THE STRICT NECESSITY TEST ON DATA PROTECTION BY THE CJEU: A PROPORTIONALITY TEST TO FACE THE CHALLENGES AT THE BEGINNING OF A NEW DIGITAL ERA IN THE MIDST OF SECURITY CONCERNS

Zlatan Meškić and Darko Samardžić*

Summary: Through the judgments Digital Rights Ireland and Tele2 Sverige, the CJEU emphasised the power of the CFR (in particular arts 7, 8, 52) through the fundamental right of data protection and general principles of law such as the principle of proportionality and legal certainty. Article 52 CFR represents the essence of justification. In the spirit of article 52(3) and (4) CFR it becomes evident that the CJEU, the ECtHR and the German Constitutional Court go in the same direction. The CJEU was brave enough to deliver a scathing verdict on data retention. More strongly than the German CC, the CJEU safeguards data protection. Hence, the decisions of the CJEU were described as milestone decisions and the CJEU as a Court of fundamental rights. On the other hand, the CJEU focused all its power on proportionality expressed through the element of strict necessity. It is astonishing that the Court does not use the existing methodology on proportionality to strengthen legal discipline and confidence. Although proportionality may be assessed differently in single legal systems and cultures, the broad constitutionalisation and application of proportionality in jurisdiction proves the power of this general principle of law. The exploration of this principle is rather challenging, but most beneficial for the future application of primary law.

1 Introduction

Digitalisation penetrates fundamental, private and intimate areas of life, science, the economy, society and privacy. Drones, robots or automated driving are prominent symbols of product digitalisation. Closely linked to digitalisation is the use of algorithms and data processing. People like Edward Snowden have shaken the public and raised new awareness of data.[1] Hacker attacks and fake news have unsettled many people.

* Professors at the University of Zenica, Faculty of Law. Authors' contacts: zmeskic@prf.unze.ba; darko.samardzic@gmx.de.

[1] Matthias Bäcker, 'Das Vorratsdatenurteil des EuGH: Ein Meilenstein des europäischen Grundrechtsschutzes' (2014) 36 JA 1263, 1269.

Artificial intelligence is not a physical object we can hold in our hands. Perhaps objects or subjects of artificial, autonomous intelligence are or will be smarter than people and are already or will soon become dominant. Additionally, there is asymmetry of the parties involved, in particular among individuals, experts, big players and state authorities. These are the reasons why data protection, with a few remarkable judgments on data retention, is the subject of this paper.

The legislation on data rights of the last few decades may give the impression that state powers act without a clue or that they can hardly keep up with the developments. Data protection is one of the legal governance instruments the legislator has to regulate and operate. The overriding role of security concerns as put forward by the legislator is one of the key drivers to be assessed and in doing so the legislator touches on the balance of freedom and security.[2] The legislation on data retention was a specific expression of the wish for preventive security in a transforming world.[3] Thus, Directive 2006/24 (the Data Retention Directive) on data retention came into focus.[4] This directive demands data service providers to retain data preventively, generally and in a widespread manner. This means that data may be collected without any reasons given. A dozen questions are raised thereby. The CJEU summarises the main reasons of disproportionality under the umbrella of strict necessity which leads to the condensed question of the justification of interference in the fundamental right of data protection in the light of proportionality as anchored in article 52(1) of the Charter of Fundamental Rights (CFR): is the restriction of the right to personal data brought about by widespread data retention proportionate to the objective of preventive security pursued by the state? Therefore, we have to understand why and how the CJEU focuses on strict necessity in order to clarify conformity to the principle of proportionality. The judgments on data retention are of ground-breaking significance, touching on general principles of primary law.

