural nature and concern technical and enforceability

[136] DRD Judgement, para 62.

[137] DRD Judgement, paras 63, 64.

[138] AG Opinion, para142.

[139] AG Opinion, para 149.

[140] See also Guild/Carrera, p. 8, who qualify the data protection requirements as a "second set of criteria" that are necessary to pass the test.

aspects. The rules foreseen by the DRD are in view of the Court certainly not nearly enough to meet these standards, as they do not protect "against the risk of abuse and against any unlawful access and use of that data."[141]

(1) Technical aspect

Concerning the technical aspect, the Court holds Article 7 DRD to be insufficient as the rules foreseen relate in no way to the specifics of the data collection and storing introduced by the DRD:

> "Article 7 of Directive 2006/24 does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data […] Furthermore, a specific obligation on Member States to establish such rules has also not been laid down."[142]

This list makes it clear that the Court expects an especially high level of protection and safety measures against abuse because of the amount and significance of the data. In order to satisfy the requirement the provision would have had to take this specificity into consideration and in a very clear manner without the possibility of diluting the obligations lay the rules down. The Court expects rules that for the retained data "ensure the[ir] full integrity and confidentiality".[143] The Court uses technical terms, such as integrity and confidentiality, thereby suggesting that also the access to the retention systems itself needs to be particularly protected. Whether such protection can result in a right for individuals to "IT-security" that was developed by the German Constitutionals Court in 2008[144], is not clear from the use of these formulations but may be subject to future developments in EU law either on legislative level or a judgement of the CJEU. Not only does the DRD not foresee these IT-security rules itself, it refrains from obliging the Member States to introduce rules suffice to the requirement. This also is a clear answer to the AG's line of argument in his opinion supporting the temporary upholding of the DRD until a rectified version of the DRD is decided upon, because the Member States in most cases introduced rules which he saw as being more adequate to protect the data.[145] Much to the contrary, the Court clarifies that the safeguarding rules must be directly linked with the provisions requesting the collecting, storing and processing of data.

(2) The delegation of the retention to private parties

The Court goes further by criticizing that the DRD does not ensure the implementation of a "particularly high level of protection"[146] by the providers of the communications services. Instead, providers are actually expressly allowed to take into account economic considerations when determining the level of security they implement through technical and organisational

[141] DRD Judgement, para 66.

[142] DRD Judgement, para 66.

[143] DRD Judgement, para 66.

[144] Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, compare BVerfG, 1 BvR 370/07 of 2 February 2008.

[145] AG Opinion, paras 117, 132, 157 et seq.

[146] DRD Judgement, para 67.

measures.[147] This evidently is more likely to water down safety requirements than keep them at a very high level. A final failure of the DRD to comply with the minimum technical standards is seen by the Court in the fact that the ultimate removal of the data is not specifically guaranteed. The lack of a provision ensuring the irreversible destruction of the data at the end of the retention period is equal to a lack of security measures concerning the data.[148]

(3) The problem of the location of the data

Concerning the enforceability the Court criticizes the lack of rules concerning the location at which the retention of the data takes place:

> "[…] it should be added that that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8 (3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured".[149]

The Court reminds that Article 8 (3) CFR requires the possibility of supervision by an independent authority. According to the Court, this supervision is a crucial part of data protection as it helps enforcing the data protection rights. Supervision ensuring the compliance with the rules governing the integrity and confidentiality of the stored data can only be carried out on the basis of EU law. Therefore, in order to – as the Court puts it[150] – *fully* ensure the efficiency of control by the independent authority, the supervision has to take place within the territory of the EU, which in turn suggests that the servers containing the stored data have to be located within the EU and that there are at least provisions governing data location. Consequently, the storage of data outside the EU which would have been possible by the standards of the DRD does not meet the requirements of Article 8 CFR.[151] Although this last conclusion by the Court would strictly speaking not have been necessary, as the DRD was already regarded as being clearly in violation of the necessity standard, the fact that it points out the importance of data security and data protection rules shows that an additional limitation for any type of data retention schemes than merely the proportionality standard in a narrower sense exists and needs to be met.[152]

---

[147] DRD Judgement, para 67.

[148] DRD Judgement, para 67.

[149] DRD Judgement, para 68.

[150] Emphasis added.

[151] Cf. similarly AG Opinion, paras 78 et seq., but there in the context of the interference test.

[152] Cf. also Roßnagel, MMR 2014, 372, 375 who identifies this as the introduction of a "new requirement".

D. Impact of the Judgement on existing Data Retention Regimes in the Member States

The immediate result of the Judgement of the CJEU on the Data Retention Directive was the invalidity of the Directive. As a consequence there is no longer a specific legal act on the EU level that obliges Member States to introduce or maintain data retention regimes. It is noteworthy that the CJEU declared the Directive in its entirety to be in contradiction with fundamental rights. This is different from earlier cases in which a violation of fundamental rights was stated but the consequence was the invalidity of only specific parts of that legislative act and not the whole measure.[153] Furthermore, the Court did not leave room for a temporary continued application of this piece of legislation but instead with no interim period declared it invalid with immediate effect.[154]

As an immediate consequence, the European Commission announced to end proceedings against Member States that were in violation of EU law by not having transposed the Directive within the given time limits; most importantly this concerned Germany, whose Federal Constitutional Court had struck down the national act amending the telecommunications law and therefore was without an implementing measure since 2010, even as the transposition period had already ended a year before.[155]

Unsurprisingly, the strong and clear wording of the judgement has led several Member States to consider whether under the circumstances national retention schemes for electronic communications data – especially if they were introduced as implementing measure and followed the Directive extensively – should not be re-assessed.[156] Also, the first reaction by a national Court was swift: the Slovak Constitutional Court in a case pending since October 2012, decided to review the respective national law and for the time being suspend the applicability of the relevant provisions of the Slovak implementing law.[157] For the purpose of this study it is

---

[153] Cf. e.g. CJEU Case C-236/09 *Association belge des Consommateurs Test-Achats ASBL et al. v Conseil des ministres (...)* (*Test-Achats v Conseil des ministres*), para. 35 (in that case a specific paragraph of one article of a Directive was declared void).

[154] Cf. DRD judgment para. 34.

[155] CJEU Case C-329/12 *Commission v Germany*; the Commission – according to an order by the President of the Court of 5 June 2014 - has withdrawn its action except for the costs, cf. Wilkens, Vorratsdatenspeicherung: EU-Kommission zieht Klage gegen Deutschland zurück, News item, Heise, at 07.05.2014 10:02, http://www.heise.de/newsticker/meldung/Vorratsdatenspeicherung-EU-Kommission-zieht-Klage-gegen-Deutschland-zurueck-2184019.html; Sweden is also concerned, but the infringement proceedings of the Commission had already ended with a negative outcome for Sweden (Case C-270/11 *Commission v Sweden*, decision on a lump sum payment of 3 Mio. Euro by Sweden) before the DRD judgment was handed down, however, in the EP plenary session of 16 April 2014 Commissioner Malmström confirmed that as a consequence of the Court's DRD Judgement Sweden would be paid back the fine, cf. www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20140416+ITEM-017+DOC+XML+V0//EN&language=EN.

[156] Cf. e.g. the comment by the Luxembourgish Justice Minister on the day of the judgment announcing that a detailed analysis of possible consequences for the national law will be undertaken, Communiqué, Ministère de la Justice, 8 April 2014, http://www.gouvernement.lu/3641093/08-cjue.

[157] Cf. press information by European Information Society Institute (EISI), a Slovak organisation that initiated the proceedings before the Constitutional Court together with a number of Members of Parliament,

relevant, whether or not the DRD judgment of the Court also has an indirect effect on the existing national implementation measures even if a Member State chooses not to react to the judgment on its own initiative.

I. Member States Law and EU Fundamental Rights

1. General Relevance of EU Fundamental Rights

As has been shown there is a multitude of ways that fundamental rights are valid and take effect in EU law. Already when fundamental rights were "only" protected as general principles due to the development by the (then) European Court of Justice, but also since they are part of the binding Charter of Fundamental Rights of the European Union, they have been valid on the same level of primary law (equal to the Treaties). Therefore, all secondary law and actions of the EU's bodies must be in compliance with these rights. Beyond that the Court has always also considered that Member States' actions (including legislation) are also under the scrutiny of the EU fundamental rights standard – at least as long as their action takes place within the area of application of EU law.[158] The exact extent of this approach will be shown below, but this amounts to an effect of judgments of the Court also, albeit indirectly, with effect for national legislation and application. Irrespective, there exists the path to Strasbourg for individuals claiming that a State which ratified the ECHR has violated Convention rights by its actions (including legislation). The close link between the Courts in Strasbourg and Luxembourg is not one-directional in the sense that case law of the ECtHR influences the CJEU. The ECtHR reviews national laws and this includes legislation passed in fulfilling the transposition obligation deriving from EU law. In that way a national measure which originally transposed the DRD could be the subject of a case before the ECtHR and it is not likely that the ECtHR would conclude differently concerning the interference with fundamental rights by the DRD than the CJEU did (and in doing so followed the previous ECtHR case law as demonstrated above).

It is necessary to remember that the Court had already established an extensive body of fundamental rights jurisprudence and a differentiated system of protection both in view of EU law and Member State actions, even before a binding catalogue of fundamental rights existed. However, the entry into force of the Charter of Fundamental Rights of the European Union as law on the same level as the Treaties and the clear and manifold references to fundamental rights including the demand for accession of the EU to the ECHR in the new Article 6 TEU seemingly have given the Court a new impetus for a more elaborated fundamental rights protective approach.

Concerning the validity of EU (secondary) law in light of the CFR, it did not take long before a Directive was corrected for reasons of violation CFR provisions: in 2011 the Court declared

---

http://www.eisionline.org/index.php/projekty-m/ochrana-sukromia/75-ussr-pozastavil-sledovanie with a link to the Press Release of the Constitutional Court (only in Slovakian).

[158] Cf. for an early example CJEU Case C-260/89 *ERT v. DRP*, para 42 et seq.

invalid one provision of an EU Directive in *Test-Achats v Conseil des ministres*[159] because it violated Articles 21 and 23 of the Charter. More important in this context is the impact of the CFR on the laws and actions of the Member States which will be discussed in the following.

2. Effects of EU Fundamental Rights

a) Scope of Application of the Charter of Fundamental Rights

The CJEU has defined the scope of application of Article 51(1) of the Charter in a line of case law. Article 51 itself states in its first paragraph that the provisions of the Charter are primarily "addressed to the institutions and bodies of the Union" and to the Member States "only when they are implementing Union law". Article 51(2) explicitly provides that the scope of competence of the EU is not extended beyond the situation as defined in the Treaties.

In *DEB v Germany*[160], the plaintiffs sought legal aid under the German Code of Civil Procedure to bring an action against Germany for failure to transpose a European Directive into national law. They relied on Article 47 of the EU Charter, the Court stressed that Member States are bound by the Charter when implementing EU law.[161] The Court came to the conclusion that, in application of the Charter, legal persons must be able to be relieved from advance payment of the cost of legal proceedings under the right to access to justice under Article 47 of the Charter.[162]

Asked about the precise scope of Article 51(1) of the Charter, the Court in *Pringle v Ireland*[163] ruled that the provisions of the Charter are addressed to the Member States only when implementing EU law and Article 51(2) limits the scope of the Charter to those areas within the competence of the EU.[164] In that case the Member States were not implementing EU law when concluding an international Treaty that fell outside the competence of the EU and therefore outside the scope of the Charter.[165] But it already became evident that the Court would only accept that a Member State measure is completely outside the scope of the Treaties to a limited extent.

Finally, in two judgements that were rendered on the same day in February 2013, the Court confirmed the wide scope of application of the Charter by giving a broad interpretation of the scope provision. In *Åkerberg Fransson* it stressed that the fundamental rights guaranteed under the EU legal order apply "in all situations governed by European Union law"[166] and that "applicability of European Union law entails applicability of the fundamental rights guaranteed by the Charter."[167] This wording is clearly distinguished against the narrower phrase

---

[159] CJEU, Case C-236/09 *Test-Achats v Conseil des ministres*.

[160] CJEU, Case C-270/09 *DEB Deutsch Energiehandels- und Beratungsgesellschaft mbH v Bundesrepublik Deutschland (...)* (*DEB v Germany*).

[161] CJEU, Case C-270/09 *DEB v Germany*, para 30.

[162] CJEU, Case C-270/09 *DEB v Germany*, para 59.

[163] CJEU, Case C-370/12 *Thomas Pringle v Government of Ireland, Ireland, The Attorney General (...) (Pringle v. Irleland)*

[164] CJEU, Case C-370/12 *Pringle v. Irleland*, para 179.

[165] CJEU, Case C-370/12 *Pringle v. Irleland*, para 180.

[166] CJEU, Case 617/10 *Åklagaren v Hans Åkerberg Fransson (Åkerberg*), para 19.

[167] CJEU, Case 617/10 *Åkerberg*, para 21.

"implementation" as contained in Article 51(1) CFR. The Court further qualified that in matters that are governed only partially by EU law, Member States may apply national standards of protection as long as the protection provided under the Charter is not compromised.[168] In *Melloni,* the Court added that Member States are prevented – in order to guarantee the primacy and effectiveness of EU law – to apply fundamental rights protected by their national constitutions, if this application would have the consequence of not applying EU law provisions, in particular the CFR.[169]

The cases read together give the Charter a very wide scope of application covering all cases that are within the competence and therefore application of EU law. The institutions of the EU are always bound by the Charter while Member States are bound only when they apply EU law. In the latter case, however, the obligation to give effect to the Charter goes to the extent that even constitutional fundamental rights guarantees which go beyond the protection offered under the Charter, cannot be applied if they would hinder the proper application of EU law, as *Melloni* clarified. In an even more recent case, which has not yet been decided by the Court, Advocate General Cruz Villalón in evaluating the parody-exception in intellectual property law, made some further observations concerning the validity of fundamental rights of the Charter. Even though it is not clear whether the Court will refer to this section of the Opinion in its decision, it is worth mentioning that in his view it is evident from the very beginning that fundamental rights in the European Union, as they were linked to the general principles, also have an "objective" dimension as an overarching value in the legal order. In that way, beyond being purely "subjective" instruments of defence against intrusion by the State, they form the relationship between private parties as far as EU law governs them.[170]

b) The significance in the context of fundamental freedoms

Apart from the general validity of Charter rights in the application of EU law by Member States, there is a specific field in which fundamental rights play a significant role. This may well be the most important case for application of fundamental rights so far, namely when fundamental freedoms are relevant in a situation of Member States action. Since the cases of *Schmidberger*, *Familiapress*, *Dynamic Medien* and others[171], the Court has clarified that limitations to fundamental freedoms can be justified by referring to the necessity of protecting fundamental rights.

In other words, a Member State may take an action that limits a fundamental freedom, because it sees the necessity of protecting the fundamental rights. This can be illustrated by the case of *Schmidberger*, in which the blocking of a motorway by a demonstration meant an infringement of the free movement of goods but was justified by respecting the right to demonstrate. The Court also pointed out that in situations in which the infringement of the fundamental freedom additionally

---

[168] CJEU, Case 617/10 *Åkerberg*, para 29.

[169] CJEU, Case C-399/11 *Stefano Melloni v Ministeria Fiscal (Melloni)*, para 58 et seq.

[170] AG Opinion on Case C-201/13 *Johan Deckmyn et al. v. Helena Vandersteen et al. (Deckmyn)*, paras 76 et seq., esp. fn. 29.

[171] CJEU, Case C-368/95 *Vereinigte Familiapress Zeitungsverlags- und vertriebs GmbH v Heinrich Bauer Verlag*, para. 18; Case C-112/00 *Eugen Schmidberger, Internationale Transporte und Planzüge v Republik Österreich*, para. 74; Case C-244/06 *Dynamic Medien Vertriebs GmbH v Avides Media AG*, para. 42; Case C-36/02 *Omega Spielhallen- und Automatenaufstellungs-GmbH v Oberbürgermeisterin der Bundesstadt Bonn*, para. 35.

means an interference with fundamental rights, a limitation based on the fundamental rights of the other parties concerned may not be sufficient. Again to illustrate, in the case of *Familiapress,* a journal could not be exported from one Member State to another and the national law prohibiting this was based on the need to uphold media pluralism which is covered by Article 10 ECHR and the case law that the CJEU follows. On the other hand, with this measure not only the fundamental freedom of the publisher was concerned but also his fundamental right to freely express and disseminate his opinion (again covered by Article 10 ECHR). Given this conflict, the Court demanded the national courts to reconsider the balancing of interests.[172] All of these cases were developed based on the notion of fundamental rights as general principles of EU law.

Only in a very recent case, *Pfleger* which was decided in April 2014, did the Court have the opportunity to confirm that this same approach also continues to apply under the Charter. Therefore, national measures which impede a fundamental freedom (i.e. in the case at hand the freedom to provide services) must be interpreted in line with the general principles of EU law including fundamental rights enshrined in the Charter.[173] Member States are thus allowed to justify derogations from the fundamental freedom by reference to fundamental rights as they are now protected by the Charter. Importantly, the use of such fundamental rights as a justification is to be regarded as "implementing Union law" within the meaning of Article 51 (1) CFR.[174] As a result, any restriction of fundamental freedoms based on the argument of protecting (national) fundamental rights, must itself comply with fundamental rights laid down in the Charter.

As has been explained previously, the legal basis for the DRD was the harmonisation provision. Differing rules on data retention in the Member States (and the lack of them in many) were the reason for proposing the Directive in the first place.[175] Indeed, such differing rules are a potential hindrance of the free movement of services as they increase difficulties for service providers (telecommunications service providers, ISPs) to apply the same service and billing procedures in several Member States. Therefore, data retention schemes are within the field of application of one of the fundamental freedoms of the TFEU, Article 56. In that case, the limitation to a fundamental freedom or the enabling of such a freedom by creating new (harmonized) provisions by the EU needs to respect fundamental rights as part of primary EU law. Member States' rules that continue to exist after the judgement of the Court therefore need to be measured as potential infringements of the freedom to provide services and that is why they must respect the fundamental rights concerned. With the decision of the Court the exact criteria for determining when the measure is incompatible with fundamental rights standards, have now been set.

3. The specific case of Data Protection

As has been shown above, any infringement of fundamental freedoms under EU law must satisfy the fundamental rights test in order to survive scrutiny. However, beyond this general rule, there is a specific reference to fundamental rights standards in the EU rules on data protection which require this adherence by the Member States in the case of data retention

[172] Cf. paras. 29-31 ; generally also Fink/Cole/Keber, para. 49 et seq.

[173] CJEU, Case C-390/12 *Robert Pfleger and Others (Pfleger)*, para. 35.

[174] CJEU, Case C-390/12 *Pfleger*, para. 36.