Remarkably, the CJEU in its decision in *Digital Rights Ireland* in 2014 declared the Data Retention Directive as invalid, confirming this understanding in 2016 in its case *Tele2 Sverige*. In these judgements, the CJEU further developed the concept of strict necessity as an integral

---

[2] Markus Kotzur, 'Wider den bloßen Verdacht – zur grundrechtssichernden Verantwortung des EuGH im Spannungsfeld von Freiheit und Sicherheit'(2014) 41 EuGRZ 589; Jürgen Kühling, 'Der Fall der Vorratsdatenspeicherungsrichlinie und der Aufstieg des EuGH zum Grundrechtsgericht' (2014) 33 NVwZ 681, 685.

[3] Spiros Simitis, 'Die Vorratsdatenspeicherng – ein unverändert zweifelhaftes Privileg' (2014) 67 NJW 2158, 2159.

[4] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ 105/54.

part of the proportionality test on data protection.[5] The term 'strict necessity' was used by the ECtHR as far back as 1978, in its *Klass* decision, where the ECtHR stated that 'Powers of secret surveillance of citizens, characterizing as they did the police state, were tolerable under the Convention only insofar as strictly necessary for safeguarding democratic institutions'.[6] The CJEU first used this test in *Satamedia* 2008, before the CFR entered into force, stating 'the protection of the fundamental right to privacy requires that the derogations and limitations in relation to the protection of data (..) must apply only in so far as is strictly necessary'.[7] The CJEU has used the strict necessity test in relation to the right to data protection in a consistent manner ever since. Even before *Digital Rights Ireland* in 2014, the CJEU considered the 'strict necessity' test to be settled case law.[8] The ECtHR in the meantime forgot about its own invention[9] and remembered it only after it was used by the CJEU in *Digital Rights Ireland*. It did so by direct reference to this judgment.[10]

However, in the previous cases the CJEU did not demonstrate what 'strict' and 'necessary' were in the established proportionality test for data protection. It did so after the *Satamedia* case, wondering about what 'strict' for this purpose meant and if it was even a valid criterion.[11] The colliding interests had also been different in previous cases, as data protection was balanced against the fundamental right to freedom of expression,[12] transparency of the use of funds,[13] and the right of the subject to be informed about the processing of his personal data for the purpose of a private detective's investigation.[14]

The initial question raised here is if the strict necessity test copes with the goals of security with the fundamental right of data protection

---

5 cf the concept of strict necessity already commented on by Andreas Wehlau and Niels Lutzhöft, 'Grundrechte-Charta und Grundrechts-Checkliste – eine dogmatische Selbstverpflichtung der EU-Organe' (2012) 23 EuZW 45, 48.

6 *Klass and others v Federal Republic of Germany* (1979-80) 2 EHRR 214, para 42.

7 Case C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy (Satakunnan)* ECLI:EU:C:2008:727 para 56.

8 Case C-473/12 *Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert and Others* ECLI:EU:C:2013:715, para 39.

9 The ECtHR did not use or mention the strict necessity test in its fundamental decisions on data protection: *Leander v Sweden* (1987) 9 EHRR 433; *S and Marper v the United Kingdom* (2009) 48 EHRR 50; *Nada v Switzerland*, (2013) 56 EHRR 18.

10 *Szabó and Vissy v Hungary* App no 37138/14 (ECtHR, 12 January 2016) paras 23 and 73.

11 Wouter Hins, 'Case C-73/07, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy, judgment of the Grand Chamber of 16 December 2008, not yet reported' (2010) 47(1) CMLR 215, 216, 233.

12 *Satakunnan* (n 7) paras 53f.

13 Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and others v Land Hessen* ECLI:EU:C:2010:662, paras 77 and 86.

14 Case C-473/12 *Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert and Others* ECLI:EU:C:2013:715, para 26.

on the grounds of the principle of proportionality as stipulated in article 52(1) CFR. An analysis of the concept of strict necessity of the CJEU with regard to data retention in comparison with other jurisdictions should reveal the novelties in the application of the proportionality test: is it a necessity test, what are the overall assessment criteria used in this test, and how does the element of the strict necessity test correlate with the methodology of proportionality as a whole? A comparison with the jurisprudence of the ECtHR and the German Constitutional Court (CC), in particular its decision on data retention in 2010, are of great help in this regard. Namely, a couple of years before *Digital Rights Ireland* in 2010, the German CC declared as invalid the national legislation on data retention based on the EU Data Retention Directive. Between these judgments, several convergences as well as divergences stand out. German jurisdiction on data protection has existed since 1983 and its methodology on justification and proportionality may be valuable for further comparison.[15] Additionally, the case law of the ECtHR on fundamental rights, proportionality and fair balance may be of significance.

2 Data protection legislation as a reaction of state authorities to innovation and security

2.1 Legislation strongly driven by security concerns

The following graph shows the legislative beginning of data protection within single Member States of the EU, followed by international developments in positive law.[16] From 1995 we can see the legislative activism of the EU which caused the judgments of the CJEU in 2014 and 2016 on the Data Retention Directive and the judgment of the German CC in 2010 due to the German legislator who had immediately implemented the Data Retention Directive in national laws through the so-called Law on the Revision of Telecommunication Monitoring in 2007.[17]

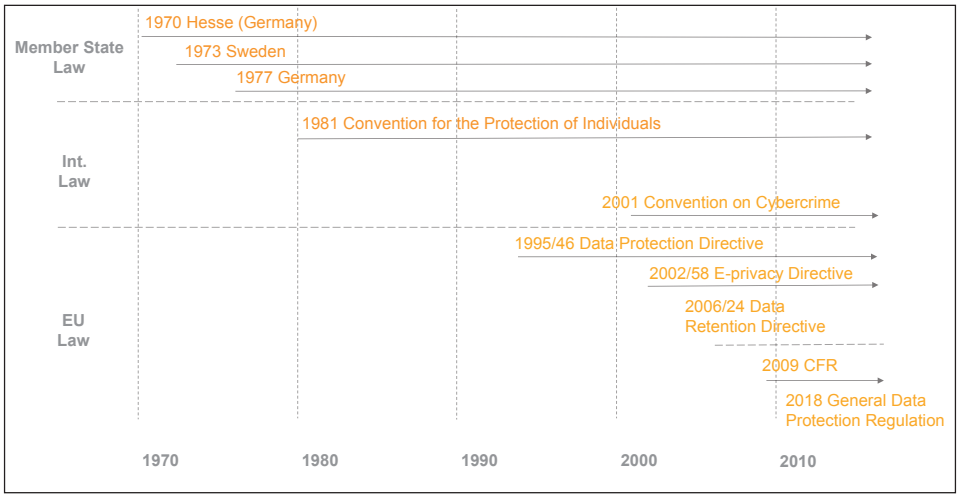
Remarkably, we can identify two waves of legislation. One wave occurred in the 1970s and one at the beginning of this century. The first wave was driven by innovation due to missing positive law on data protection as an answer to the rise of information technology. Firstly, we can

[15] Spiros Simitis, 'Einleitung' in Spiros Simitis (ed), *Bundesdatenschutzgesetz* (8th edn, Nomos 2014) 92.

[16] Extended, initial version of the graph, Jürgen Kühling, Christian Seidel and Anastasios Sivridis, Datenschutzrecht (CF Müller 2015) 62.

[17] This is an omnibus law which means that different laws had to be revised. The main changes were made in the Telecommunications Act. This law serves preventive data retention. The repressive approaches to data monitoring for criminal prosecutions led to a revision of the Criminal Procedure Code.

notice such legislation in Hesse, one of Germany's 16 federal states.[18] Sweden, and Germany as an entire state, followed.[19] International and EU legislation shows there has been a global demand for regulation. Logically, the legislation approaches differ. The spectrum ranged from abstract framework legislation up to sectoral governance, as well as combinations of these approaches. This is interesting due to the analogous discussion nowadays on how to approach data protection.[20]



After these first codifications, the EU in 1995 started to establish positive law on data protection to give different national regulations a common framework.[21] This second wave of European legislation was certainly driven both by technological progress and economic interests. But it seems that the legislators were very much driven by security concerns.[22] The first step was taken with the adoption of the Budapest Convention on Cybercrime adopted by the Council of Europe in 2001.[23] The Cybercrime Convention is the first international treaty on crimes committed via the internet and other computer networks.[24] Since 9/11, terrorist concerns

[18] Kai von Lewinski,'Einleitung' in Martin Eßer, Philipp Kramer and Kai von Lewinski (eds), *BDSG* (Carl Heymanns Verlag 2015) 93, para 22; Simitis '(n 15) 82.