[175] Cf. recital 6.

schemes. This more specific link between Member States' action in the field and EU fundamental rights plays an important role in the aftermath to the invalidity of the DRD.

a) General Framework in Directive 95/46/EC

Initially, the Data Protection Directive of 1995 set the general rule that processing of data must occur only under certain circumstances (cf. mainly Article 6), but it further included an exception provision in Article 13 (1). According to this rule in Directive 95/46/EC, Member States were entitled to pass laws that restrict the rights and obligations foreseen especially in Article 6 under the conditions that the measures were necessary to safeguard certain interests such as defence and public security. When the sector-specific data protection Directive for the electronic communications field was passed, this included a specific exemption-provision, as well. According to Article 15 (1) Directive 2002/58/EC there are exceptions – and they are actually meant to be only exceptions – to the general rule that data can only be stored and kept for a limited time and purpose. The list of objectives that allow for derogations from the general principle of restricted and limited collection entails the combating of crimes, national security or defence and public security. Although there is this sector-specific rule in Directive 2002/58, it is still possible to invoke Article 13 Directive 95/46 in the context of rules concerning e.g. Internet services that do not fall under the definition of electronic communications service providers.

b) The role of Article 15 (1) of Directive 2002/58/EC

Article 15 (1) Directive 2002/58/EC is remarkable in several ways. Although it repeats the approach taken in Article 13 Directive 95/46/EC (and expressly refers to it), the EU legislature saw the need to highlight some points more clearly than in the general data protection framework. Again, exceptions are introduced to the restrictions on data processing under Article 6 of Directive 2002/58/EC (obligation to erase stored traffic data after it is no longer used for technical reasons of the communication or billing purposes or if it is not covered by prior consent), but also to the confidentiality of communications (Article 5), the calling line identification (Article 8) and location data (Article 9). However, this time not only a vague mention of a necessity criterion, but instead a very detailed fundamental rights compatibility standard was included that explicitly resounds the formulations of the ECHR: "when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security …" (Article 15 (1)). Already with this, not only Article 8 ECHR but also the accompanying case law of the ECtHR have their place in the examination of such exceptional measures of the Member States. The exception provision goes even further by additionally mentioning that all such measures "shall be in accordance with the general principles of Community law, including those referred to in Article 6 (1) and (2) of the Treaty on European Union". Not only ECHR standards but the approach of the CJEU before entry into force of the Charter as binding law, is therefore taken into account.

This high standard is reflected in the relevant recital 11, which starts out with the Member States competence to act with exceptional measures but also then underlines even more extensively the fundamental rights limitations to this. In addition to the points referred to in the

substantive provision of Article 15, the recital calls for necessity and accordance "with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights". This is regarded as meaning that the measures must be "appropriate, *strictly* proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards"[176]. The "strict proportionality" test serves as a reminder that these measures are only exceptionally allowed and because of the dangers connected with them need to be accompanied by guarantees for the concerned individuals. Because Article 15 (1) expressly mentions, as one possible measure to be taken by Member States, the introduction of data retention schemes that allow storage of data for a limited period in case of one of the legitimate aims necessitating such storage, it is this provision that establishes the measure for the scrutiny test which is to be applied to such State action. In absence of the DRD it is again the place to find the measure for national legislative acts.

Therefore, when the DRD was passed, Article 15 (1) Directive 2002/58 was supplemented with a provision (1a) that qualifies the Member States acts transposing the DRD as being exempt from the normal exception rule of paragraph 1.[177] The reason for this amendment was to underline that from the perspective of EU law the proportionality test had already taken place and the requirement to store that data (as required by the DRD) was so to speak "automatically" covered by the exemption rule. This expectation of compatibility has been completely disapproved by the DRD judgement. In addition, the newly inserted Article 15 (1a) left untouched other Member States data retention rules that were not linked to the DRD specific data and had been introduced in line with Directive 2002/58/EU, whilst avoiding the creation of Member States rules in the scope of application of DRD which go beyond what is required according to that harmonizing Directive.

With the Court's DRD judgement, the newly inserted provision in Article 15 of Directive 2002/58 is void as well. As a result, now again only Article 15 (1) Directive 2002/58 is applicable for data retention schemes. This provision – as demonstrated above – clearly states that any State measure providing for data retention must be in accordance with EU law, above all its general principles encompassing fundamental rights. This is evident anyway, because the retention possibility given to the Member States as such is already a derogation from a principle set by EU (secondary) law. Today, adherence to fundamental rights implies the applicability of the CFR and its interpretation and application by the CJEU. In other words, any national measure that would now come under scrutiny would be tested by the Court in the framework of Article 15 (1) Directive 2002/58. Because of the parallelism of the provisions in the now void DRD and Directive 2002/58, according to which the principle is the prohibition of retention and the exception is the limited allowance in view of legitimate aims, the DRD judgement will guide the CJEU in a possible review of Member States retention rules, irrespective of whether these were

[176] Emphasis added.

[177] This makes perfectly sense as Article 3 of the DRD explained that the core of the Directive is a derogation from the principal rules of Directive 2002/58.

initially introduced under Directive 2002/58 or later as transposition of DRD. Another argument suggesting a review of national measures will likely lead to the same result, is that the CJEU requested that the legislature foresee adequate safeguards in any legal acts setting an exception to the rule in order to avoid a misbalance. The provision in Article 2002/58 merely allows Member States to act and gives no specific details on the kind of safeguards that would ensure the compatibility with fundamental rights. Therefore, any measure that in its design is similar to DRD is also in violation of EU law under Directive 2002/58.

II. Judicial and Other Means for Reviewing National Measures

The DRD Judgement of the CJEU has finalized the fate of the Directive by declaring it void *ex tunc*. All but one Member State have created national laws implementing this Directive in response to the transposition obligation in EU law. This original obligation to introduce data retention regimes in line with the DRD has vanished, but the Member State measures are still in place in the form of national laws that concern an area which, from a competency perspective, can be dealt with by the EU but is also open to Member State action. Therefore, the question now arises what consequences the DRD judgement has for the national legislation implementing the DRD.

1. General impact of the DRD Judgement for legislature and judiciary

The impact of the DRD Judgement on national measures is not clear. There is no general rule established by the European Courts in this context nor does the Court of Justice give any guidance in this specific case. Generally spoken there is a rule of primacy of EU law and national acts have to be in conformity with EU law. In case of a lack of a legislative act on EU level, however, Member States can introduce any national legislation as long as these acts do not violate EU law for other reasons such as unjustly infringing fundamental freedoms. With the DRD situation there is the peculiarity that many Member States struggled in finding a transposition that was not in violation of their national legal order. Now the “original” legal act has disappeared so these efforts were in a way, in vain.

If the Court had only found the EU instrument invalid due to procedural reasons, Member States would not have to draw a consequence. They could easily continue applying the transposing acts, as there would not be a violation of EU law by the substantive provisions of the respective instrument (and thereby the national acts). However, as has been shown in detail above, in the case of the DRD Judgement the Court found a substantive and severe violation of fundamental rights by the core provisions of the DRD which lead to the invalidity of the legislative act in total. It is therefore hardly imaginable that a Member State transposing act that follows the structure and content of the core provisions of the DRD can remain unchanged without itself being in violation of the fundamental rights standards set by the Court in its judgement. Moreover, as has also been shown, for the specific area of data retention there is not only the general rule of Member States being bound to EU law (including fundamental rights of the CFR) when applying measures in the scope of application of EU law, but also the more specific limitation set in

Article 15 (1) Directive 2002/58. This observation is relevant not only for the national governments and parliaments when considering what to do with their data retention schemes but in addition for national courts that are confronted with a review of national law in this field. Unsurprisingly, not only legislatures have started to react in analyzing whether the national laws can still be upheld[178], but the first courts have declared national transposition acts void, foremost the Austrian Constitutional Court[179] after having received the answer from the CJEU, but others such as the Slovenian Constitutional Court[180] have very recently, followed suit. The latter included an order to delete already retained data immediately.

Irrespective of such actions in some Member States, it needs to be stressed that the declaration of invalidity of the EU act does not have a direct impact on national law which is why it remains valid – even though possibly under the threat of being declared void on the first opportunity a court can seize – until concrete steps for amendment or revocation by the national legislatures are taken or a court rules on the validity of its applicability. In light of these observations, States basically have two options to respond to the challenges arising out of the invalidity of the DRD.

The first and recommendable option is that States start reviewing their national data retention regime, verifying whether it complies with Article 7 and 8 CFR as interpreted by the CJEU in the DRD Judgement.[181] This review will most likely result in finding amendments being necessary so in a next step Member States should then either invalidate the relevant law or enact a new law in conformity with the demanded changes. As pointed out, some states, such as Luxembourg for instance, immediately initiated the review process and plan to change their data retention regimes as soon as possible to adapt them to the new requirements.[182] As the Court's DRD Judgement does not leave much room for data retention schemes in general amended national laws will be critically monitored and will be subject to scrutiny before courts.

The second option is not to initiate any changes in domestic law and wait for further clarification on EU level. This could entail waiting for a new framework for data retention proposed by the Commission. However, such a new version of the DRD has neither been provided so far (which is not surprising given the circumstances of the upcoming end of the mandate of the current Commission) nor is it clear that this will happen in the near future. In actual fact, the (current)

---

[178] E.g. the case of Luxembourg where the Justice Minister announced already on the day of the DRD Judgment that a detailed analysis of possible consequences for the national law will be undertaken, Communiqué, Ministère de la Justice, 8 April 2014, http://www.gouvernement.lu/3641093/08-cjue.

[179] Cf. Austrian Constitutional Court, Decision of 27 June 2014, No. G 47/2012. So far only the press release is available at http://www.vfgh.gv.at/cms/vfgh-site/attachments/5/0/0/CH0003/CMS1403853653944/presseinformation_verkuendung_vorratsdaten.pdf

[180] Cf. Press Release of the Information Commissioner of 11 July 2014 concerning Constitutional Court of the Republic of Slovenia, Decision of 3 July 2014, No. U-I-65/13-19, available at https://www.ip-rs.si/index.php?id=272&tx_ttnews[tt_news]=1256&cHash=2885f4a56e6ff9d8abc6f94da098f461.

[181] Cf. on this possibility also Priebe, EuZW 2014, 456, 458.

[182] Cf. above and additionally Opinion of the CNPD (National Data Protection Commission) No. 214/2014 of 13 May 2014, http://www.cnpd.public.lu/fr/decisions-avis/2014/Vorratsdatenspeicherung/index.html. But see also on the other hand the preliminary result of the review as presented by the Minsitry of Justice, Denmark: Data retention is here to stay despite the CJEU ruling, 04 June 2014, available at http://edri.org/denmark-data-retention-stay-despite-cjeu-ruling/.

Commissioner for internal affairs expressed herself in the last hearing of the newly elected Parliament in April in a way that leaves it open whether a new proposal will come.[183] If a State therefore chooses to remain quiet on the issue, its national law created for transposition of the DRD is presumably in contradiction with the standards set in the DRD Judgement and can therefore be challenged before (national) courts subject to such mechanisms foreseen in domestic law. The goal of such proceedings would be to verify compliance with Article 7 and 8 CFR, if necessary by including the CJEU in the decision-making process. In the following, the study will briefly evaluate the different options which exist to verify national law that was enacted in consequence of the now void DRD. Since legal recourse systems in the Member States vary to a great extent and depend on national traditions, the following section is restricted to observations of a more general nature. Whether or not a national review procedure exists e.g. for individuals in the form of a constitutional complaint is dependent on a case-by-case analysis of the situation in the law of that specific Member State.

2. Claims before national courts

The most promising possibility for individuals to challenge the national act transposing the DRD is the initiation of legal proceedings in front of national courts. Depending on the procedural framework in the respective Member States such claims are possible by individuals affected by the data retention scheme, possibly by NGOs or interest groups representing a society interest and most likely also by the communications service providers that are charged with the retention of the data.

Claims of individuals or NGOs/associations could be directed against the service providers retaining the data claiming that this retention violates their human rights or the rights of the individuals represented by them. Depending on the constellation under national law the defendant of such a claim could also be the State that created the transposing act. Such claims can not only be brought against newly enacted legislation but – due to the changed circumstances for the evaluation of a data retention scheme after the DRD judgement – also against existing regimes and even if an earlier claim was unsuccessful. This possibility may be excluded due to cut-off dates included in national procedural provisions. Where the claim is admissible, these actors can invoke a violation of Articles 7 and 8 CFR, Article 8 ECHR as well as the corresponding national constitutional provisions. If there are no corresponding domestic statutory provisions, the violation of the provisions of the CFR and ECHR can still be invoked, since at least the provisions of the CFR apply directly in the Member States in this case due to the links demonstrated above between national retention schemes and the CFR standards provided for inter alia in Article 15 (1) of Directive 2002/58. The reference to ECHR provisions depends on national law, but in many legal systems in Europe the Convention has a special

[183] Commissioner Malmström at the European Parliament on 16 April 2014, cf. www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20140416+ITEM-017+DOC+XML+V0//EN&language=EN.

status that allows courts on every instance to refer to the framework that can be derived from it when assessing the validity of national laws.

Because companies active in the electronic communications sector are concerned in multiple ways they also could have an interest in bringing proceedings before Courts. On the one hand they are under the obligation to retain data on a massive scale, for which in many cases they have to cover the costs themselves which may be detrimental to their business success. On the other hand, individuals may have justified claims against the companies in view of their retention activities. Therefore, they are in a precarious situation. Complying with the national rules about data retention might lead them to be in violation of EU law. If individuals approach the companies with the request to have their data deleted immediately, arguing the retention infringes their right to privacy as established by the Court in the DRD judgement, they have to make a decision. Deciding against ignoring the national provisions on retention may lead to a violation of individuals' privacy rights which could have serious consequences. These consequences depend again on the national data protection laws but may include the obligation to pay damages or possibly even criminal liability. Service providers could further argue that they are no longer bound by the data retention requirements because the still existing national laws are inconsistent with supreme EU law. Should they argue like this and start deleting the retained data, they may in turn infringe national law with the risk of legal consequences, too.

Having this in mind, companies therefore have a genuine interest in legal certainty and are interested in reaching a clarification. It is more a question of practice why such a clarification might not be sought by the companies directly before a court: on the one hand the major players in the sector are multinationally active companies and they may have a genuine interest to be able to continue to use the systems set up in response to the national data retention requirements that were introduced or harmonized due to the DRD. On the other hand, many of these players may shy away from confronting the national legislatures with legal proceedings and rely on political lobbying instead. Smaller enterprises active in some of the Member States as electronic communications service providers may not be inclined to invest in a clarification before courts. Certainly, the status quo with its unclear terrain puts all of the service providers in a difficult situation. As a consequence some providers have already declared that they will no longer adhere to the national laws until clarification is reached[184], in other Member States the governments are considering the re-introduction of data retention laws aimed at respecting better the requirements of the CJEU in order not to loose the currently stored data.[185] States themselves should be interested in clarifying the situation as soon as possible, as it is not excluded that the companies would later turn to them with claims for damages if they retained

[184] Cf. Tung, Four of Sweden's telcos stop storing customer data after EU retention directive overthrown, 11 April 2004, available at http://www.zdnet.com/four-of-swedens-telcos-stop-storing-customer-data-after-eu-retention-directive-overthrown-7000028341/.

[185] Cf. in the UK where an emergency legislation was introduced in July, available at: https://www.gov.uk/government/publications/the-data-retention-and-investigatory-powers-bill. This will be discussed further below.

data in fulfilment of national law but were ordered to compensate individual users in a court proceeding for having continued with a practice that is regarded to be in violation of EU law.

National courts confronted with claims of the kind above would then be in a situation to review the national law which transposed the DRD not only in view of the domestic constitution but especially taking into account the relevant EU law, namely the provision of Article 15 (1) Directive 2002/58 and thereby the EU fundamental rights standards. In doing so, the courts would have to include the interpretation of Articles 7 and 8 CFR of the CJEU in its DRD judgement in order to compare whether national laws fail the test for the same reasons. If the courts would feel uncertain about being able to answer the question, they would have to ask the CJEU for advice by initiating a ruling in a preliminary reference procedure. There is a possibility that the CJEU would declare a question in this context as inadmissible in light of its *acte claire*-doctrine. According to this doctrine questions referred to the Court are unnecessary if there is previous case law that unequivocally answers the request already. The Court could come to the conclusion that its findings in the DRD judgement are sufficiently clear for questions relating comparable national measures. On the other hand, the Court may answer such requests in light of an interpretation of Article 15 (1) Directive 2002/58. Domestic courts are increasingly confronting the CJEU with CFR related and more specifically data protection questions giving the Court the opportunity to further differentiate its findings so far. One recent example is the Irish High Court that again is requesting clarification from the CJEU on questions about transfer of data to third countries and the status of the safe harbour agreement with the US.[186]

3. Proceedings before the ECtHR

A further possibility with regard to judicial review of national measures is the individual complaint's procedure at the ECtHR in Strasbourg. If a final decision in domestic law, usually by the highest Court of the Country, is reached and thereby domestic remedies have been exhausted unsuccessfully, the claimant can take his case further to the ECtHR. This court can review national measures against the standards set in the ECHR. With the already extensive relevant case law interpreting Article 8 ECHR in data related cases broadly and mostly in favour of the plaintiffs and now the interpretation of the CJEU in the DRD Judgement in which it closely refers to that standard, chances are high that a possible case of an individual against a national data retention measure might succeed. The disadvantage of this procedure is, however, the length of time it takes. Not only must national remedies be exhausted, after this the admissibility hurdle has to be cleared and then it is still likely that such proceedings would run for a couple of years.

It is worth mentioning that there is currently a case pending that originated in the United Kingdom and concerns the revelations of E. Snowden regarding the PRISM programme.[187] Although it is not yet clear, whether the case will be admissible or whether there is a lack of

[186] Cf. the Irish High Court in re. Maximilian Schrems v. Data Protection Commissioner, 2013 No. 765 JR, Judgement delivered on 18 June 2014 to stay the proceedings, available at Europe-v-facebook.org.

[187] Application no. 58170/13, *Big Brother Watch and others v the UK*.

exhaustion of domestic remedies, the questions put forward by the court to the parties promise a further interesting forming of Article 8 ECHR.

4. Infringement proceedings against EU Member States

In addition to the two mentioned options before national courts (and there possibly indirectly before the CJEU) and the ECtHR, another possibility to challenge the acts transposing the DRD, are infringement proceedings against Member States. As has been discussed above, serious doubts arise whether national transposition acts can be upheld if they were transposed in proximity to the provisions of the DRD. The Commission's role as guardian of the Treaties requires it to monitor Member States compliance with EU law and in cases of doubts to initiate infringement proceedings according to Article 258 TFEU. For political reasons it is to be expected that the Commission will not move on its own initiative in this direction very fast, but in principle there is an obligation to enter into such proceedings if a violation of EU law is likely. In the first steps of the proceedings there is a dialogue between Commission and the respective Member State about whether there is indeed a violation of EU law and how this may be rectified, before ultimately the Commission can take the Member State to Court. The CJEU can then not only declare the Member States action, e.g. a legislative act, to be in violation of EU law but in a second step also decide on fines of either regular nature applying to every continued day of the violation, or lump sum payments. This is a standard procedure and usually the threat of initiating such investigations already leads to a cooperation by the Member States. However, although chances are high that an analysis of at least a number of the Member States transpositions in the data retention area would result in a declaration of violation, the role the Commission played in preparing and enforcing the DRD makes it unlikely that it will now be the first to confront States with such proceedings. The Commission can start proceedings on its own initiative, but also be informed about a suspected EU violation by external sources including individuals, so politically this might be a viable way to put pressure on the Commission to act.

Theoretically, infringement proceedings can also be initiated by a Member State against another Member State (Article 259 TFEU) but this is an instrument that has hardly ever been used and in this case its use is very unlikely. More promising in case of continued lack of action on the side of the Member State is to consider whether possibly a proceeding for failure to act could be initiated against the Commission (Article 265 TFEU). Other than the privileged applicants such as the institutions no other admissible plaintiff can be considered here. Political pressure on Members of European Parliament may ultimately result in investigating this possibility. However, requirements for this proceeding are high and it is seldom used. It is very unlikely this procedure would lead to a result which ultimately causes a review of national data retention measures.

5. Other possibilities

In addition to the above mentioned judicial possibilities – partly combined with necessary political lobbying for the case – there are also indirect means for individuals to propose and request some form of action. The case at hand confirms that the lack of an individual review

mechanism directed against EU legislative acts (apart from the possibility of initiating procedures for annulment in case of decisions directed at individuals by these) is problematic and in many cases would lead to a faster resolution of controversial issues. However, this situation will not change in the near future, because the Court has always interpreted the admissibility of such claims under the current Treaty situation in the negative and an amendment of the Treaties expanding the jurisdiction of the Court is not very likely.

In the meantime, if no action is taken on the level of the EU and formal proceedings are not within reach for the individual one last possibility is to approach the European Ombudsman and request him to revisit the situation and moderate between the individual and the EU institutions. Concretely, the lack of response of the Commission to a possible request to initiate an infringement procedure against a specific State could be made subject of a complaint before the Ombudsman. The latter would then try and clarify the situation and probably ask the Commission to reconsider its decision of not acting. A concrete case in a related situation has already taken place, where a complainant from Germany requested a clarification why the Commission is not initiating an infringement procedure against Germany for non-transposition of the Directive 2002/58 as amended in 2009 (specifically concerning the "cookie" provision).[188]

III. Status Quo of Member States' Transposition and Data Retention Acts

In the previous two sections, this study has shown how the DRD Judgement of the CJEU influences national legislation and what means there are to achieve a review in case a Member States do not take action by themselves.

In the past couple of weeks, States have been increasingly responding to the need for review of their national situation and because every State's national implementation process differs in parts, a comprehensive overview of provisions in Member States' legislation that need to be adapted is neither necessary, nor possible in the context of this study. However, during the time that Germany was studying whether and how the DRD could be "re-transposed" after the judgement of the Federal Constitutional Court that struck down the initial transposing act, an extensive comparative study was commissioned. The results of the study suggesting a different balance between the interests at stake was published last year[189], but more importantly all reports on the situation in all of the EU Member States between 2011 and 2013 have been published.[190] These give valuable indications as to which of the Member States' transpositions are especially problematic now that the Court's DRD Judgement has confirmed that there is an infringement which is difficult to justify and in the case of the Directive was not justified.

In the present study only some recent developments and problematic situations shall be highlighted.

---

[188] Cf. http://www.ombudsman.europa.eu/en/cases/draftrecommendation.faces/en/54439/html.bookmark.

[189] Roßnagel/Moser-Knierim/Schweda, Interessenausgleich im Rahmen der Vorratsdatenspeicherung.

[190] The reports are available in English at http://www.emr-sb.de/gutachten-leser/items/forschungsprojekt-invodas-laenderberichte.html.

Some States now urgently feel the need to assure that companies do not start deleting the retained data. One example is the British Government which has introduced emergency legislation. The so called "Data Retention and Investigation Powers Bill"[191] was published on 10 July and passed the Parliament only 5 days later on 15 July.[192] The proposal consists of two parts, with the first part being a direct response to the DRD Judgement. It obliges communications service providers to continue to retain communications data of their customers through so called "retention notices". According to the British Government, the legislation is needed to make sure that LE and intelligence agencies keep their ability to access communications data. A second part introduces measures to increase transparency and oversight.

Although the three main parties support the emergency legislation[193], there is criticism with regard to the timing of the action. The bill was introduced just shortly before the summer recess and Members of Parliament did not have time to scrutinise the law in detail and propose possible changes. Due to the untypical emergency procedure, there was not much time for other critical voices to be heard. If, however, the UK bill merely re-legislates the former data retention requirements, it is doubtful whether this new measure would then comply with the DRD Judgement. Individuals as well as civil rights groups could take steps as described above to verify whether the new act complies with EU fundamental rights guarantees.

Other Member States, such as Austria, have seen an annulment of their national data retention laws in light of the DRD Judgment. In a decision of 27 June 2014 the Austrian Constitutional Court declared the Austrian Act void.[194] This was not surprising in view of the answer the CJEU had given the court to its questions in the preliminary reference procedure. In accordance with the CJEU for the DRD, the Austrian Court did not grant a period for amendments to the Austrian legislature. The reasons to annul the Austrian data retention act were similar to those of the CJEU. The Court referred to the guarantees of Article 8 ECHR that is directly applicable in Austria, to annul the act. While the full text of the judgement of the Austrian Constitutional Court will only be available in a few months, yet available, the press release of the court gives some indications why it came to similar conclusions as the CJEU. The far-reaching scope of the data retention act constituted the most serious interference with the right to data protection the Constitutional Court has so far decided on.[195] The possibility to create profiles of individuals,

[191] Available at: https://www.gov.uk/government/publications/the-data-retention-and-investigatory-powers-bill.

[192] Cf. https://www.gov.uk/government/publications/the-data-retention-and-investigatory-powers-bill and http://www.-bbc.com/news/uk-28305309.

[193] Cf. http://www.theguardian.com/politics/blog/2014/jul/10/cameron-announcing-emergency-surveillance-legislation-politics-live-blog.

[194] Cf. http://www.vfgh.gv.at/cms/vfgh-site/attachments/5/0/0/CH0003/CMS1403853653944/presseinformation_-verkuendung_vorratsdaten.pdf and http://blog.lehofer.at/2014/06/vfghvds.html; http://www.rechtsblog.at/-verfahrensrecht/page/2. The publication of the court's declaration on invalidity was published in the Austrian Gazette on 30 June 2014 with the consequence of the invalidity of the act from the day after, Österr. BGBl I 2014/44.

[195] Cf. http://www.vfgh.gv.at/cms/vfgh-site/attachments/5/0/0/CH0003/CMS1403853653944/presseinformation_-verkuendung_vorratsdaten.pdf.

the insufficient control regarding the access to the data and the missing security requirements motivated the Austrian Court to annul the act.

In further countries similar developments have occurred to the one in Austria. The Republic of Slovenia's Constitutional Court also annulled the national data retention provisions in a judgement of 3 July 2014 and ordered deletion of the currently retained data held by companies.[196] According to press articles, the arguments of the Slovenian Constitutional Court resound the CJEU Judgement.

As mentioned above, the Romanian Constitutional Court had in an earlier decision declared the national data retention act transposing the DRD void in 2009. Therefore, a new act had been introduced in 2012 to much criticism as it was even more far-reaching than the original one and did not reflect the spirit of the court's judgement. This act was again declared unconstitutional in a unanimous decision by the Romanian Constitutional Court on 8 July 2014 in the aftermath of the DRD Judgement.[197] Although the reasoning for the judgement is not yet available, it is remarkable to see the court revisiting its original stance. This will likely have a similar impact when the court will have to decide in autumn of this year about the constitutionality of a law that was passed immediately after the DRD Judgement and concerns the obligation for all users of pre-paid SIM cards to register and which would enter into force on 1 January 2015 if not declared invalid.[198]

Apart from the UK, it seems that the DRD Judgement has had a domino effect on the currently still existing data retention acts in the Member States. Although the full texts of the above mentioned cases are not available in all cases yet, the arguments of the CJEU in the DRD Judgement unsurprisingly seem to give a clear guidance and support to the national constitutional courts to also annul the data retention acts of the Member States.

IV. Conclusion

The way Member States ought to react to the Court's judgment is especially relevant since the Commission announced it would not work on a replacement Directive that would be aimed at an entry into force in a relatively short period of time.[199] This observation comes from the still current European Commission (more precisely the responsible Commissioner), but it is very unlikely this will change with a new Commission and without link to the progress on the ongoing data protection reform process. Irrespective of a (lack of) political will to move forward on EU level, the question remains – and with it as has been shown in detail previously the doubts –

[196] Cf. http://www.noodls.com/view/CBCC11E1961CEAD647CBDAE7AB42C32F1DFA58E2?7018xxx1405095291.

[197] Cf. http://www.ccr.ro/noutati/COMUNICAT-DE-PRES-99.

[198] Cf. http://www.avp.ro/comunicate-de-presa/comunicat_9iulie2014.pdf on the reference of the Act to the court by the Romanian Ombudsman for assumed unconstitutionality because of privacy rights violations.

[199] Cf. http://www.welt.de/politik/ausland/article128698101/EU-will-keine-neuen-Regeln-fuer-Vorratsdaten.html; cf. also comments of Commissioner Malmström in the EP plenary session of 16 April 2014, www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20140416+ITEM-017+DOC+XML+V0//EN&-language=EN.

whether a blanket data retention scheme is still possible on EU level at all. In the meantime, Member States acts remain in place until they are changed or declared void by a court.

If States do not react and change their data retention regime that were based on the now void DRD, claims before national courts and/or proceedings in front of the ECtHR (after having exhausted domestic remedies) remain possible within the constraints of the respective national procedural laws. Individuals, NGOs as well as companies may initiate such proceedings claiming a violation of Articles 7 and 8 CFR, 8 ECHR and the respective provisions of national constitutions. National courts confronted with such claims would then be obliged to review national data retention measures and take EU law, in particular the respective guarantees stemming from Article 7 and 8 CFR, into account. Therefore, there is a high chance that courts of Member States will also declare the national transposing act void, as it can be seen in first proceedings (e.g. in Austria and Slovenia) on this issue.

Other options to challenge a national act relate to the possible enactment of infringement proceedings against a Member State not changing its national data retention act by the Commission or – mentioned for the sake of completeness, but as explained above completely unlikely – by another Member State. Although the Commission decides itself about initiating infringement procedures, the clarity of the Court's DRD Judgement leaves hardly any room not to react at all to it, if Member State transposition acts remain in place and had from the beginning "repeated" the mistakes that have now been identified by the Court. In addition, in nothing happens, individuals could approach the European Ombudsman complaining that the Commission is not initiating infringement proceedings against a Member States that refuses to change its national data retention law.

E. Impact of the DRD Judgement on other existing Data Retention Measures of the EU

The following section refers to the impact of the DRD Judgement on existing or planned data retention schemes at the EU level. The expressed doubts regarding the question of whether blanket data retention regimes are still possible in the EU should be answered with regard to specific instruments providing for data retention. While there are several data retention measures in place at the EU level, the study refers to seven exemplary measures to illustrate their possible (in)compatibility with the standards set in the DRD Judgement. Apart from the proposal for a data protection Directive in the LE sector, which is analyzed for the sake of completeness, the examples have been chosen according to the following shared characteristics: they all provide for mass data collection and create large-scale databases throughout the Union. Additionally, some of them allow (or intend to allow) access by LE authorities to data of unsuspected persons that are collected by private parties or the EU for another purpose. To complete the picture of data protection in the LE context, the impact on the proposal for a data protection directive in the LE sector is briefly mentioned. The listed examples are generic and refer to the most problematic points of each of the mentioned measures.

I. Impact on PNR systems

1. EU-US PNR

The Agreement between the US and the EU on the use and transfer of passenger name records obliges air carriers to provide Passenger Name Record data (PNR) contained in their reservation systems to the United States Department of Homeland Security (DHS).[200] The current Agreement entered into force on 1st of July 2012. Previous versions of the present Agreement were subject to strong criticism. The first PNR Agreement[201] was declared void by the CJEU after the Court found that there was a lack of legal basis for the decision of the Council to conclude the Agreement.[202] The follow-up Agreement was signed in 2007, but never ratified and thus only – or, one may want to add, nonetheless – applied provisionally.[203] After the entry into force of the Treaty of Lisbon, the consent of the European Parliament (EP) to the Agreement became

[200] 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, OJ 2012, L 215/5.

[201] 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, OJ 2004, L 183/84.

[202] Both Article 95 and Article 300 TEC were not considered to be the appropriate basis, cf. CJEU, Joined Cases C-317/04 and C-318/04, *European Parliament v. Council and Commission*.

[203] Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS), OJ 2007, L 204/18.

necessary. Instead of giving consent, the EP demanded improvements with regard to data protection standards. The result of the subsequent renegotiations is the current Agreement.

The main purpose of the Agreement is the transfer of PNR data to the US. PNR data is the information provided by passengers and collected by air carriers during the reservation and check-in procedures. It includes information such as name, dates of travel and travel itinerary, ticket information, address and phone numbers, means of payment used, credit card number, travel agent, seat number and baggage information. The transfer of PNR by the carriers to the US can take place using two different methods: either the so called "push" or "pull" method. With the "push" method carriers transmit the required PNR data into the database of DHS. With the "pull" method, the DHS can reach in to the carrier's reservation system and extract a copy of the required data into their database.

As with its predecessors, the current EU-US PNR Agreement has recently been heavily debated. When comparing it with the requirements demanded by the DRD Judgement, some serious doubts arise regarding the compatibility of the Agreement with principles mentioned in the judgement concerning the CFR.[204]

a) Purpose and use

Article 4 of the EU-US PNR Agreement allows the use of PNR for different purposes and determines the conditions for its usage by the DHS. Generally, PNR may be collected, used and processed for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and related crimes as well as other crimes that are punishable by a sentence of imprisonment of three years or more and that are transnational in nature.[205] Based on this wording it is already clear that the purpose of the Agreement is formulated very broadly. Article 4 contains subparagraphs, which expand upon the mentioned offences by providing examples to describe terrorist offences and related crimes. There is also a description of other crimes that intends to clarify when a crime is considered to be transnational in nature. Additionally, paragraphs 2 to 4 of Article 4 mention further (exceptional) purposes PNR may be used for.

Article 4 para 1 of the EU-US PNR Agreement includes the described examples of terrorist offences, related crimes and other crimes of transnational nature. The catalogues given in this paragraph contain the words “including”, “respectively” and “in particular”. This wording indicates that the mentioned examples are not exhaustive. Other crimes could also serve as a legal basis to process PNR. This can produce considerable legal uncertainty with regards to the possible purposes of the use of PNR.

The question of which legal system will serve as the benchmark with regard to other crimes that are punishable by a sentence of imprisonment of three years or more and that are transnational in nature should be explored. Referring to a variable factor, such as three years, allows for a wide-ranging discretion of the (respective national) legislature and opens the possibility for the

[204] Guild/Carrera, p. 11.

[205] Paragraph 1 (a) and (b) EU-US PNR Agreement 2012.

US to later change the range of sentences to include different offences or introduce new ones that could qualify for PNR processing under the stated criteria.

Paragraph 2 of Article 4 of the EU-US PNR Agreement presents further possibilities for PNR processing. It can be processed, on a case-by-case basis, where necessary in view of a serious threat and for the protection of vital interests of any individual or if ordered by a court. This paragraph is not linked to the requirement of the first paragraph of Article 4. Due to this missing connection to paragraph 1 it appears that the use of PNR is allowed for any purposes as long it is ordered by a court.[206] This entails the risk of broadening the scope to undefined purposes.

Article 4 Paragraph 3 further extends the list of purposes for which PNR data can be used. The wording appears to include the use of PNR for a wide range of border control purposes which go beyond the listed purposes of terrorist-related crime or other serious offences, which formed the original purpose of the Agreement.[207] Moreover, the wording of Article 4 paragraph 4 leaves room for broad interpretation of the scope of application of this article. PNR can also be used "where other violations of law or indications thereof are detected in the course of the use and processing of PNR". Since it is not clear what is meant by "other violations of law or indications thereof", it seems that PNR can be used for various other purposes. Consequently, Article 4 allows for the use of PNR for a large range of purposes, opening the door to the use of PNR in other situations such as minor offences that should have been initially excluded from the scope of the Agreement.[208]

One important requirement demanded by the Court in the DRD Judgement is that EU legislation must lay down clear and precise rules governing the scope and application of the measure in question.[209] Purposes and offences for which the data may be used need to be defined in a clear and narrow way. The descriptions of the aforementioned provisions clearly do not comply with this requirement and hence run the risk of enabling abuse based on these undefined purposes. Furthermore, the CJEU raised the criticism that the DRD did not expressly provide for the restriction on the access and subsequent use of the data in question, although the data are used for another purposes than the initial purpose of collection.[210] Transferring these statements to the EU-US PNR Agreement, a serious conflict with regards to these requirements appears. The Agreement leaves plenty of room for the use of PNR that is linked neither to fighting terrorism nor serious crime, hence leaving its purpose open to a variety of other uses.

---

[206] Compare also in this regard the draft recommendation of rapporteur Sophia in't Veld, 30 January 2012, 2011/0382 (NLE) and the following opinions: Opinion 7/2010 of the Article 29 Working Party, WP 178 (2010); Opinion of the EDPS of 9 December 2011 on the Proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, OJ C 35/03, 9.2.2012; Note from the Commission legal service to DG Home affairs of 18 May 2011; Letter from the Article 29 Working Party to the Members of the LIBE Committee of the European Parliament of 6 January 2012.

[207] Hornung/Boehm, p. 10.

[208] Hornung/Boehm, p. 11.

[209] DRD Judgement, para 54.

[210] DRD Judgement, para 54.

b) Retention period

As already mentioned, the implementation of a time limit is a safeguard to avoid indiscriminate storage of personal data. The EU-US PNR Agreement provides for a retention period in Article 8. It is structured in the following way: The PNR are retained in an "active database for up to five years" whereby "after the initial six months of this period, PNR shall be depersonalized and masked […]".[211] After the five years, the PNR are "transferred to a dormant database for a period of up to ten years". There, the data can be "re-personalized" in "connection with law enforcement operations" related to "an identifiable case, threat or risk". Data collected for the purposes of Article 4 (1) (b) (transnational crimes that are punishable by a sentence of three years or more), should only be re-personalized for a period of up to five years.[212] Following the dormant period, the data are not deleted, but "fully anonymized" without the possibility of re-personalization.[213] However, data relating to a "specific case or investigation may be retained in an active PNR database until the case or investigation is achieved".[214]

It is noteworthy that data can be re-personalized, until it has left the dormant database. Thus, this possibility makes the data "personal data" in the meaning of Article 2 (a) of Directive 95/46/EC for the full period of fifteen years. After the dormant period there is an obligation to fully anonymize PNR. Although the data are already retained for the very long period of 15 years, the anonymized PNR are still retained. This means that there is no time limit to the retention of anonymized PNR, making the retention period infinite. It is very clear that such an unlimited retention period does not effectively balance the interests of unsuspected individuals with crime prevention purposes thereby contradicting the DRD Judgement. Moreover, although being officially anonymized, re-personalization seems to be possible; otherwise an indefinite retention period of completely anonymized data without specifying the reasons for retention, would not make much sense. This constitutes a risk for the rights of individuals. Frequent travellers or those with unusual PNR sets may be the first targets of such re-personalization.[215]

Even if one assumes that the possibility of re-personalization is only theoretical, the conditions set by the CJEU with regard to legal clarity are not fulfilled. This requirement is not met when using undefined terms such as "anonymization", "masking out" and "re-personalization". A clarification of these terms is of utmost importance if the Agreement should comply with EU case law.