[19] Simitis '(n 15) 134.

[20] Martin Eßer, Philipp Kramer and Kai von Lewinski, *DSGVO-BDSG* (5th edn, Carl Heymanns Verlag 2017); Jürgen Kühling, *Datenschutz Grundverordnung* (CH Beck 2017); Gernot Sydow, *Europäische Datenschutzgrundverordnung* (Nomos 2017).

[21] Simitis (n 15) 166.

[22] Kotzur (n 2) 589; Antonie Moser-Knierim, *Vorratsdatenspeicherung – zwischen Überwachungsstaat und Terrorabwehr* (Springer 2014).

[23] Council of Europe, Committee of Ministers, 8 November 2001.

[24] Convention on Cybercrime (European Treaty Series no 185 <www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185> accessed 29 May 2017.

have determined legislators' behaviour significantly.[25] The terror attacks in London in 2005, and before that in Madrid 2004, evoked rapid reactions from the EU.[26] In a rather fast legislation process, the EU implemented the Data Retention Directive. Perhaps these rapid reactions were the reason for the dubious quality of this directive. This background knowledge is of importance when the CJEU assesses the validity of the directive. The historical circumstances may explain the need for such a regulation and may also indicate the disproportionate content of the directive.

2.2 CJEU on data retention 2014 and 2016 – Invalidity of the directive on data retention

In focus here is the application of the strict necessity test by the CJEU in its cases *Digital Rights Ireland* and *Tele2 Sverige*. In *Digital Rights Ireland* in 2014, the whole of the Data Retention Directive was under question. After the CJEU declared this directive invalid in its case *Tele2 Sverige*, the Court in 2016 had to decide, on the legal basis of article 15(1) of Directive 2002/58, if and to what extent national legislation on data retention was in conformity with European law. At this point, we shall briefly recall why the directive on data retention was questioned, thus leading to the preliminary ruling before the CJEU. The same will be shown briefly with regards to the development of the latest jurisprudence of the German CC on data retention and protection. Focus will be placed on essential points taken into account in the proportionality test by the courts. A concrete analysis of the single steps of the proportionality test follows a short overview of the respective case law.

2.2.1 Digital Rights Ireland 2014

In the case *Digital Rights Ireland* the CJEU had to examine the validity of the Data Retention Directive on data retention. The CJEU declared the directive invalid due to non-conformity with the fundamental right of data protection (arts 7 and 8 CFR) and the principle of proportionality (art 52(1) CFR). The directive was adopted subsequent to different terror attacks to unify the various rules on data protection in the Member States. In 2012 the High Court of Ireland and the *Verfassungsgerichtshof* of Austria requested a preliminary ruling pursuant to article 267 TFEU on the validity of the directive above. Different claimants from Ireland and Austria protested against the directive, claiming that the fundamental rights of data protection, freedom of speech (arts 7, 8, 11 CFR) were violated, as were the economic interests of the telecommunication service providers who were obliged to retain data. Such providers were instructed to retain

[25] Florian Becker, 'Grundrechtliche Grenzen staatlicher Überwachung zur Gefahrenabwehr' (2015) 34 NVwZ 1335; Kühling (n 2).

[26] Alexander Roßnagel, 'Die neue Vorratsdatenspeicherung' (2016) 69 NJW 533.

all communication data (eg location, duration, participants, metadata) of all subjects for a retention period of six to twenty-four months. Concrete suspicion or facts justifying retention were not required. The goal was to ensure security through the fight against, for example, international terrorism or serious crime. State authorities were allowed to use such data.