Moreover, with regard to the retention period, the Court demands legal distinctions between the categories of data on the basis of their possible usefulness for the purposes of the objective pursued or according to the categories of persons concerned.[216] In addition, the principle of proportionality requires a determination of the retention period that is based on objective

[211] Article 8 (1) EU-US PNR Agreement 2012.

[212] Article 8 (3) EU-US PNR Agreement 2012.

[213] Article 8 (4) EU-US PNR Agreement 2012.

[214] Article 8 (5) EU-US PNR Agreement 2012.

[215] Hornung/Boehm, p. 12.

[216] DRD Judgement, para 63.

criteria.[217] Since all data, including that of both suspicious and unsuspicious persons are retained indistinctively for up to 15 years, the Agreement contradicts the principles developed in the DRD Judgement. The indifferent treatment of suspicious and unsuspicious people in this context leads to the effect the ECtHR has termed as "risk of stigmatization" in the *S. and Marper v. UK* case[218] to which the CJEU repeatedly refers in its DRD Judgement. The non-conformity with the judgement is also supported by the fact that the Agreement does not give any guidance with regard to the application of a shorter than the maximum retention period. As a result, the lack of objective criteria for storage is evident.

c) Amount of data sets and access to PNR

The EU-US PNR Agreement provides for the collection of 19 data sets, which entail more than 34 different individual data records, put into 19 umbrella terms.[219] These data sets lead to a very comprehensive picture of an individual. Similar to the retention system established by the DRD, PNR is collected by the persons providing the service, i.e. the air carriers. The DHS accesses the data in a second step. But contrary to the electronic communications providers in the DRD context, the air carriers are not only obliged to retain the data, they must also tolerate the direct access of the DHS to their databases.

This structure is clearly inconsistent with the legal approach set out by the CJEU. The Court criticised that the DRD does not contain substantive and procedural conditions that could limit the access by the competent national authorities to the data and their subsequent use. By referring to these limitations, the CJEU shows that both access and use of personal data collected by private parties for non LE-purposes by LE authorities must be the exception rather than the rule. Therefore, the Court demands that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto.[220] In the EU-US PNR Agreement, the restrictions mainly concern the use of the data and do not give limitations as to the access. Consequently, the DHS has unlimited access to huge amounts of data sets.

This contradicts one further key statement of the CJEU. Data retention is only considered lawful if there is a connection between data to be retained and a threat to public security. That is why the Court demands, alternatively or cumulatively, restrictions (i) to cases in which the data pertains to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.[221] Contrary to this, the PNR Agreement obliges air carriers to retain the data solely based on the reason that a person is

[217] DRD Judgement, para 64.

[218] ECtHR, S. and Marper, para 122.

[219] Compare Hornung/Boehm, p. 14.

[220] DRD Judgement, para 61.

[221] DRD Judgement, para 59.

taking a flight to or from the US. Thus, the Agreement affects in a comprehensive manner all persons, without establishing a link between the purpose of retention and a threat. The persons, whose data is being retained, do not relate even indirectly to a situation that is liable to give rise to criminal prosecutions.[222] Consequently, the Agreement fails to establish this crucial link necessary for the establishment of data possible retention regimes.

d) Access and transfer

As outlined above, air carriers are obliged to make PNR data accessible to DHS. The primary method for air carriers to make the data accessible is according to Article 15 (1) EU-US PNR Agreement the "push" method. This procedure had to be implemented by every carrier by 1st July 2014. Alternatively, the "pull" method could be used until that deadline, which means that DHS had direct access to the airlines' reservation systems. This method of direct access can be extended for technical reasons, if the air carrier cannot respond timely to requests and in exceptional circumstances, according to Article 15 (5) EU-US PNR Agreement.

The reasons why the DHS may claim to need these so-called ad-hoc "pulls" are manifold: If due to technical reasons the air carrier is not in a position to send the data via the "push" method, direct access is needed. Further, if there is a need to provide PNR between or after the regular PNR transfers in order to respond to a specific, urgent and serious threat. Moreover, in the case that a flight with no US connection will land on US soil for reasons linked to weather conditions or other unforeseen reasons, immediate PNR transfer is needed.[223] The DHS also insisted that even in the case where all air carriers affected by the Agreement will use a "push" method for transmitting the data this would not affect the use (or possibility of use) of the ad-hoc "pull" by the DHS.[224]

While the general approach of providing the DHS direct access PNR without any further control by an independent authority can already be criticised as violating fundamental rights, the use of the "pull" method is even more problematic and not in compliance with the principles developed in the DRD Judgement. The Court explicitly stated that "access by the competent national authorities to the data retained must be made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued […]".[225] Thus, due to the lack of an independent intermediary, the EU-US PNR Agreement fails to meet one key element demanded by the Court. This is especially detrimental to the protection granted by the CFR, if the "pull" method is applied by DHS. Moreover, in the three exceptional cases that could legitimate ad-hoc "pulls" there is no control by an independent authority before PNR are transferred. Therefore, there are no safeguards to

[222] DRD Judgement, para 58.

[223] EU Commission PNR report, COM(2013) 844 final, p. 18. Available at: http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/docs/20131127_pnr_report_en.pdf.

[224] COM(2013) 844 final, p. 18.

[225] DRD Judgement, para 62.

protect PNR against the risk of abuse and any unlawful access and use. Instead, in practice DHS will be able to get access to all the PNR data it regards as useful.

This finding is exacerbated by the fact that there is no independent supervision of the PNR transfer at all. Article 14 EU-US PNR Agreement provides for "independent review and oversight by Department Privacy Officers, such as the DHS Chief Privacy Officer" as well as "the DHS Office of Inspector General, the Government Accountability Office […] and the U.S. Congress". These measures nonetheless do not conform to the EU understanding of independent review. These authorities (with the exception of the US Congress) are not independent from governmental influence as required by the case law of the CJEU and mentioned in Article 8 CFR.[226] The fact that no independent review at EU level exists and that an internal DHS officer should supervise the transfer of an agency that actually is his employer, excludes by definition, independent review.[227]

Domestic data sharing and onward transfer of PNR is possible for a wide range of purposes. Article 16 (1) (a) and (b) of the EU-US PNR Agreement allow the transfer of PNR to (other) domestic authorities for various purposes, including border security or the use of PNR if ordered by a court or other violations of law. The purpose of transfer must apparently only be somehow connected to the overall purpose of the Agreement.[228] If this connection exists, the only substantive requirement for domestic sharing is that "comparable safeguards as set out in [the] agreement" are established by the receiving authority.

Article 17 (1) states that PNR may be transferred to authorities of third countries "only under terms consistent with this Agreement and only upon ascertaining that the recipient's intended use is consistent with these terms". This wording remains ambiguous, in particular with regard to the meaning of the term "consistent with this Agreement". Whereas the provisions on domestic data sharing refer directly to the purposes mentioned in Article 4, this reference is lacking in Article 17. This missing reference may allow other purposes for transfer.[229] Thus, the Agreement does not comply with a further decisive principle set by the CJEU in the DRD Judgement. There is no objective criterion by which the limits of the access of the competent national authorities to the data and their subsequent use can be determined.[230] Instead of limiting possible recipients of PNR, the broad and extensive wording of the Agreement leaves ample room for transferring data to an indeterminate number of national authorities.

e) The rights of the data subjects

The CJEU, in line with ECtHR case law, insists on a further crucial element in data retention legislation. Legislatures must impose minimum safeguards so that the persons whose data have

---

[226] Compare Cases C-288/12 *Commission v. Hungary*, C-614/10 *Commission v. Austria* and C-518/07 with regard to independent data protection authorities in Hungary, Austria and Germany.

[227] Compare for the independency requirement in EU data protection law: Case C-518/07 *Commission v. Germany*, paras 25, 30, 33 and in particular 36.

[228] Compare Hornung/Boehm, p. 13.

[229] Compare Hornung/Boehm, p. 13.

[230] DRD Judgement, para 60.

been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data.[231] Of particular importance is the guaranteed option of procedural remedies by which persons can proceed against illegitimate usage of data. With regard to this, it must be noted that the EU-US PNR Agreement mostly refers to US laws which would apply to the data subjects in any case (cf. Article 21 EU-US PNR Agreement). Experience shows, however, that the practical enforcement of remedies in the US for EU citizens is difficult. Obtaining effective protection in the US is therefore at best doubtful.

2. EU-PNR

Parallel to the discussion about the EU-US PNR Agreement, the Commission developed the idea of an EU PNR system aiming to control PNR of air carriers operating flights between a third country and the territory of at least one Member State.[232] Air carriers would be obliged to transfer PNR of international flights departing or originating in the EU to the competent authorities in the Member States, which are known as Passenger Information Units (PIUs). The PIUs would then conduct LE analysis and forward, on request, the data to national LE authorities of the Member States.

On 6th November 2007 the Commission adopted a proposal for a Council Framework Decision on the use of Passenger Name Record data for law enforcement purposes.[233] Upon entry into force of the TFEU, the Commission proposal, not yet adopted by the Council, became obsolete because the Lisbon Treaty required a participation of the parliament in the LE sector (former third pillar). Therefore, on 2nd February 2011 the Commission adopted a new version of its proposal, now in the form of a directive which includes the participation of the Parliament in the legislative process.[234] Now, in 2014 – more than three years later – the legislative process is still in progress. While the LIBE committee rejected the 2011 proposal of the Commission in its meeting in April 2013 by a vote of 30 to 25, a majority of the European Parliament decided to postpone its voting and to transfer the proposal back to the LIBE committee in June 2013.[235]

This difficult legislative procedure is the result of contradictory opinions on the content of this proposal. The DRD Judgement is likely to support the critical voices mentioned above. Since the basic idea of an EU-PNR system is very similar to the now void DRD and moreover, it is based in many essential points of the EU-US PNR Agreement, most of the criticism issued above, can be

---

[231] DRD Judgement, para 54.

[232] Proposal for a directive of the European Parliament and the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final.

[233] Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, COM(2007) 654.

[234] EU-PNR proposal, COM(2011) 32 final.

[235] Rejection of the LIBE Committee on 24th April 2013 and postpone decision on 10th June 2013, compare procedural file: http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?id=589738 and press release regarding the rejection: http://www.europarl.europa.eu/news/de/news-room/content/20130422IPR07523/html/Civil-Liberties-Committee-rejects-EU-Passenger-Name-Record-proposal.

transferred to the discussion about the EU-PNR.[236] For instance, as in the DRD case there is no relationship between the types of data that can be retained and a threat to public security.[237] The mere fact that a person is taking a flight to or from the EU cannot establish such a "link"[238]. Instead of restricting the retention according to the suggestions of the CJEU[239] the proposal provides for general storing of PNR data to hold them available for further analysis.

Nonetheless, since plans still exist to establish this EU-PNR system in the near future, the proposal is analysed in detail in the following section.

a) Purpose and use

The purpose of the EU-PNR proposal is mentioned in Article 1 (2). Processing of PNR data may only be conducted for the prevention, detection, investigation and prosecution of terrorist offences, serious crime and serious transnational crime. The definition of "terrorist offences", "serious crimes" and "serious transnational crimes" is laid down in Article 2 (g), (h) and (i) EU-PNR proposal. Contrary to the EU-US PNR Agreement, the list of crimes in the EU-PNR proposal is more specific and refers to the crimes listed in these articles. However, this list is formulated in an exhaustive way. Article 5 (5) EU-PNR proposal provides for a further exception to the list: The permission to further process PNR data only for the mentioned purposes "shall be without prejudice to national law enforcement or judicial powers where other offences, or indications thereof, are detected in the course of enforcement action further to such processing". PNR can therefore also be used for other purposes, in particular for minor offences, if national law provides for it. This provision clearly weakens the purpose limitation that is foreseen in the Article 1 (2) of the proposal.

In addition, in particular the term "serious crime" leaves room for interpretation. For instance, if offences that are mentioned in the Framework Decision on the European Arrest Warrant[240] to which Article 2 (h) of the EU-PNR proposal refers to, like "illicit trafficking in narcotic drugs and psychotropic substances", "corruption", "computer-related crime" and "racism and xenophobia" are punishable by a "custodial sentence or a detention order for a maximum period of at least three years under the national law of a Member State", they are regarded as "serious crime".[241] A range of sentences of more than three years for criminal offences is, however, frequently found in a majority of national criminal codes.[242] Therefore, it is possible to interpret the term "serious crime" very broadly and, if necessary, to adapt the range of sentences in national criminal law in a way that allows expanding the possibility to process PNR data. The ability to interpret the term serious crime in a far-reaching manner seems to be

---

[236] Compare also: Guild/Carrera, p. 11.

[237] DRD Judgement, para 59.

[238] Cf. DRD Judgement, para 58.

[239] Cf. DRD Judgement, para 59.

[240] Article 2 (h) EU-PNR proposal refers to the offences described in the Council Framework Decision 2002/584/JHA on the European Arrest Warrant.

[241] Article 2 (h) EU-PNR proposal.

[242] Compare for instance the Luxembourgish Criminal Code.

doubted by some Member States and even the Commission itself. Article 2 (h) EU-PNR proposal provides for exceptions for Member States which want to exclude "those minor offences" (wording of article 2 (h)) from the processing of PNR. This possibility shall ensure conformity with the principle of proportionality in the respective national laws. By implementing the exception to the rule in Article 2 (h) it appears that the Commission itself regards the list as too extensive and therefore not (unavoidably) necessary in a democratic society. If, however, some Member States apparently reach the conclusion that the processing of PNR for "minor offences" does not comply with the proportionality principle, the application of the measure to such offences should be generally questioned, particularly because the principle of proportionality must be fulfilled in an equal manner across the EU and at EU level.

In addition, the possibility of exceptions in national law is likely to produce legal uncertainty with regard to the determination of "minor crimes". Some Member States would be able to use PNR in these cases, others not. This would result in an inconsistent use of PNR across the Member States.

As a result, leaving Member States a wide margin for discretion with regard to the transposition of the purpose of processing is not compatible with the required precision and clarity the CJEU explicitly demanded in its DRD Judgement.[243]

b) Retention period and distinction between different categories of data

The EU-PNR proposal contains a time limit for data retention in its Article 9. Firstly, the PNR data are retained in a database at the PIU for a period of 30 days. The period starts with the transfer to the PIU of the first Member State on whose territory the flight is landing or departing. Secondly, after the 30 days-period the data must be retained at the PIU for a further period of five years.[244]

While identification of the passenger is easily possible during the 30 day-period, according to Article 9 (2) the collected data must be depersonalized afterwards. To fulfil this requirement, the PIU is assigned to mask out names, address and contact information, information which could serve to identify the passenger and advanced passenger information. However, the EU-PNR proposal mentions in the very same paragraph the possibility for other PIUs to access "full PNR data without the masking out" also after the 30 day-period in case of a specific threat, specific investigation or prosecution related to terrorist offences or serious crimes.[245] This means in consequence that depersonalization is useless, if data are needed for any kind of investigations in such cases, including those investigations for minor offences, as the purpose for access also includes "serious crime" (as it is to be defined by the Member States).

It is worth noting that the data must be regarded as "personal data" in the meaning of Article 2 (a) of Directive 95/46/EC for the full period of storage. This means that data of initially unsuspicious persons are constantly available for a period of 5 years for LE purposes. This

[243] DRD Judgement, para 54.

[244] Article 9 EU-PNR proposal.

[245] Article 7 (3) EU-PNR proposal.

situation is very similar to the DRD situation which the CJEU has just declared void. It also needs to be remembered that in the PNR case the retention period is considerably longer than the period which was declared void in the DRD Judgement. Therefore, the five years-storage period with permanent access for LE to the data hardly seems compatible with necessity and proportionality requirements.

In addition, the CJEU in the DRD Judgement repeatedly referred to the relevant ECtHR case law and demanded safeguards that prevented stigmatizing persons through data retention. Such safeguards, however, cannot be found in the EU-PNR proposal since PNR data of all persons (flying from third states to the EU and vice versa) would be retained for a period of up to 5 years and 30 days irrespective of whether they are regarded as suspicious persons in a crime and without making a distinction between different data categories. The EU PNR proposal simply provides for the retention of the whole bulk of PNR data (with the exception of sensitive data).[246]

Another shortcoming that can be found when analysing the proposal against the background of the DRD Judgement is the absoluteness of the retention period. The CJEU demands that there have to be objective criteria in order to ensure that the retention period is limited to what is strictly necessary.[247] The EU-PNR proposal provides for retention length of five years and 30 days without any exceptions and without any criteria that could be applied to result in a shorter retention period. Such a general rule that is not based on objective criteria and does not provide for any exemptions cannot be regarded as strictly necessary.

Consequently, this very long and for the most part, indifferent retention period for data of mainly unsuspected persons with the constant possibility of LE access, does not fairly balance the LE interests with the rights of the persons concerned, as it is required by the CJEU in the DRD Judgement.

To sum up, similar shortcomings as outlined in the analysis of the EU-US PNR Agreement can be observed. Firstly, the proposal does not make a distinction between categories of data on the basis of their possible usefulness for the purposes of the objective pursued or in relation to the persons concerned. Secondly, the risk of stigmatization appears because PNR of suspected as well as of unsuspected persons are retained for up to five years and 30 days. Lastly, no objective criteria are laid down that could enable the application of a shorter retention period.

c) Amount of data sets

The EU-PNR proposal provides for the collection of the same 19 data sets that are mentioned in the EU-US PNR Agreement (cf. annex of the proposal). According to Article 6 (1) EU-PNR proposal, the air carriers are obliged to collect the data and make them accessible to the PIUs without further requests within 24 to 48 hours before the scheduled time for flight departure. Additionally, PNR has to be transferred again immediately after flight closure/boarding.

---

[246] Article 11 (3) EU-PNR proposal.

[247] DRD Judgement, para 64.

The obligation to transfer all PNR to the PIUs would produce extensive databases at the PIUs, which are directly controlled by the State. Further, there is no independent intermediary controlling access to this data. This is particularly astonishing in light of the quantity of data retained. In contrast to the DRD situation, where "metadata" were collected, the collection of PNR entails the direct gathering and processing of content. The 19 collected data sets encompass more than 34 different individual data records, put into 19 umbrella terms.[248] These data sets cover a wide range of information about persons, relating to meal habits, credit card information, including which tickets are paid with the same credit card, accompanying persons, possible hotel bookings, all travel agency information etc.[249] The retained data sets allow for a comprehensive picture of an individual, including his/her connections to other persons. This makes the retained data very sensitive and enables the deduction of important conclusions regarding the individual's private life. Moreover, the data sets (as well as the findings derived from the analysis thereof) could be combined with other data sets (for instance with persons having a connection to the first data set) and this leads to a very wide-ranging application and infringement of fundamental rights.

Moreover, a very high number of persons would be affected by the planned measures. More concretely, a background document to the EU-PNR proposal clarifies that "only" 36 % of the flights in the EU are flights to third countries.[250] The number of flight passengers in the EU was 632 million in 2013 according to statistics of Eurostat.[251] 36 % of 600 million is around 216 million passengers who would be then targeted by the EU-PNR proposal.

The finding above raises some serious objections regarding this proposal. The PNRs originate from unsuspicious persons making a flight reservation. The records are then retained and analysed in a very widespread and comprehensive manner for LE purposes. The amount of data retained and the purpose for which they are used is therefore not limited to what is strictly necessary.

d) Access and transfer

With regard to access to and use of the PNR data, there are some minor differences between the EU PNR proposal and the EU-US PNR Agreement. While the latter states that data must be transferred by the air carriers to DHS, Article 3 of the EU-PNR proposal provides for the implementation of PIUs in the Member States. It is possible that two or more Member States establish one single PIU. These PIUs shall be responsible for the collection, storage and analysis of PNR. The result of the analysis is then transmitted to the competent authorities. Competent authorities are authorities responsible for the prevention, detection, investigation or prosecution of terrorism and serious crime. Thus, in addition to the PIUs, various national authorities are entitled to take actions on basis of the PIU findings or to examine the PNR

[248] Compare Hornung/Boehm, p. 14.

[249] Boehm, European Flight Passenger Under General Suspicion – The Envisaged Model of Analysing Flight Passenger Data, pp. 171-199, in particular p. 173 and Hasbrouck Edward: http://hasbrouck.org/articles/PNR.html.

[250] Council of the European Union, Interinstitutional File: 2011/0023 (COD) of 28 March 2011, p. 3.

[251] Compare: http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&plugin=0&language=de&pcode=ttr00012.

further. It is also possible that staff members of the PIU may be delegated from other competent public authorities.[252] The composition of the PIU staff is therefore not clearly defined and the circle of persons having access to the data is very broad. In this context, it should be noted that any access to or transfer to another authority constitutes an additional interference with fundamental rights that requires justification.[253] Considering the current composition of the PIU and the possible transfer of PNR to other authorities, it seems that another general principle set by the CJEU may be violated. Instead of laying down objective criteria, which would limit the number of persons authorized to access and subsequently also limit the use of PNR to what is necessary, the provision leaves room for an arbitrary expansion of the persons who may access the data sets.[254]

In addition to the difference with regard to the structure of the national authority entitled to access and use the PNR data, the method of data transfer constitutes another relevant difference. Contrary to the EU-US PNR Agreement, the EU PNR proposal does not provide for the "pull"-method. Instead, it relies exclusively on the "push"-method.[255]

However, this technical difference does not alter the fact that there are other very important shortcomings with regard to the lack of an intermediary. As described above in the analysis of the EU-US PNR Agreement, the CJEU has required that access by the competent national authorities to the data retained must be made dependent on a prior review carried out by a court or by an independent administrative body.[256] The decision of an intermediary is needed to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued.

This crucial safeguard is missing. There is no independent control body between the PIUs and other national LE authorities accessing the PNR.[257] Staff of the PIU may be additionally delegated from the accessing public authorities.[258] In practice, PNR is accessed on the authorities' own initiative. Thus, the lack of independent prior control before accessing the data does not comply with the restricted access conditions required by the CJEU.

Transfer of PNR between the PIUs of the Member States is also possible.[259] Analyzing these transfer provisions, it is worth noting that the only substantive requirement for transfer between PIUs is the assumption that the PNR are regarded necessary for the prevention,

---

[252] Article 3 (1) EU-PNR proposal.

[253] Compare: DRD Judgement, para 33.

[254] DRD Judgement, para 62

[255] Article 6 EU-PNR proposal.

[256] DRD Judgement, para 62.

[257] DRD Judgement, para 62. The fact, that there is, in contrast to the EU-US PNR Agreement, an obligation providing for the implementation of a national supervisory authority generally monitoring the application of the measure (cf. article 12) is not sufficient. This supervisory authority does not have any decisive power with regard to access control.

[258] Article 3 (1) EU-PNR proposal.

[259] Article 7 EU-PNR proposal.

detection, investigation or prosecution of terrorist offences or serious crime. As already shown above, these purposes are very wide-ranging and partly imprecise.

The transfer provision is structured as following:

In general, Article 7 (1) stipulates that PNR are transferred on the PIU's own behalf if their assessment has led to the identification of a suspicious person and the PIU regards the transfer necessary for the prevention, detection, investigation or prosecution of terrorist offences or serious crime. Article 7 (2) and (3) of the EU-PNR proposal grant PIUs of other Member States the right to request PNR data in two cases: PNR collected in the period of the first 30 days (Article 9 (1)) can be accessed under the condition of necessity for a "specific case" of prevention, detection, investigation or prosecution of terrorist offences or serious crime. PNR retained after the 30 days period are "masked out" and can be requested if deemed necessary for those purposes, even in the absence of a specific case. In an "exceptional case", data are transferred in an unmasked version.[260]

Exceptionally, according to Article 7 (5) a PIU of another Member State has the right to request for PNR data transfer where early access is necessary to respond to a "specific and actual threat" related to terrorist offences or serious crime. Additionally, competent foreign authorities may address a request directly to a PIU if it is necessary for the prevention of an "immediate and serious threat" to public security.[261]

Consequently, the exchange of PNR may take place between different Member States without any prior review by an independent body that can verify whether the access conditions are fulfilled. Additionally, the access conditions are very broad and not limited to objective criteria as required by the Court according to the standards of its DRD Judgement.[262]

3. Key findings

Both PNR systems fail to comply with the most basic requirements the CJEU stipulated in the DRD Judgement. The most striking imbalance with fundamental rights relates to the indiscriminate bulk data collection in the PNR systems. The transfer of data of EU citizens to the US due to the EU-US PNR Agreement is highly critical and not in line with the EU and ECtHR case law. But also the planned EU-PNR system is not compliant with EU privacy and data protection guarantees in many ways. Both systems affect an enormous amount of individuals without ever considering the necessity of such globally applicable measures.

In both cases, the systematic and indiscriminate storage and analysis of data of unsuspicious persons are not in line with fundamental rights. Major problems arise with independent oversight as well as, most importantly, with the required link between a threat to public security and the data stored. Further, the retention period – that is indefinite in case of the US-system

[260] Article 7 (3) EU-PNR proposal.

[261] Article 7 (4) EU-PNR proposal.

[262] DRD Judgement, para 60.

and very long in the EU-PNR proposal – fails to strike a fair balance between the different interests at stake.

To sum up, both PNR systems in essential points fail to comply with basic requirements of CJEU and ECtHR case law.

II. Impact on terrorist finance tracking programmes

1. EU-US TFTP Agreement 2010

The current agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the EU to the US for purposes of the Terrorist Finance Tracking Program (TFTP) was signed in Brussels on 28th June 2010 and entered into force on 1st August 2010.[263] The Agreement covers the transfer of "financial payment messages" (bank data) stored in S.W.I.F.T. (Society for Worldwide Interbank Financial Telecommunication) databases to the US. Bank data include information about bank transfers such as the sender, the date and time of transfer, the amount transferred, the purpose etc. in addition to bank clearing[264] and "related data".[265] Data concerning EU-internal bank transfers in the Single Euro Payment Area (SEPA) are excluded from the scope of the 2010 agreement.[266] Included, however, are other EU-internal bank transfers in another format than SEPA.[267] As a consequence of the NSA revelations in summer 2013, the European Parliament requested the suspension of the TFTP agreement in October 2013.[268] When comparing the current TFTP agreement with the requirements included in the DRD Judgement of the CJEU, serious doubts regarding the compatibility with Article 7 and 8 CFR arise.

a) Bulk data transfer

According to Articles 2 and 4 of the EU-US TFTP Agreement, the data transferred should relate to the transfer of specific data sets for the purpose of the prevention, investigation, detection or prosecution of terrorism or terrorist financing. In practice, however, technical difficulties and the US interest in keeping confidential from the bank data provider the exact data sets it requests and uses, lead to the transfer of considerably more data than only terrorist related data. The Commission explains this commonly known practice as follows:

> "[…] the implementation of the EU-US TFTP Agreement entails the provision of large amounts of personal data ("bulk data") to U.S. authorities - the vast majority of this data

[263] Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, OJ 2010, L-195/5 (EU-US TFTP Agreement 2010).

[264] Data related to the fact that the banks clear the financial transfers of their clients with other banks.

[265] Article 1 (1) (a) EU-US TFTP Agreement 2010.

[266] Article 4 (2) (d) EU-US TFTP Agreement 2010 clarifies that the data transferred shall not include "data relating to the Single Euro Payment Area" (SEPA).

[267] Ambrock, S. 75, with reference to the EDPS Opinion of 22 June 2010, p. 3.

[268] Compare: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+IM-PRESS+20100209IPR68674+0+DOC+XML+V0//EN

concern citizens who have nothing to do with terrorism or its financing. The data is provided in bulk (on the basis of relevant data categories) rather than on an individual basis (in response to a request concerning one or more individuals), due to the fact that the provider of these data does not have the technical capacity to provide the data on an individualised basis."[269]

Even though this statement was made in 2011, the situation regarding the mass data transfer has not changed since. The latest report of the Joint Supervisory Body of Europol (JSB) emphasises this point, repeating that currently there is "a massive, regular, data transfer from the EU to the US" which concerns mostly non-suspects.[270]

In addition to the mentioned technical difficulties seemingly not allowing for a more targeted transfer, there is also the interest of the US not to inform the provider (S.W.I.F.T.) of which individuals are actually subject of an investigation. US officials fear that the information of the provider could have "an impact on the effectiveness of [such] investigations".[271] In practice, although the transfer of data should be limited to specific cases according to Article 4 of the EU-US TFTP Agreement, millions of data sets with no link to terrorism are transferred.[272]

Moreover, if the data are not used and therefore not extracted, they can nonetheless be stored for a five-year period.[273] Consequently, the TFTP database contains bank data of unsuspicious EU citizens for a long period of time although there never existed a reason to transfer them in the first place.

The common practice of bulk data transfer and the subsequent storage of these data are clearly not consistent with many of the requirements stipulated by the Court in the DRD Judgement. The required relationship between the data subject and a threat to public and/or criminal prosecutions, for instance, is not met. Further, the transfer of non-suspect's data to a third country not meeting the EU adequacy standard is clearly not necessary for the purpose of the agreement.[274] Therefore, the transfer of data regarding non-suspects, at the very least, contradicts the proportionality requirement as extracted in the DRD Judgement. In addition, the data are not only transferred, but also stored for up to five years in the US, even if they are not relevant for any investigation. This aggravates the situation in many ways. Independent control and redress mechanisms are almost entirely excluded. In this context, the Court in the DRD Judgement emphasized the importance of the place of storage in light of Article 8 (3) CFR with regard to the retained data. Thus, if the transfer of data of unsuspicious EU citizens to the US is

---

[269] Communication from the Commission to the European Parliament and the Council – A European terrorist finance tracking system: available options, COM(2011) 429 final, pp. 2-3.

[270] Publicly available report of the Joint Supervisory Body of Europol of 18 March 2013, available at: http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en. There is also a non-public classified version of this report that is of course not available on the website. Therefore, the exact number of data sets transferred to the US is not made public.

[271] COM(2011) 429 final, p. 3.

[272] There is no targeted search in the EU, compare: Ambrock, p. 127.

[273] Article 6 (4) EU-US TFTP Agreement 2010.

[274] DRD Judgement, paras. 58 and 59.

not necessary, the subsequent storage for such a long period of time in a country where EU based authorities have no ability to independently monitor the storage, fails to satisfy the necessity requirement.

Considering these arguments, there are strong doubts regarding the proportionality and necessity of the bulk data transfer to the US and its subsequent storage.[275]

b) Independent oversight

Another key element to assure proportionality with regard to the serious interference caused by the transmission of data to a LE authority is the prior review of access requests carried out "by a court or by an independent administrative body".[276] The decision of an independent authority is important to "limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued".[277] The independent control requirement is also stipulated in Article 8 (3) CFR which emphasizes that compliance with data protection rules shall be subject to control by an independent authority.

In case of the EU-US-TFTP Agreement however, access requests are directed to Europol, the EU LE agency responsible for the prevention and combating of organized and serious crime as well as terrorism. This agency then decides whether the access conditions of the US are complied with. In addition, Europol does not only verify the access conditions, it is also entitled to ask for information obtained from the TFTP analysis. The agency has thus a strong interest in permitting US access to S.W.I.F.T. data.

There is no doubt that this concept – a LE agency with genuine and singular interest in the data analysis, controlling the access of another LE agency – does not correspond to the independence requirement of the Court. The objective of limiting access to the strictly necessary can thus not be obtained by the current oversight mechanism.

c) Information of persons concerned and redress

Further doubts relate to the information rights of persons concerned. According to Article 14 TFTP, the US Treasury Department is obliged to provide general information about the Agreement. However, there is no specific obligation to inform the data subject about the data transferred to a third country. In addition, redress seems to be restricted to extracted data.[278] As a consequence, persons whose data have been transferred, but not (yet) accessed, have no possibility to obtain information regarding the processing or transfer of their data. The missing information and redress mechanism contradicts established case law of the ECtHR to which the

[275] One alternative that would lead to equal results could be the filtration by EU authorities and transfer of specific data to US, compare Ambrock, p-131-136.

[276] DRD Judgement, para 62.

[277] DRD Judgement, para 62.

[278] EDPS comments on the Communication from the Commission to the European Parliament and the Council – A European terrorist finance system (EU TFTS), COM(2013) 842 final and its accompanying impact assessment of 17 April 2014, para 33 with reference to the Article 29 Working Party letters of 7 June 2011 to the US Treasury and of 29 September 2011 to Commissioner Malmström.

Court refers in its DRD Judgement.[279] In particular, in the admissibility decision *Weber and Saravia v. Germany*, the Strasbourg Court recognized the importance of a notification in the context of surveillance measures.[280] The arguments of the ECtHR relate to the possibility of individuals to obtain effective remedies before courts. Only if one has the means to challenge the legality of a possible surveillance measure, effective control and redress mechanisms are possible.[281] If it is an essential requirement to be able to challenge a surveillance measure in order to comply with fundamental rights, it is even more fundamental to be able to challenge the legality of a data transfer. In particular, in cases in which the data are accidentally transferred within the bulk data sets, information is the minimum safeguard required as a means to counter the concern of constant surveillance as it is mentioned in the DRD Judgement.[282] To avoid the possibility that that every person concerned (in fact, every EU citizen carrying out a bank transfer to a third state) would have to make regular requests to the TFTP, information about the transfer should be issued proactively and not only upon request.

2. EU-TFTS Proposal

Due to the unsatisfactory conditions of the EU-US TFTP agreement, there are proposals to install a proper EU-TFTS (European Terrorist Financing Tracking System). The main argument in favour of the EU system is that with an EU-TFTS, the analysis of bank data could take place within the borders of the EU, EU intelligence services could improve their analytical capabilities and a more targeted transfer to the US could take place.[283] Article 11 of the EU-US TFTP anticipates this possibility. According to this provision, if the EU decides to establish an EU-TFTS, the US "shall cooperate and provide assistance and advice" with regard to the EU system.[284] Changes to the current EU-US TFTP Agreement would then be necessary.

a) Discussion about changing the EU-US TFTP in favour of an EU-TFTS

In November 2013 the Commission carried out an impact assessment concerning this possibility and came to the conclusion that an EU-TFTS system would be too costly and "data intrusive".[285] Therefore, the status quo (the EU-US TFTP Agreement) should be maintained.[286] The scenarios of *amending* (option A) or *terminating* (option B) the current EU-US Agreement were briefly mentioned by the Commission, but then not assessed and finally discarded for several reasons.

---

[279] DRD Judgement, para 35.

[280] ECtHR, Weber and Saravia v. Germany, No. 54934/00 of 29 June 2006.

[281] Compare to the requirement of notification: Boehm/de Hert, European Journal of Law and Technology, Vol. 3, No. 3, 2012.

[282] DRD Judgement, para 37.

[283] Communication from the Commission to the European Parliament and the Council – A European terrorist finance system (EU TFTS), COM(2013) 842 final and its accompanying impact assessment.

[284] Article 11 EU-US TFTP Agreement 2010.

[285] It was not specified what „data intrusive" actually means.

[286] Executive summary of the impact assessment accompanying the document A Communication from the Commission to the European Parliament and the Council – A European terrorist finance system (EU TFTS), COM(2013) 842 final, SWD(2013) 489 final of 27 November 2013, p. 10.

This non-assessment of the two options has already been criticised by the EDPS[287], but shall be briefly reviewed here. The arguments identified by the Commission as reasons not to analyse option A and B any further, refer, with regard to option A, to "the fact that this option depends on the consent of a third country" and that this option "would also not have a guaranteed positive impact on ensuring the full protection of fundamental rights".[288] The argument with regard to new negotiations in case of possible amendments to the current TFTP seems to be rather pre-textual, to avoid a thorough assessment of the current agreement, which would most certainly reveal the fundamental compliance issues that exist with EU data protection requirements mentioned above.

Option B was considered having too negative consequences for EU intelligence agencies. The Commission only mentioned the interest of EU intelligence in obtaining TFTP analysis from the US counterparts that would have been less frequently shared, if the Agreement was to be terminated. The Commission worried that "it may be unlikely that the US would accept requests for searches from the EU and Member States and/or provide leads spontaneously" if the Agreement were terminated.[289] None of the arguments concerning option A or B mention the positive effect an amendment or the termination of the EU-US TFTP Agreement would have on fundamental rights. Thus there was no proportionality test carried out in connection with the two more privacy friendly options. An impact assessment, however, should discuss and balance the different interests at stake in a comprehensive manner.[290] But the report of the Commission almost completely ignored the most privacy friendly solutions, providing only a superficial analysis of the two options. No in-depth debate about amendments or the termination of the EU-US TFTP Agreement has taken place. In this regard, the DRD Judgement necessitates a reassessment of the EU-US TFTP Agreement, including a serious and comprehensive necessity and proportionality test evaluating all possible options, including privacy friendly amendments as well as the termination of the EU-US TFTP Agreement.

b) General remarks on the EU-TFTS proposal

As mentioned above, in its impact assessment the Commission evaluated different options to start an EU-TFTS and came to the general conclusion that, for the time being, the establishment

[287] EDPS comments on the Communication from the Commission to the European Parliament and the Council – A European terrorist finance system (EU TFTS), COM(2013) 842 final and its accompanying impact assessment of 17 April 2014.

[288] Communication from the Commission to the European Parliament and the Council – A European terrorist finance system (EU TFTS), COM(2013) 842 final, p. 21.

[289] Communication from the Commission to the European Parliament and the Council – A European terrorist finance system (EU TFTS), COM(2013) 842 final, p. 22.

[290] D. Wright/de Hert, Privacy Impact Assessments, Springer 2012.

of an EU TFTS would be too costly and data intrusive.[291] It found that currently there are not enough technical capabilities to establish such a system in the EU.[292]

Having excluded the two best options from a data protection point of view, the Commission recommends keeping the current EU-US TFTP Agreement. In light of the considerations above, the language used to describe the current functioning of EU-US TFTP seems to be more than optimistic, even euphemistic. The report declares that the current system "is proper functioning" and there are "robust control measures" in place as well as safeguards to guarantee that individuals' rights, "including those on personal data protection, are duly respected".[293] Apart from these very general statements – which are not necessarily in line with the assessments of the EU-US TFTP Agreement performed by other actors (such as the EDPS or the Article 29 Working Party)[294] – there is no systematic and comprehensive assessment of the question whether the current agreement is proportionate and necessary with regard to EU data protection requirements. Now, after the DRD Judgement, this assessment seems to be all the more necessary and should be carried out as soon as possible, considering the impact of the new case law.