2.2.2 Reasons for a second judgment on data retention after 2014: Tele2 Sverige 2016

The *Tele2 Sverige* case arose after many question in *Digital Rights Ireland* remained unanswered.[27] It was unclear to what extent the invalidity of the directive affected national legislation on data retention. Many national legislators remained convinced that their national legislation was in line with articles 7 and 8 GRC, despite the *Digital Rights Ireland* ruling. It was unclear if widespread data retention of all subjects and all means of communication was allowed at all. It was also quite unclear which elements caused the invalidity of the directive, whether all the aspects all together violated the principle of proportionality or whether each single element caused disproportionality.[28] The High Administrative Court in Stockholm and the Appeal Court of England and Wales requested a preliminary ruling because the national laws on data retention served to implement the Data Retention Directive which had become obsolete after the judgment in *Digital Rights Ireland*. Instead, Directive 2002/58 served from then on as the legal basis for data protection at the EU level. The CJEU was requested to answer whether EU law was applicable and if the national laws conformed to the fundamental right of data protection. The Court declared that article 15(1) of Directive 2002/58 had to be interpreted in the light of articles 7, 8, 11 and 52(1) CFR.[29] Hence, the widespread retention of traffic and location data at the national level of all people and all means of communication was not allowed. This means that not only was the Data Retention Directive invalid, but the same processing at the national level was also not allowed.

2.3 German CC on the invalidity of laws on data retention 2010

Germany was rather fast in implementing the Data Retention Directive. This is astonishing when compared to other directives where Germany exhausted the implementation period right up to the end, exceeded the time limits, or tried to avoid parts of the implementation. The German legislator may be driven by strong security interests, but this is no excuse. In 2007 the legislator implemented the Data Retention Directive through

[27] Bäcker (n 1) 1265; Spiros Simitis, Die Vorratsdatenspeicherng – ein unverändert zweifelhaftes Privileg (2014) 67 NJW 2158; Kühling (n 2) 683.

[28] Kühling (n 2) 683; Bäcker (n 1) 1269.

[29] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen* ECLI:EU:C:2016:970, para 92.

establishing new rules within different laws such as the Code of Criminal Procedure or the Telecommunication Monitoring Regulation.[30] This shows that data retention from the preventive point has a police law dimension and from the repressive point of view a criminal law dimension. In 2010 the German CC declared the laws unconstitutional.[31] In doing so, it was yet again participating in European constitutional discourse,[32] this time on data protection.

3 The essence of the right to data protection

To examine the essence of fundamental rights is rather demanding.[33] First of all there is no common understanding of the content and limits of the essence of a right. It is even unclear if interference with the essence of a right is justifiable. This is comparable to a discussion on human dignity in terms of whether interference with a so-called untouchable right is justifiable. Methodologically, different opinions exist about the kind of examination of essence. Partially, it is seen as the final evolution of proportionality. However, the CJEU seems, in accordance with the wording and systematic structure of article 52(1) CFR, to prefer the opinion that essence is an independent element of justification to be examined chronologically before proportionality.

With regard to doctrinal discussions on the essence of rights, it is astonishing that the CJEU in the case of data retention states that the essence of data protection is untouched, because the Directive does not permit the acquisition of knowledge of the content of the electronic communications as such.[34] It may not be concluded that the CJEU tried to avoid deeper elaboration of this difficult issue. Namely, only one year later in the fundamental *Schrems* judgment, the CJEU consistently applied the very same criteria for the essence of the right to private life with regards to data retention and came to the opposite conclusion.[35] The CJEU stated importantly 'that permitting the public authorities to have access on a generalised basis to the content of electronic communications must be