This assessment seems also to be necessary when looking at the different reasons for the EU and the US to establish a TFTP or TFTS. The objective of the US TFTP is clearly related to the detection, prevention and/or investigation of global terrorism, mainly from Islamist groups. The aim of the EU-TFTS would however be different due to a different threat scenario. In the EU, terrorist movements "mainly come(s) from separatist, religiously inspired, left-wing and anarchist terrorists".[295] The threat in the EU is therefore "quite different from the threat to the US".[296] The EU is rather faced with a regional form of terrorism[297], whereas the US faces more global menaces.[298] The outcomes of the US-TFTP analyses are therefore only partially helpful in detecting EU-related forms of terrorism. This very different threat scenario, which is important

---

[291] Executive summary of the impact assessment accompanying the document A Communication from the Commission to the European Parliament and the Council – A European terrorist finance system (EU TFTS), COM(2013) 842 final, SWD(2013) 489 final of 27 November 2013, p. 10.

[292] Executive summary of the impact assessment accompanying the document A Communication from the Commission to the European Parliament and the Council – A European terrorist finance system (EU TFTS), COM(2013) 842 final, SWD(2013) 489 final of 27 November 2013, p. 6.

[293] Executive summary of the impact assessment accompanying the document A Communication from the Commission to the European Parliament and the Council – A European terrorist finance system (EU TFTS), COM(2013) 842 final, SWD(2013) 489 final of 27 November 2013 p.6-7.

[294] For instance: EDPS comments on the Communication from the Commission to the European Parliament and the Council – A European terrorist finance system (EU TFTS), COM(2013) 842 final and its accompanying impact assessment of 17 April 2014.

[295] Communication from the Commission to the European Parliament and the Council – A European terrorist finance system (EU TFTS), COM(2013) 842 final and its accompanying impact assessment, p. 11.

[296] Communication from the Commission to the European Parliament and the Council – A European terrorist finance system (EU TFTS), COM(2013) 842 final and its accompanying impact assessment, p. 11.

[297] Compare the figures mentioned by the Commission in its Communication COM(2013) 842 final, p. 7: there have been 1359 terrorists attack in the EU between 2007-2009, but only 4 related to global terrorism.

[298] Communication from the Commission to the European Parliament and the Council – A European terrorist finance system (EU TFTS), COM(2013) 842 final and its accompanying impact assessment, p. 7: "Europol's TE-SAT 2011 report indicates that, in 2010, in 9 Member States, 249 terrorist attacks were completed, failed or foiled, of which 160 as part of separatist terrorism, 45 by left-wing terrorism and 3 by Islamist affiliations."

for the justification of the interference with fundamental rights, should be duly considered when assessing the necessity of the EU TFTS and also of the EU-US TFTP.

In the framework of the impact assessment at hand, the options finally tested by the Commission include systems at EU level, such as a data retention regime for all payment transactions providers with the possibility for LE to access these data. In particular the latter option seems to be similar to the now void DRD.

Moreover, this option would include even more data than the current solution in which only data from one provider (S.W.I.F.T.) are analysed.[299] If the EU establishes such a system, plans exist to extend the retention requirement to the other payment providers as well.[300]

In particular, the structure of the retention system and the persons concerned – bulk data collection concerning every person making a bank transfer – seems to be very similar to the data retention regime, which was declared void by the Court in the DRD Judgement. An EU-TFTS would certainly seriously interfere with Article 7 and 8 CFR by, *inter alia*, contradicting the purpose limitation principle through the use of bank transfer data for LE purposes. Moreover, it would concern the entire EU population and cover, just as the DRD did in the comparable context, in a generalised manner, all persons making a bank transfer. In addition, the Court required a relationship between the purpose of retention and the threat to public security.[301] Such a link cannot, however, be established when using and processing bulk data of unsuspicious persons, as would be possible in the proposed EU-TFTS.

3. Key findings

The current EU-US TFTP should be reassessed in light of the DRD Judgement, in particular with regards to the necessity and proportionality of bulk data transfer. The CJEU requires a link between the data retained and a threat to public security as well as independent oversight. The current system of EU-US TFTP Agreement does not comply with these requirements. In particular, the transmission of bulk data of unsuspicious persons and the subsequent storage in the US as well as the supervision of the access to the S.W.I.F.T. database through a LE agency, contradict the basic tenets of the DRD Judgement.

For these reasons, the possibility to amend or terminate the current Agreement should be seriously considered, even if this requires a renewal of negotiations with the US.

The establishment of an EU-TFTS merits special consideration, particularly with regards to whether the already unsatisfactory and legally questionable EU-US TFTP Agreement should serve as the basis for a similar mass data retention system at EU level.

---

[299] Executive summary of the impact assessment accompanying the document A Communication from the Commission to the European Parliament and the Council – A European terrorist finance system (EU TFTS), COM(2013) 842 final, SWD(2013) 489 final of 27 November 2013, p. 8.

[300] Communication from the Commission to the European Parliament and the Council – A European terrorist finance system (EU TFTS), COM(2013) 842 final and its accompanying impact assessment, p. 11 et seq.

[301] DRD Judgement, para 59.

III. Impact on Eurodac

Regulation (EU) No. 603/2013 on the establishment of Eurodac[302] includes the right for Member States' LE authorities and Europol to access Eurodac data for LE purposes. Just like the other measures mentioned above, the Eurodac database was initially not created for LE purposes, but to determine the Member State that is responsible for the examination of an asylum application. There are several issues that may raise concern when taking the Court's DRD Judgement into account.[303]

1. Verifying the Access to Eurodac data

The Regulation does not give the LE agencies direct access to Eurodac, but provides for a National Access Point acting as an intermediary that communicates with the Central System. One or several "verifying authorities" at the national level examine whether the access conditions laid down in Regulation 603/2013 are met. If they are, the authority forwards the request for the comparison of fingerprints to the National Access point. Such verifying authorities are, however, authorities responsible for "the prevention, detection or investigation of terrorist offences or of other serious criminal offences"[304] and therefore do not represent independent courts or independent authorities as required by the Court in the comparable context of the DRD Judgement.[305]

In addition, the *same* national LE authority which is authorized to request the comparisons with Eurodac can act as the verifying authority on the condition that the "the verifying authority shall act independently" and "shall not receive instructions" from the requesting authority "as regards the outcome of the verification".[306] In practice, the operating unit requesting the data should not be the same unit acting as the verifying authority, but nonetheless, they can be part of the same organization. This is also true with regard to the access of the EU LE agency Europol. "Duly empowered Europol officials" should verify whether Europol complies with the access conditions. As a result, LE authorities themselves can determine the lawfulness of their own access requests. Requesting and verifying authorities are part of the same LE agency. This "double-function" of the LE authorities – being the requesting and approving authority at the

---

[302] Regulation No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' LE authorities and Europol for LEpurposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast).

[303] Compare also: Guild/Carrera, pp. 12 et seq.

[304] Article 6 (1) Regulation No. 603/2013.

[305] DRD Judgement, para 62.

[306] Article 6 (1) Regulation No. 603/2013 that stipulates that "the designated authority and the verifying authority may be part of the same organization, if permitted under national law".

same time – clearly contradicts a proper system of checks and balances[307] and cannot replace control by a court or another independent authority.

2. Storage period and proportionality

Eurodac primarily does not serve LE purposes and therefore includes a rather long data storage period amounting to a period of up to ten years for data relating to applicants for international protection and 18 months for persons arrested in connection with the irregular crossing of an external border.[308] The retention requirement applies to every person of at least 14 years of age. Therefore the Eurodac database includes the fingerprint data of minors. During this data storage period, LE agencies can request access to the data sets.[309] This specific structure of Eurodac actually results in a database storing fingerprint information of a particularly vulnerable group of persons, which are not suspected of any crime, for a very long period of time and keeping the data, including those of minors, constantly available for LE purposes. This set-up is unique in the EU, as will be shown in the following.

There is no other EU-wide database storing biometric data of non-suspected persons for such a long period of time and holding them available for LE purposes. Databases storing biometric data at national level exist, but where they do, they are usually limited to the storage of data of criminals, such as the UK National Criminal Intelligence DNA Database (NDNAD) that was subject of the *S. and Marper v. UK* case of the ECtHR.[310] In that case, the storage of fingerprint data of two innocent minors was regarded by the Court as not being necessary in a democratic society. The stigmatizing effect, the violation of the presumption of innocence, the very long storage period, as well as the retention of biometric data of minors were persuasive arguments leading to the conclusion of a violation of Article 8 ECHR. The CJEU referred to this ECtHR case in its DRD Judgement and heavily criticised a retention period that was comparably much shorter, ranging from six months to two years.

The arguments used in the DRD Judgement and in the *S. and Marper v. UK* case can also be invoked with regard to the LE access to Eurodac. Although the main purpose of the Eurodac database does not serve LE purposes, Regulation 603/2013 still establishes the possibility of access in specific cases to data that are stored for up to 10 years, including data of minors. It is exactly this change of the initial purposes that breaches the principle of purpose limitation and can easily have a discriminatory effect on asylum seekers. If one compares the situation of asylum seekers to EU citizens and imagines (in the abstract) that the EU would plan to establish an EU-wide biometric database of data of EU citizens, including minors, with a storage period of 10 years and access provided for LE, strong opposition against such a project would be very likely. Even though the reason for retention is different, the blanket and wide-ranging retention

[307] EDPS Opinion of 5 September 2012, para 50.

[308] Article 12 and 16 Regulation No. 603/2013.

[309] If the data are once transferred to a LE agency and are then not required for the purpose of the specific ongoing investigation, they must be erased after one month (Article 33 (5) Regulation No. 603/2013).

[310] See above, *S. and Marper*.

resembles what was criticized in the DRD Judgement. With respect to these two situations, the CJEU's DRD Judgement raises strong doubts regarding the compatibility of the current LE access to Eurodac.

3. No distinction between different categories of data

Further, Regulation 603/2013 does not make any distinction between the different categories of data and access to them. Data of minors, victims of crime or perpetrators can be accessed and stored under the same conditions. In this context, it should be considered that the persons concerned already represent a particularly vulnerable group. Not making any distinction with regard to the storage period and the access conditions is not in line with the DRD Judgement.[311]

4. Key findings

The LE access to a database that initially serves other purposes seems to be a general tendency in EU law. The access of LE authorities to Eurodac is only one example for this trend, one can also compare the Entry-exit, PNR and TFTP/TFTS instruments. In view of the DRD Judgement which is subject of this study, the following points are particularly striking:

Access control to the Eurodac data is exercised by a LE authority. This practice clearly contradicts the DRD Judgement in which the CJEU required that a court or an independent administrative body able to limit the access to the data initially collected for non-LE purposes decides on access requests to avoid abuse and unlawful access.

As Eurodac was set up in a non-LE context, the storage period of Eurodac data amounts up to a period of 10 years, including data of minors. During this period, data can be accessed by LE. This retention period may be justified in light of the initial purpose of Eurodac. However, the extension of its use to LE necessitates a re-assessment of this retention requirement, especially with regard to the criticism issued in the DRD Judgement in this context. Further criticism relates to the lacking distinction between different categories of data. There is for instance no distinction made between data of minors, victims of crime or perpetrators regarding the access condition of LE and the storage period.

IV. Impact on Entry-Exit System and Smart Borders

The smart border initiative aims at controlling the external borders of the EU. Several measures serving this purpose are already in place. Others are planned. One of the latest proposals in this context is the establishment of an entry-exit system (EES) that complements the already existing Schengen Information System (SIS II) and the Visa Information System (VIS).[312] The new EES

[311] DRD Judgement, para 63.

[312] Proposal for a regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union, COM(2013) 95 final. The VIS is an EU database storing the fingerprint data of visa applicants to avoid multiple visa applications in the different Member States. The SIS II serves mainly LE purposes and was established for

would be an additional tool to collect further data in the context of EU border control. It consists of an electronic system that stores all ten fingerprints of all third-country travellers to the Schengen area. Within this system, frequent and business travellers should profit from a so called "Registered Traveller Programme" (RTP) that facilitates fast-track entry to the Schengen Area for pre-approved third country nationals.

While the establishment of the EES can be criticised from various angles going beyond the format of this study, the following section briefly examines the EES in light of the DRD Judgement and the possible use of EES data for LE purposes.[313]

1. Possible use for LE purposes

The aim of the EES is to discover so-called "overstayers", third country nationals who stay in the EU longer than permitted (usually three months are allowed for a short stay). According to statistics, third country nationals amount to roughly 150 million persons every year.[314] The EES would therefore create a huge centralised EU-database with millions of data of third country nationals. So far the data use is limited to the purpose of identification of overstayers and calculation of their stay. The data of overstayers should be stored for up to five years.[315] A possible use for LE purposes is provided for in Article 46 of the EES proposal as a future opportunity, depending on an initial evaluation two years after the entry into force of the system. Access from LE authorities of third countries is also intended. This possibility should be equally evaluated after two years.

2. Necessity in light of the DRD Judgement

The taking and storing of the 10 fingerprints of third country Schengen travellers must be understood in the light of the above mentioned future development. It must be considered that if the purpose of the data was solely to identify travellers and calculate their stay, two samples would likely suffice, making the recording of all ten fingerprints superfluous. However, the possible extension of purpose of the EES to LE would make having ten fingerprints valuable to LE. For example, having ten fingerprints would aid in the identification of traces of fingerprints left at crime scenes.[316] In the national laws of the Member States, the taking of all 10 fingerprints happens usually in cases where persons are suspected of a crime.[317] Constructing the EES in the currently proposed form seems to prepare the EES data for the later use for LE purposes. The third country travellers are however, not suspected of any crime and cannot therefore be treated in the same way as potential criminals. While the taking of fingerprints in

---

border control, customs and police authorities to exchange information on persons involved in crimes. The SIS II includes also data relating to missing persons or property.

[313] For a comprehensive study on this topic compare: Bigo et al.,"Study for the LIBE committee, Evaluating current and forthcoming proposals on JHA databases and a smart borders system at EU external borders", November 2012.

[314] Bigo et al., p. 35.

[315] Article 20 (3) of the EES proposal, COM(2013) 95 final. Data of other third country nationals are intended to be stored for a maximum period of 6 month.

[316] Compare also Opinion of the EDPS of 18 July 2013, p. 16, para 66.

[317] E.g. § 163b Strafprozessordnung (German Code of Criminal Procedure).

criminal proceedings may be necessary to resolve crime investigations, the legality of the same procedure for travellers appears to be doubtful at best. Treating third country travellers like suspected persons certainly has a discriminatory effect[318] and it is questionable whether this can be properly justified in light of Article 7 and 8 CFR.

3. Key findings

The concerns above highlight the importance of a comprehensive assessment of the necessity of this measure *before* collecting data such as all 10 fingerprints of all third country travellers, including the fingerprints of minors over the age of 12. Weighing this policy against the requirements of the DRD Judgement and the case law of the ECtHR is essential. The following issues must be considered in this context:

The use of biometric data is a clear interference with fundamental rights and requires a thorough analysis of the necessity of the measure. EDPS demands a "targeted impact assessment on biometrics (fingerprints)" before starting to introduce fingerprints in the EES and evaluating *ex ante* the usefulness of this function in contrast to other countries that base their entry-exit system solely on alphanumerical data.[319] This assessment is also strongly advisable to ensure the protection of fundamental rights, ideally (and legally required) through the identification of less intrusive means for the identification or calculation of stay.

In the DRD Judgement as well as in *S. and Marper v. UK* and the *M.K. v. France* case, both Courts were very critical with regard to the storage of data, including fingerprints, of unsuspected persons. The *S. and Marper* case particularly referred to the problematic retention of data of minors. This aspect needs further consideration, especially due the amount of data stored. In this context, the stigmatizing effect of having taken all ten fingerprints needs to be duly evaluated.

In addition, a detailed analysis of the purpose of the EES must be carried out. If the purpose is limited to identification and calculation of the stay, the taking of all 10 fingerprints seems unnecessary. If the establishment of the EES is only a pretext for the later establishment of a LE database, this (pre-arranged) function creep must be avoided from the outset, for instance by limiting the amount of data included in the EES.

In view of the critical remarks of the Court regarding the retention period of retained data, the 5 years storage period for fingerprint and other data of overstayers needs to be reconsidered.

[318] Compare in this sense the standards established by the ECtHR in *S. and Marper* and *M.K. vs. France*.

[319] Opinion of the EDPS of 18 July 2013, p. 15 et seq.

V. Impact on the proposal for a data protection directive in the law enforcement sector

The possible effect of the DRD Judgement on the proposal for a data protection Directive in the LE sector[320] should be briefly mentioned here. Since the legislative deliberations regarding the adoption of the proposal are an ongoing process, the following remarks do not refer to the specific wording, which is still subject to much discussion. Instead, certain contexts will be analyzed, such as independent oversight and the transfer to third countries, rules on cooperation with the private sector, profiling and key definitions.[321]

1. Independent oversight and transfer to third states

Independent and effective oversight in a law enforcement context is an evolving topic of particular importance since an investigation's results as well as potential abuses can have serious consequences for persons concerned.[322] In the context of data transfer to third states, the Court highlighted the importance of independent control and the associated risks incurred through storing data in third countries. The Court indicated that independent oversight in the sense of Article 8 (3) CFR means that data must be ideally stored in the EU.[323] Therefore, the transfer provisions in the draft Directive, and in particular the exemptions allowing for transfer without an adequacy decision, should be adapted to the requirements of the Court. This concerns, for instance, draft Article 36 which provides for considerable deviations from the adequacy requirement. The conditions currently stipulated in this article are very far-reaching and allow for example the transfer to a third state if it "is essential for the prevention of an immediate and serious threat to public security" or in other defined cases. Currently, no provisions exist that would guarantee the influence of EU data protection authorities with regard to third state transfer. Follow-up procedures, such as for instance follow-up reports to the sending authority or to the responsible data protection authority, could assure that the transferred data remain accessible to independent EU control.

The Parliament considered these shortcomings regarding Article 36 of the draft and proposed several improvements in March 2014.[324] One of them relates to the documentation of data transfer in the absence of an adequacy decision that must be then made available also to the

---

[320] Proposal for a Directive of the European Parliament and of the Council on the protection of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final.

[321] Compare: the latest amendments made by the European Parliament in a resolution of 12th of April 2014: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0219&language=EN&ring=A7-2013-0403; as well as the Council version of 28 March 2014, interinstitutional file: 2012/0010(COD), 7507/14, DAPIX 44 etc. Chapters VII-X.

[322] Article 29 Working Party, opinion 04/2014, WP 215, pp. 8 et seq; Roßnagel, MMR 2014, pp. 372-377, in particular, p. 376.

[323] DRD Judgement, para 68 and with regard to the proposal of the general data protection regulation: Roßnagel, MMR 2014, pp. 372-377, in particular p. 376 et seq.

[324] Compare: the latest amendments made by the European Parliament in a resolution of 12th of April 2014: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0219&language=EN&ring=A7-2013-0403

supervisory authority. This proposal is certainly a step in the right direction to assure compliance with the DRD Judgement. However, there is still room for other improvements in the upcoming legislative process, in particular with regard to a thoughtful review of the deviations from the adequacy requirement, to fully consider the conditions for compliance with EU law as stipulated by the Court in the DRD Judgement.

2. Rules on cooperation with the private sector

One of the key questions in the DRD Judgement concerned the problem of access to data collected by private parties for a specific purpose that are then later used for LE purposes. It is crucial to point out that this change in purpose seriously infringes one of the most important data protection principles, namely purpose limitation. This in turn makes the addition of specific, clear rules and safeguards imperative to limit the serious infringement caused. According to the Court the rules on cooperation between the public and the private sector must include "substantive and procedural conditions relating to the access" of LE authorities as well as rules relating to the subsequent use of the accessed data.[325] These rules must assure "that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto".[326] The Court has developed detailed criteria that relate to objective rules determining the number of persons authorised to access as well as to rules assuring that the subsequent use is "limited to what is strictly necessary in the light of the objective pursued".[327] Additionally, the Court demanded a prior and independent review of the access to private sector data to ensure that the access is limited to what is strictly necessary.[328] The statements above clearly express the need for precise rules on public-private cooperation in the LE sector in order to comply with the DRD Judgement. At the moment, the draft of the Commission does not entail said rules. Again, it was the Parliament that proposed rules in this regard in its resolution of March 2014. A new Article 4a should regulate the access to data initially processed for non LE purposes.[329] Recital 65a (new) relates to the transmission of personal data to private parties.[330] These proposals should now be extended and adapted to the mentioned requirements of the Court.

3. Profiling

The DRD Judgement will impact the planned provisions regarding profiling. So far, Article 9 of the draft Directive deals with measures based on profiling and automated processing. The Court noticed that profiling measures allow the drawing of precise conclusions concerning the private

[325] DRD Judgement, paras 60 et seq.

[326] DRD Judgement, para 61.

[327] DRD Judgement, para 62.

[328] DRD Judgement, para 62.

[329] Compare: the latest amendments made by the European Parliament in a resolution of 12th of April 2014: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0219&language=EN&ring=A7-2013-0403.

[330] Ibid.

lives of individuals.[331] The mix data of suspicious and unsuspicious persons can lead to an undifferentiated treatment of the persons concerned, an outcome that the court heavily criticized.[332] In addition, attention must be paid to the stigmatizing effect that LE measures, and in particular profiling measures, can have on unsuspicious persons. The Court also referred to the impact of data retention and possible profiling measures resulting from the use of this data on the society as a whole. These measures have the capacity "to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance".[333] Therefore, the use and analysis of metadata in the DRD Judgement constituted a particularly serious interference with fundamental rights necessitating the Court to point to the need for special safeguards in this context.[334] The framing of the future profiling provision in the draft Directive must reflect these concerns and provide for strong safeguards against the indifferent treatment of suspicious and unsuspicious persons, as well as unlawful access and abuse.

4. Definitions of key terms

The importance of defining key terms is another requirement that can be derived from the DRD Judgement. The court insisted that terms such as "serious crime" be defined, including when a crime would justify an intrusion into fundamental rights. Referring only to general terms and leaving key definitions to Member States does not necessarily meet the proportionality test at EU level.[335] In other words, if the EU introduces a measure restricting fundamental rights, it bears the responsibility to limit associated interference to what is strictly necessary and proportional by defining key elements. Leaving this essential step to the Member States is not compliant with EU law.

This is important not only in the light of the draft Directive, but also with regard to the other EU measures mentioned above. If framing provisions of the future Directive were to allow Member States to restrict fundamental rights, the limits of these restrictions should be clear and precise. One example of such a necessary specification could be a European-wide definition of serious crime that would list specific offences. As "serious crime" constantly serves as a legal basis for the restriction of Articles 7 and 8 of the Charter[336], the DRD Judgement could serve as a good starting point to begin a discussion toward a common understanding of this notion.

5. Key findings and general remarks

Although the impact on the future data protection Directive in the LE sector is only briefly touched upon here, a general assessment of this (draft) instrument's compatibility with the DRD Judgement must be carried out. This assessment should include the points mentioned above. In

[331] DRD Judgement, para 27.

[332] DRD Judgement, para 55 et seq.; compare also Article 29 Working Party, opinion 04/2014, WP 215, pp. 4 et seq.

[333] DRD Judgement, para 37.

[334] DRD Judgement, para 55.

[335] DRD Judgement, para 60 et seq.

[336] Compare for instance the measures mentioned above and Guild/Carrera, pp. 8 and 14 with further references.

addition to the verification of definitions of key terms, the provisions on independent oversight should be reviewed, which are of particular importance in a LE context. Further, the question of whether the existing provisions reflect the Court´s understanding of effective and independent oversight must be checked. The link between third state transfer and effective supervision needs to be considered in detail. The rules on profiling and the risk of stigmatization as well as the legal status of any cooperation with the private sector, including access control through an independent intermediary, are further important issues in that regard. Above all, any change in purpose needs to be considered more intensively and it must be guaranteed that any change in purpose be limited to the strictly necessary and preserves compliance with the proportionality criterion.

In addition to the mentioned topics, the rights applying to individuals in a LE context need to be taken into account more seriously. This includes the verification of the provisions governing the different categories of data, for instance the question of whether the difference between suspicious and unsuspicious persons has been duly considered in the proposal. Finally, it must be assured that possible data retention periods are limited to what is strictly necessary to attain the objective pursued.

VI. Interim conclusion

Chapter E analysed the impact of the DRD Judgement on seven exemplary EU measures that provide to some extent for data retention measures, with the exception of the proposal for a data protection directive in the LE sector. One essential outcome of the analysis is that all the measures have considerable shortcomings when comparing their content to the DRD Judgement of the Court. The most striking discrepancy with the Court's understanding relates to the still prominent opinion that bulk data collection and transfer of data of unsuspicious persons is in line with fundamental rights. The Court clearly opposed this position by requiring a link between the data retained and a threat to public security. This understanding holds enormous consequences for existing as well as planned EU data retention measures. The rationale of measures such as the bulk transfer of PNR as well as bank data (TFTP) to the US and the planned EU-PNR as well as EU-TFTS systematically lack this required link and are therefore not in line with Article 7 and 8 CFR.

This link also influences the relationship between private and public actors in a LE context. The Court unambiguously demanded strong safeguards, such as independent oversight and access control to data originally collected for another purpose, thereby insisting on the fact that this change in purpose must remain the exception rather than the rule and is only compliant with fundamental rights in restricted and specific cases. Therefore, measures such as the LE access to Eurodac or the planned LE access to the EES must be subject to critical scrutiny. The current practice of access control to the data of unsuspicious persons stored in the databases that is exercised by a LE authority does not comply with the Court's requirements in any case and needs to be changed. Similar measures not being subject of this study, such as the LE access to

the Visa Information System or the Schengen Information System II, show comparable deficits and need to be tested for compliance with the DRD Judgement as well.[337]

A further important outcome of the analysis is that in all cases the EU and the Member States are obliged to demonstrate the necessity of data retention measures as well as the need to access data that are not LE related in much more detail than before. This includes a transparent proof that the data retained actually aids the resolution of (serious) crimes. The DRD Judgement also influences another subject of much debate. So far, the EU has avoided defining key terms, such as "serious crime", to allow for a broad interpretation of such terms in Member States or in third states. Now, after the Court demanded clarifications with regard to the use of data for crime prevention purposes, it is necessary to specify what is to be understood under broad umbrella terms. An EU-wide definition of what constitutes serious crime for instance seems therefore to be necessary.

The analysed subject matter has shown that several existing or planned LE measures in the EU entail similar rationales as the DRD. In particular, the mentioned PNR as well as the TFTP systems target a large amount of unsuspicious individuals. In addition, the access of LE to databases that store data for non-LE purposes has increased as well (Eurodac, EES, VIS etc.). This development has led to an increase in surveillance measures in different fields of daily life of individuals. Surveillance is taking place when making bank transfers, taking flights, travelling to the EU or applying for visas.

The impact of the increase in surveillance measures on individuals is not yet analysed in a comprehensive manner, but there are national Courts referring to this issue. In the data retention judgment of the German Constitutional Court of 2 March 2010[338] this development was mentioned. The German Court referred to the accumulation of groundless surveillance measures. As a result, if the German legislature plans to enact further data retention measures, it must consider the entirety of the already existing databases and take into account the situations in which individuals are already confronted with surveillance.[339] The "perception of liberty" ("Freiheitswahrnehmung") of the individuals limits the margin for any other data retention measure, also at EU level.[340] The German legislature is therefore obliged to consider all existing retention measures when it plans to retain data of unsuspicious persons.

To conclude, all the measures mentioned here need to be reviewed against the background of the DRD Judgement. The stigmatising effect that data retention measures and the later use for LE purposes can have, should be duly considered when carrying out this review. Although

[337] This view is also expressed clearly in the Information Note by the General Secretariat for the Council of the European Union, 5 May 2014, para. 19-21 in which it is underlined that high levels of protection are necessary, that any mass data collection is problematic and that the Commission has to draw the consequences of the DRD Judgement for all existing, proposed and in future newly introduced legislative acts of the EU.

[338] Judgment of the German Constitutional Court of 2 March 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, cf. Gerrit Hornung and Christoph Schnabel, "Verfassungsrechtlich nicht schlechthin verboten. Das Urteil des Bundesverfassungsgerichts in Sachen Vorratsdatenspeicherung", Deutsches Verwaltungsblatt 2010, pp. 824-833.

[339] Judgment of the German Constitutional Court of 2 March 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, para 218.

[340] Ibid.

changes to instruments still in the legislative process are easier to be carried out, they are equally necessary with regard to existing instruments, too, even if this requires a possible lengthy and painful re-negotiation process with the US in case of the PNR and TFTP. Changes to all of the mentioned instruments are in any case essential to assure future compliance with fundamental rights.

F. Conclusion and Perspectives

In this conclusion the main results of the study are summarized and an outlook is provided. The first section relates to the extensive analysis of the DRD Judgement provided. The second section briefly summarizes the impact of the judgement on data retention measures in the Member States which is complemented in the third section by the impact analysis on other EU data retention measures. The final section is dedicated to perspectives stemming from this judgement and as a consequence of the results of this study.

I. The DRD Judgement of the CJEU

The recent DRD decision delivered by the Court of Justice of the European Union represents a major Judgment with significant implications. It has opened a new level of scrutiny of EU measures in light of the CFR and has raised expectations for future reviews of legislative acts. The unequivocal holding of the Court went beyond the Advocate General's Opinion in the case by not even considering a continued interim validity of the DRD before the enactment of a new Directive as he had suggested, but by clearly stating its invalidity from the beginning. The Court's analysis in the judgement is characterized by several important statements that are essential for the current and future discussion about data protection and privacy in a LE context and therefore go beyond the mere consequence for the original DRD. The Court clearly opposed the general and indiscriminate nature of the measure foreseen by the DRD.

One essential outcome of the DRD Judgement relates to the interaction between the right to data protection and the right to private life in data protection cases. The Court clarifies that data retention measures touch upon both Article 7 and 8 CFR. One important implication for the future structure of these two fundamental rights is the acknowledgement that a single measure, such as data retention or similar cases can simultaneously infringe on both rights. These rights are interlinked and require a detailed and strict test with respect to the necessity and proportionality of any relevant data storage.

Of possibly rather symbolic significance is the fact that the CJEU felt the urge to assess whether even the essence of Article 7 and 8 CFR was violated by the provisions of the DRD. Symbolic, because it quickly concedes that the essence is not violated, but nonetheless striking as it is the first time the Court actually analyses this point in a fundamental rights case since the CFR has gained binding value with entry into force of the Lisbon Treaty. The explanation the Court provides for the lack of a violation of the essence of rights is as follows: concerning Article 7 CFR the lack of storing obligations of the content of communication is regarded as being sufficient to meet the "respecting the essence test"; in regard to Article 8 CFR the Court is satisfied with the existence of technical safeguarding measures and security against unlawful access, modification or destruction of the retained data whilst it does not expect particular requirements to be met in order to be appropriate and respecting the essence.

In addition, the Court referred – in contrast to the Advocate General – frequently to the guarantees of the ECHR and the interpretation in the ECtHR case law in the context of data retention measures. By taking this approach, the CJEU has irreversibly linked the two legal orders even closer than in the past and opens the possibility to interpret Article 8 ECHR and Article 7 and 8 CFR in a parallel way. This allows the possibility to derive general conclusions on the treatment of other data retention measures in the EU as one can relate to previous decisions of the ECtHR on such comparable national measures and their impact on Article 8 ECHR. In particular, the Court included important principles in its arguments stemming from the case law of the ECtHR in cases such as the *S. and Marper v. UK* and *M.K. v. France*. Therefore, the statements of the Court do not only refer to the singular case of the DRD, but establish general principles for similar data retention measures. Statements such as the rejection of blanket data retention or an indefinite retention period are crucial for the future understanding of data retention measures in the EU.

Another parallelism to the ECtHR case law is that the CJEU considers every collection, use and transfer to another authority as being a separate interference with fundamental rights that therefore needs a separate justification. This is particularly important for the access of LE to data originally not collected for those purposes because it necessitates a reconsideration of the relationship between public and private actors in the LE sector. Analyzing data for LE purposes is a very sensitive issue and can have a serious impact on the lives of individuals. The Court reminds that "very precise conclusions" can be drawn not only from the content of communication, but also from metadata, such as the "habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them".[341] Profiling measures, for instance, influence the perception of surveillance in society and it needs to be avoided that the persons concerned have the feeling that their private lives are under constant surveillance.[342] The risk of stigmatization stemming from the inclusion of data in LE databases, which was subject of the ECtHR's *S. and Marper* case, needs to be considered and should be taken into account when reviewing other existing or planned data retention measures at EU and Member States level (e.g. PNR, TFTP, TFTS, Eurodac, EES). It should not be forgotten that the collection of the data is already the first infringement, but as mentioned this is followed by a series of further infringements that need to be justified separately.

Effective procedural rules are therefore required to protect the data of persons concerned; one example are access rules for authorities concerning data collected for other (non-LE related) purposes. Access to these data must be limited to what is strictly necessary and must stay the exception rather than the rule. Again as was the case concerning the qualification of the interference, these procedural rules that are needed are of particular importance when it comes to the cooperation between the private and the public sector in the LE context. If the government authorities seek access to data originally collected for other purposes, special

[341] DRD Judgement, para 27.

[342] DRD Judgement, para 37.

safeguards are needed. Limited data retention periods and the possibility to have the data removed from LE databases constitute further important findings of the judgement.

With this analysis the Court has made it very clear that the DRD was an instrument that did not fit into the general framework of data protection rules that need to balance infringement carefully with the goals supposedly achieved by the infringing measure. Although the Court did not give a final conclusion that data retention per se is in violation of the fundamental rights analyzed it actually has set such high standards and expectations to the necessity test that any form of blanket data retention on the EU level that is not referring to suspects or initiated on a concrete decision in every case seems not compatible with the CFR.

II. Impact on data retention measures in the Member States

Due to the standards set by the CJEU in the DRD Judgement national measures transposing the DRD need to be amended if they contain provisions similar to those of the DRD which was declared void by the Court. If the fundamental points that need to be safeguarded (as described above) are not included in the national law, thereby correcting the "wrong" template that was the DRD, then this will also impact the evaluation of the Member States' legislative act. This conclusion makes a re-assessment of national data retention laws in light of the DRD Judgement necessary.

Member States laws are under scrutiny of EU fundamental rights law as far as the measure is within the scope of application of EU law which goes beyond a mere transposition of EU law. The study has been shown that in the specific field of data retention several connection exist that directly link the national acts to the fundamental rights standards of the CFR. Not only were the national acts passed in transposition of EU law, but they also affect the realization of fundamental freedoms and therefore have to be assessed in light of the fundamental rights. Most importantly, however, for the area of data retention there is a rule in another instrument of secondary legislation of the EU that regulates the extent to which Member States can foresee national data retention schemes and that these need to be in line with EU fundamental rights.

Article 15 (1) Directive 2002/58 ("e-privacy Directive") gives Member States the possibility to exceptionally introduce data retention schemes in the electronic communications sector that deviate from the general prohibition to collect and store data beyond the reasons provided for in the other parts of the Directive. But it ties this possibility to a very strict and detailed measure of compatibility with fundamental rights standards, taking into account the formulation of Article 8 ECHR. This test of a national measure against Article 15 (1) Directive 2002/58 needs to be performed by courts on national level as well as by the CJEU if they are confronted with cases concerning national acts in the future. There are several ways how the impact of the DRD Judgement on national law could be resolved. Primarily, it is up to governments and the legislature to react to the decision by reviewing whether their national law still stands the fundamental rights test after having been provided by clear guidance of the Court, although the latter obviously only analyzed the "original", i.e. the DRD. There is no direct consequence on

national law of the declaration of invalidity by the Court, but in a case like this one, in which the Court gave a very clear and fundamental negative evaluation of a Directive, the national acts transposing the Directive are so-to-speak automatically also in suspicion of being in violation of fundamental rights.

If governments and parliaments in the Member States do not move on own initiative after this judgement, there are ways to challenge the national laws before courts which likely would lead to a similar consequence for the national law as the Court drew for the EU legislative act. In actual fact, several courts and not only one of the courts that had requested the ruling of the CJEU, have shown such reaction and declared the national law void, too.

The most promising way to have a national data retention law reviewed in light of its compliance with fundamental rights and compatibility with EU law is the initiation of legal proceedings in front of national courts, even in cases where earlier decisions were taken affirming the national law. The domestic courts must then review the national transposing act in considering respective EU law mentioned above and including Article 15 (1) Directive 2002/58. If the court has doubts about the compatibility of the national act with EU law it needs to initiate a preliminary ruling by the CJEU. Thereby, it would be back to the fundamental rights assessment which it already did in detail in the DRD Judgement and therefore most likely the outcome for the national law would be the same as it was for the Directive, even though the Court would possibly leave this conclusion to be drawn by the national court.

An alternative would be to use the path to Strasbourg. Individuals could claim that the national data retention scheme violates their rights stemming from the ECHR, in this case Article 8 ECHR. Evidently, this is not possible before the exhaustion of domestic remedies, but there are some cases already pending at the ECtHR which may give more broadly applicable answers also for data retention schemes in the communications sector. The interconnection between the Luxembourg and the Strasbourg Court is not one-directional. Judgements of the two courts mutually influence each other and because the CJEU in its DRD Judgement relied heavily on the interpretation of Article 8 ECHR by the ECtHR it is more than likely that the Strasbourg Court would come to the same or similar conclusions with regard to national data retention measures as did the CJEU for the EU Directive.