---

30 Strafprozessordnung oder Telekommunikations-Überwachunsgverordnung, BGBl I 2007, 3198.

31 BVerfG - 1 BvR 256/08 of 2 March 2010, para 260.

32 Tamara Ćapeta,'Courts, Legal Culture and EU Enlargement' (2005) 1 CYELP 1, 6.

33 Elisabeth Rumler-Korinek and Erich Vranes in Michael Holoubek and Georg Lienbacher (eds), *GRCh-Kommentar* (Manz 2014) art 52 - 'Tragweite und Auslegung der Rechte und Grundsätze' 755, para 18; Andreas Wehlau and Niels Lutzhöft, 'Grundrechte-Charta und Grundrechts-Checkliste – eine dogmatische Selbstverpflichtung der EU-Organe' (2012) 23 EuZW 45, 49; Nils Schaks,'Die Wesensgehaltsgarantie, art 19 II GG' (2015) 55 JuS 407.

34 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* ECLI:EU:C:2014:238, para 39.

35 Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650, para 94.

regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter'. It seems that the CJEU developed the standard further, as not only did it take into consideration whether it was permitted for public authorities to acquire knowledge about the content of electronic communication, but also whether this was permitted 'on a generalised basis'.[36] Whether mere 'retention of the content of a communication' is sufficient, as again examined and denied one year later in *Tele2 Sverige*,[37] or whether in addition the permission needs to be a general one, will be seen in future cases. The criteria of general permission would have been fulfilled in *Digital Rights Ireland* and *Tele2 Sverige* anyway. The more important question here is if the CJEU takes a too formalistic approach by requiring direct access to the content of communication. The Court itself finds that the retention of other communication data may allow very precise conclusions on the private life of the people concerned, 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.[38] These are all content data, only gathered indirectly. It can be seen as the outcome of the principle of giving priority to direct over indirect as well as over hidden data collection.[39] Another question is whether the essence test is the right one to reach this goal.

Here the German CC goes further. The court claims that data retention allows content conclusions.[40] However, the German CC did not find that this was enough to interfere with the essence of the right to private life. Within the scope of application of the CFR, the German CC will need to change its mind. By following the reasoning of the CJEU, the question arises of the consequence when the essence of data protection is touched on by the content of the communication data. Here we have to take into consideration that in the *Schrems* judgment the CJEU did not examine the proportionality test, because the essence of the right to private life was already found to have been compromised.[41] This is in line with the

---

[36] Johannes Eichenhofer '"e-Privacy" im europäischen Grundrechtsschutz: Das "Schrems-Urteil" des EuGH' (2016) 51 EuR 76, 84.

[37] *Tele2 Sverige AB* (n 29) para 101.

[38] ibid, para 99; *Digital Rights Ireland* (n 34) para 27.

[39] Thorsten Kingreen in Christian Calliess and Matthias Ruffert (eds), *EUV/AEUV* (5th edn, Beck 2016) art 8 GRCh - 'Schutz personenbezogener Daten' 2809, para 16: 'Vorrang der unmittelbaren vor der mittelbaren Datenerhebung als auch Vorrang der offenen vor der verdeckten Datenerhebung'.

[40] BVerfG (n 31) para 211; Andreas Nachbaur, 'Vorratsdatenspeicherung "light" – Rechtswidrig und allenfalls bedingt von Nutzen' (2015) 48 ZRP 215, 217.

[41] Thomas Giegerich, 'Europäische Vorreiterrolle im Datenschutzrecht – Neue Entwicklungen in der Gesetzgebung, Rechtsprechung und internationalen Praxis der EU' (2016) 19 ZeuS 301, 334.

'absolute theory' on the essence of a fundamental right that considers interference with the essence as unjustifiable.[42] This is also in line with the fact that the essence test is now a separate criterion within article 52(1) CFR.[43] However, in line with the concept of the right to personal data as a right to self-determination, even in cases where the essence of the right is interfered with, a person should be given the opportunity to give consent to the interference and thereby make it valid.[44]

4 The proportionality test pursuant to article 52(1) CFR with regards to the fundamental right to data protection

The following analysis is based on the recognised logic of proportionality, fully aware that different opinions on the logic of proportionality exist.[45] Nevertheless, the four steps of the legitimate objective, appropriateness, necessity and reasonableness (proportionality in the narrow sense) may be identified as an essential skeleton in the judgments of the CJEU.[46] If the legitimate objective is deemed an autonomous element to be examined separately before proportionality, the structure of proportionality consists of three elements.[47] The methodology or, as other authors emphasise, rationality in balancing is key.[48] This is irrespective of the next question of how subjective or how objective proportionality or balancing can be.[49] Although the CJEU does not consistently examine the principle of proportionality, the Court basically supports the logic of a three-step proportionality test.[50] The most common formula used by the Court is that

---

[42] Eichenhofer '(n 36) 85.

[43] Thorsten Kingreen in Christian Calliess and Matthias Ruffert (eds), *EUV/AEUV* (5th edn, Beck 2016) art 52 GRCh, 'Tragweite und Auslegung der Rechte und Grundsätze' 2982, para 64.

[44] Jürgen Kühling and Johanna Heberlein, 'EuGH "Reloaded": "Unsafe Harbor" USA vs "Datenfestung" EU' (2016) 35 NVwZ 7, 10.

[45] Margit Bühler, *Einschränkung von Grundrechten nach der Europäischen Grundrechtecharta* (Duncker & Humblot 2005) 104.

[46] Case C-365/08 *Agrana Zucker GmbH v Bundesminister für Land- und Forstwirtschaft, Umwelt und Wasserwirtschaft* ECLI:EU:C:2010:27, Opinion of GA Trstenjak, para 60; Case C-34/09 *Gerardo Ruiz Zambrano v Office national de l'emploi* ECLI:EU:C:2010:560, Opinion of GA Trstenjak, para 62; Kingreen (43) art 52 GRCh, 2983, para 65; Clemens Ladenburger and Hannes Krämer in Klaus Stern and Michael Sachs (eds), *EUV/AEUV* (Beck 2016) art 52 GRCh - 'Tragweite und Auslegung der Rechte und Grundsätze' 798, para 48ff.

[47] Rumler-Korinek and Vranes (n 33) art 52 GRCh 755, para 16; Nicolas Raschauer and Thomas Riesz in Michael Holoubek and Georg Lienbacher (eds), *GRCh-Kommentar* (Mnz 2014) art 8 GRCh - 'Schutz personenbezogener Daten' 119, para 33; Matthias Klatt and Moritz Meister, 'Der Grundsatz der Verhältnismäßigkeit' (2014) 54 JuS, 193, 196.

[48] For instance, Klatt and Meister (n 47) 195.

[49] Concretely on the understanding of objectivity, see Klatt and Meister (n 47) 198.

[50] Wolfgang Weiß, 'Grundrechtsschutz durch den EuGH: Tendenzen seit Lissabon' (2013) 24 EuZW 287, 290; Kingreen (43) art 52 GRCh, 2982, para 65.

> measures adopted do not exceed the limits of what is appropriate and necessary in order to attain the objectives legitimately pursued by the legislation in question; when there is a choice between several appropriate measures, recourse must be had to the least onerous, and the disadvantages caused must not be disproportionate to the aims pursued.[51]

Here we can find the previously identified four elements: the legitimate objective, the appropriate measure, 'the least onerous measure' criterion that can be attributed to the necessity test, and the 'not disproportionate to the aims pursued' criterion as reasonableness/proportionality in the narrow sense.[52] The Court itself refers to proportionality in *Digital Rights Ireland* and *Tele2 Sverige* as settled case law.[53]

Admittedly, the CFR does not provide good support for the differentiation between the necessity and reasonableness requirement. But reasonableness is not directly referred to and may be derived from the repeated mentioning of proportionality, and therefore interpreted as proportionality in the narrow sense.[54] From other jurisdictions and legal literature, it becomes clear that proportionality in the narrow sense is the final step of proportionality, whether as a separate step or included in one of the other elements of proportionality.[55] But data protection served as an essential motor for the justification test after the