Other possibilities to have national data retention laws reviewed include the initiation of infringement proceedings against a Member State because of violation of EU law. This procedure is commonly used by the Commission (according to Article 258 TFEU, theoretically also by a Member State against another according to Article 259 TFEU) against Member States for incomplete or wrongful transposition of EU law or because of taking measures that are in violation of EU law. As shown above, the data retention laws in the Member States are likely to be also in violation of EU fundamental rights. For this reason the Commission ought to at least analyze whether starting infringement procedures against States that refuse to change their national laws to bring them in line with the requirements of the DRD Judgement is necessary. The Commission can act on its own behalf or after being called upon by external sources such as individuals and there are political pressure instruments that can be used if no action is taken

although these do not necessarily lead to a consequence. Theoretically, proceedings for failure to act could be initiated against the Commission in the case it does not act against Member States (Article 265 TFEU) but the requirements are high and it is unlikely this would lead to a result. The lack of a review mechanism open to individuals and concerning legislative acts on EU level, shows once more the problematic consequence in a case such as the DRD.

III. Impact on other data retention measures in the EU

The impact of the DRD Judgement is crucial when looking at the consequences for other data retention measures that provide similar forms of mass data collection and targeting of unsuspicious individuals. The study therefore tested seven exemplary EU measures on compatibility with the standards set by the DRD Judgment, namely the EU-US PNR Agreement, the EU-PNR proposal, the EU-US TFTP Agreement, the EU TFTS proposal, the LE access to Eurodac, the EES proposal and the draft data protection directive in the LE sector. All analyzed measures provide for data retention and affect an enormous amount of (unsuspicious) individuals. Some of the measures seem to be even more infringing than the DRD was.

The compatibility test revealed fundamental compatibility problems, in particular when it comes to indiscriminate bulk data collection and transfer of flight passenger and bank data to the US (PNR and TFTP Agreement). This holds true additionally for the respective plans to establish similar systems at EU level (EU-PNR as well as EU-TFTS). The rationale of these measures contradicts in essential points the DRD Judgement's findings. The Court required a link between the data retained and a threat to public security that cannot be established if the data of unsuspicious persons is retained in a bulk.

The required link significantly influences the relationship between private and public actors in a LE context. The Court unambiguously demanded strong safeguards such as independent oversight and access control to data originally collected for another purpose. In addition, access to data originally not collected for LE purposes should be restricted to specific cases. However, the PNR and the bank data transferred to the US can be used for various purposes. Further shortcomings relate to the missing independent access control. None of the PNR or the TFTP/S systems have an independent oversight mechanism in place and contradict the Court's requirements. The same is true with regard to Eurodac and the draft EES. Access control is currently exercised by a LE authority and not by an independent body as required by the Court. Therefore the current practice of access control to the data of unsuspicious persons transferred to the US or stored in EU databases urgently needs restructuring. Within this process the concerns of the Court with regard to the independent control of data of EU citizens transferred to third states must be taken into account.

In addition to the mentioned shortcomings, further need for review concerns the necessary establishment of clear limits to the retention period. This is of particular importance in the cases of the EU-US PNR, EU-PNR and the TFTP/S systems as well as with regard to Eurodac where LE is allowed to access data not collected for LE purposes for a very long period of time, partly up to

ten years and beyond. The Court demanded objective criteria to ensure that the period is "limited to what is strictly necessary".[343] This test has not been carried out yet and must therefore be part of the review process.

To sum up, the analysis has shown the urgent need for action in light of the amount of EU measures potentially violating Article 7 and 8 CFR. All measures need to be reviewed against the background of the DRD Judgement. Similar measures not being subjected to this study, such as the LE access to the Visa Information System or the Schengen Information System II, show comparable deficits and need to be tested for compliance with the DRD Judgement as well. The Commission is therefore called upon to carry out this work.

IV. Concluding Perspectives

To conclude, the analysis has demonstrated the far-reaching impact of the DRD Judgement. Essential is that the blanket retention data of unsuspicious persons for the later use for LE is not in line with Article 7 and 8 CFR since it is not possible to establish a link between the data retained and a threat to public security. For any other possible future data retention measure, the EU as well as the Member States are obliged to demonstrate the necessity of the measures in every single case. In addition, the need to access data that are not LE related has to be established in much more detail than it was done in the DRD. This requires a solid proof that the data are necessary for LE purposes to avoid unnecessary data collection from the outset.

A further important outcome for EU policy making is that if the EU enacts measures infringing Articles 7 and 8 CFR, it needs to define key terms that justify the infringement, such as the use of the data for serious crime purposes to avoid a diverse interpretation of such key terms in the EU Member States.

Moreover, the principles of the DRD Judgement also require a review of measures with the same rationale (PNR, TFTP, TFTS, LE access to EES, Eurodac, VIS). The EU bodies, in particular the Commission, must review the existing and planned data retention measures and duly consider the DRD Judgement. This concerns the seven measures analysed in the study, but similar instruments, too, such as the VIS and the SIS II as well as the possibilities offered to Europol. In addition, the DRD Judgement offers input for the debate about data protection standards in third states. The principles of the DRD Judgement require a review and re-negotiation of international agreements (EU-US PNR and EU-US TFTP) since these agreements do not comply with the DRD Judgement, even if this may result in painful and lengthy discussions with third states. It is not unlikely that in the near future the ECtHR will decide on a case that concerns the transfer of data to third countries or access to data by foreign intelligence units. Furthermore, the CJEU will have the opportunity to discuss the question of transfer of data to outside the EU further in the preliminary ruling initiated by the Irish High Court in June concerning the Safe Harbour Agreement with the US, in which the referring Judge considers inter alia whether the

[343] DRD Judgement, para 64.

situation has to be re-assessed after entry into force of the CFR.[344] This development shows that the DRD Judgement calls for a review of measures taken under other parts of EU data protection law as they can similarly impact the position of individuals.

Further, the judgement necessitates a redefinition of the relationship between public and private actors with regard to mutual data access and exchange. Rules on this relationship could be integrated in the draft Data Protection Directive in the LE sector. The same instrument should reflect the stigmatising effect that data retention measures can have. Rules to protect unsuspicious individuals need to be introduced in that proposal and generally spoken the need to reform the data protection framework of the EU has become even more evident with the DRD Judgement. In that context one should remember what the German Federal Constitutional Court has said and what the CJEU in its judgement alludes to: that with the technological possibilities available and the collection of data taking place in an overall manner by public and private institutions and entities, when considering a measure one should do a stock-taking that evaluates the measure in its place of the overall situation. A vague feeling of constant surveillance, as it has been phrased, may impact communication behaviour and certainly seems to be in contradiction to the framework set by constitutional fundamental rights on Member States and EU level.

[344] Cf. The High Court in re. Maximilian Schrems v. Data Protection Commissioner, 2013 No. 765 JR, Judgement delivered on 18 June 2014 to stay the proceedings, available at Europe-v-facebook.org.

G. Bibliography

Books, journal articles and other contributions

Ambrock — Die Übermittlung von S.W.I.F.T.-Daten an die Terrorismusaufklärung der USA, Duncker & Humblot, Berlin 2013

Bigo et. al. — Study for the LIBE committee, Evaluating current and forthcoming proposals on JHA databases and a smart borders system at EU external borders", November 2012

http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462513/IPOL-LIBE_ET%282012%29462513_EN.pdf

Boehm — European Flight Passenger Under General Suspicion – The Envisaged Model of Analysing Flight Passenger Data, in Gutwirth et al, Computers, Privacy and Data Protection: An Element of Choice, Springer 2011, p. 171-199.

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, Berlin 2011

Boehm/de Hert — Notification, an important safeguard against the improper use of surveillance – finally recognized in case law and EU law, European Journal of Law and Technology, Vol. 3, No. 3, 2012

http://ejlt.org/article/view/155/264

Cole/Boehm — EU Data Retention – Finally Abolished? – Eight Years in the Light of Article 8, CritQ, 1/2014, 58

De Vries — 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.

Eder/Schiltz — EU will keine neuen Regeln für Vorratsdaten, DIE WELT-online, 4 June 2014

http://www.welt.de/politik/ausland/article128698101/EU-will-keine-neuen-Regeln-fuer-Vorratsdaten.html

Fink/Cole/Keber Europäisches und Internationales Medienrecht, C.F. Müller, Heidelberg 2008

Fučík Czech Republic: New Regulation on Data Retention, IRIS 2012-9:1/15

http://merlin.obs.coe.int/article.php?id=13910

Giegerich, Thomas Spät kommt Ihr, doch Ihr kommt: Warum wird die Grundrechtskonformität der Vorratsdatenspeicherungs-Richtlinie erst nach acht Jahren geklärt?, ZEuS 1/2014

Guild/Carrera The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive, CEOS paper in: Liberty and Security in Europe, No. 65/May 2014

Hornung/Boehm Comparative Study on the 2011 draft Agreement between the Unites States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security, 14 March 2012

http://www.uni-muenster.de/Jura.itm/hoeren/itm/wp-content/uploads/PNR-Study-FINAL-120313.pdf

in't Veld (Rapporteur) Recommendation on the draft Council decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, 17433/2011– C7-0511/2011–2011/0382(NLE), 3 April 2012

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2012-0099+0+DOC+PDF+V0//EN

Järvinen Summary of the Danish Ministry of Justice's legal analysis of the CJEU Judgement, 4 June 2014

http://edri.org/denmark-data-retention-stay-despite-cjeu-ruling/

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

http://epubs.surrey.ac.uk/282571/

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.

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

Manolea Balancing the interests in the context of data retention (INVODAS) – Romania

http://www.emr-sb.de/tl_files/EMR-SB/content/PDF/Gutachten%20Abgeschlossene/INVODAS_Country%20Report%20Romania.pdf

Priebe Reform der Vorratsdatenspeicherung – strenge Maßstäbe des EuGH, EuZW 2014, 456

Robinson Accelerating the Secondary Use of Commercial Data by Law Enforcement through E.U. legislation – A Search for Core Values (manuscript, in preparation for publication)

Roßnagel Neue Maßstäbe für den Datenschutz in Europa – Folgerungen aus dem EuGH-Urteil zur Vorratsdatenspeicherung“, MMR 2014, 372-377

Roßnagel/Moser-Knierim/Schweda Interessenausgleich im Rahmen der Vorratsdatenspeicherung, Nomos 2013.

Tung Four of Sweden's telcos stop storing customer data after EU retention directive overthrown, 11 April 2014

http://www.zdnet.com/four-of-swedens-telcos-stop-storing-customer-data-after-eu-retention-directive-overthrown-7000028341/

Wilkens Vorratsdatenspeicherung: EU-Kommission zieht Klage gegen Deutschland zurück, Heise, 7 May 2014

http://www.heise.de/newsticker/meldung/Vorratsdatenspeicherung-EU-Kommission-zieht-Klage-gegen-Deutschland-zurueck-2184019.html

Wright/de Hert Privacy Impact Assessment, Dordrecht, Springer 2012

Legislative and Administrative Documents

Article 29 Data Protection Working Party Opinion 09/2004 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 (Document of the Council 8958/04 of 28 April 2004)], WP 99, 9 November 2004

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp99_en.pdf

Article 29 Data Protection Working Party Opinion 7/2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries, WP 178, 12 November 2010

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp178_en.pdf

Article 29 Data Protection Working Party Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, WP 215, 10 April 2014

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf

Council of the European Union

Information Note from the General Secretariat of the Council to the permanent Representatives of Committee/Council, 9009/14, 5 May 2014

http://www.statewatch.org/news/2014/may/eu-council-note-data-retention-judgment-9009-14.pdf

Council of the European Union

Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime - The possible inclusion of intra-EU flights, Interinstitutional File: 2011/0023 (COD), 28 March 2011

http://www.nopnr.org/wp-content/uploads/2011/05/eu-council-eu-pnr-intra-eu-flights-8016-11-28032011.pdf

Council of the European Union

Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offence including terrorism, Council doc. 8958/04, Brussels, 28 April 2004.

European Commission

Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, COM(2007) 654 final, 6 November 2007

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0654:FIN:EN:PDF

European Commission

Communication from the Commission to the European Parliament and the Council – A European terrorist finance tracking system: available options, COM(2011) 429 final, 13 July 2011

http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com%282011%290429_/com_com%282011%290429_en.pdf

European Commission

Proposal for a Directive of the European Parliament and of the Council on the protection of personal data by competent

authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, 25 January 2012

http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_10_en.pdf

European Commission Proposal for a directive of the European Parliament and the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final, 2 February 2012.

http://ec.europa.eu/home-affairs/news/intro/docs/com_2011_32_en.pdf

European Commission Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union, COM(2013) 95 final, 28 February 2013

http://ec.europa.eu/dgs/home-affairs/doc_centre/borders/docs/1_en_act_part1_v12.pdf

European Commission Communication from the Commission to the European Parliament and the Council – A European terrorist finance system (EU TFTS), COM(2013) 842 final, 27 November 2013

http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/docs/20131127_tfts_en.pdf

European Commission Executive summary of the impact assessment accompanying the document A Communication from the Commission to the European Parliament and the Council – A European terrorist finance system (EU TFTS), COM(2013) 842 final, SWD(2013) 489 final, 27 November 2013

http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/docs/20131127_tfts_ia_summary_en.pdf

European Commission Joint Review of the implementation of the Agreement between

	the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security – Accompanying the Report from the Commission to the European Parliament and to the Council on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security, COM(2013) 844 final, 27 November 2013 http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/docs/20131127_pnr_report_en.pdf.
European Data Protection Supervisor	Opinion on PNR Agreement, 9 December 2011 https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2011/11-12-09_US_PNR_EN.pdf
European Data Protection Supervisor	Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...], 5 September 2012 https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-09-05_EURODAC_EN.pdf
European Data Protection Supervisor	Opinion of the European Data Protection Supervisor on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP), 18 July 2013 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-07-18_Smart_borders_EN.pdf
European Data Protection Supervisor	EDPS comments on the Communication from the Commission to the European Parliament and the Council on a European Terrorist Finance Tracking System (TFTS) and on the Commission Staff Working Document -Impact Assessment accompanying the Communication from the Commission to the European Parliament and the Council on a European Terrorist Finance Tracking System (TFTS), 17 April 2014

http://www.statewatch.org/news/2014/apr/eu-edps-tfts.pdf

European Parliament Debates, Wednesday, 16 April 2014 – Strasbourg

www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20140416+ITEM-017+DOC+XML+V0//EN&language=EN

European Parliament SWIFT: European Parliament votes down agreement with the US, Press Release of 11 February 2010

Information Officer of the Republic of Slovenia Press Release of 11 July 2014 concerning Constitutional Court's Decision of 3 July 2014, No. U-I-65/13-19

https://www.ip-rs.si/index.php?id=272&tx_ttnews[tt_news]=1256&cHash=2885f4a56e6ff9d8abc6f94da098f461

National Data Protection Commission of Luxembourg Opinion on DRD Judgement, No. 214/2014 of 13 May 2014

http://www.cnpd.public.lu/fr/decisions-avis/2014/Vorratsdatenspeicherung/index.html

Judgements and Opinions

Advocate General Opinion on Joint Cases C-293/12, C-594/12, 12 December 2013

Austrian Constitutional Court No. G 47/2012, Decision of 27 June 2014

Press release at http://www.vfgh.gv.at/cms/vfgh-site/attachments/5/0/0/CH0003/CMS1403853653944/presseinformation_verkuendung_vorratsdaten.pdf

Bulgarian Supreme Administrative Court Decision No. 13627, Case No. 11799 2008, Judgement of 11 December 2008

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

CJEU Case C-260/89, Elliniki Radiophonia Tiléorassi AE v Dimotiki Etairia Pliroforissis and Sotirios Kouvelas, Judgement of 18 June 1991

CJEU Case C-368/95, Vereinigte Familiapress Zeitungsverlags- und vertriebs GmbH v Heinrich Bauer Verlag, Judgement of 26 June 1997

CJEU Case C-112/00, Eugen Schmidberger, Internationale Transporte und Planzüge v Republik Österreich, Judgement of 12 June 2003

CJEU Joint Cases C-465/00, Rechnungshof v Österreichischer Rundfunk, Wirtschaftskammer Steiermark, Marktgemeinde Kaltenleutgeben, Land Niederösterreich, Österreichische Nationalbank, Stadt Wiener Neustadt, Austrian Airlines, Österreichische Luftverkehrs-AG; Christa Neukomm v Österreichischer Rundfunk (C-138/01); Joseph Lauermann v Österreichischer Rundfunk (C-139/01), Judgement of 20 May 2003

CJEU Case C-36/02, Omega Spielhallen- und Automatenaufstellungs-GmbH v Oberbürgermeisterin der Bundesstadt Bonn, Judgement of 14 October 2004

CJEU Case C-244/06, Dynamic Medien Vertriebs GmbH v Avides Media AG, Judgement of 14 February 2008

CJEU Case C-301/06, Ireland v European Parliament and Council of the European Union, Judgement of 10 February 2009

CJEU Case C-518/07, Commission v Germany, Judgement of 9 March 2010

CJEU Case C-236/09, Association belge des Consommateurs Test-Achats ASBL, Yann van Vugt, Charles Basselier v Conseil des ministres, Judgement of 1 March 2011

CJEU	Case C-279/09, DEB Deutsche Energiehandels- und Beratungsgesellschaft mbH v Bundesrepublik Deutschland, Judgement of 22 December 2010
CJEU	Case C-614/10, Commission v Austria, Judgement of 16 October 2012
CJEU	Case C-617/10, Åklagaren v Hans Åkerberg Fransson, Judgement of 26 February 2013
CJEU	Case C-270/11, European Commission v Kingdom of Sweden, Judgement of 30 May 2013
CJEU	Case C-399/11, Stefano Melloni v Ministerio Fiscal, Judgement of 26 February 2013
CJEU	Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, Judgement of 13 May 2014
CJEU	Case C-288/12, Commission v Hungary, Judgement of 8 April 2014
CJEU	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, Judgement of 8 April 2014
CJEU	Case C-370/12, Thomas Pringle v Government of Ireland, Ireland, The Attorney General, Judgement of 27 November 2012
CJEU	Case C-390/12, Robert Pfleger Autoart as, Mladen Vucicevic, Maroxx Software GmbH, Hans-Jörg Zehetner, Judgement of 30 April 2014
CJEU	Case C-594/12, Kärntner Landesregierung; Michael Seitlinger; Christof Tschohl and others, Judgement of 8 April 2014

Cypriot Supreme Court	Civil applications 65/2009, 78/2009, 82/2009, 15/2010-22/2010, Judgement of 1 February 2011
Czech Constitutional Court	Pl. ÚS 24/10, Judgement of 22 March 2011 Unofficial English version: http://www.slidilove.cz/sites/default/files/dataretention_judgment_constitutionalcourt_czechrepublic.pdf
ECtHR	No. 19522/09, M.K v. France, Judgement of 18 April 2013
ECtHR	No. 30562/04 and 30566/04, S. and Marper v. UK, Judgement of 4 December 2008 (Grand Chamber)
ECtHR	No. 54934/00, Weber and Saravia v. Germany, Judgement of 29 June 2006
ECtHR	No. 5029/71, Klass v. Germany, Judgement of 6 September 1978
German Constitutional Court	1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Judgement of 2 March 2010 http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html Press Release in English: http://www.bverfg.de/en/press/bvg10-011en.html
Irish High Court	No. 765 JR, Maximilian Schrems v. Data Protection Commissioner, Judgement of 18 June 2014 http://www.europe-v-facebook.org/hcj.pdf
Romanian Constitutional Court	Decision No. 1258, Judgement of 8 October 2009 unofficial translation: http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf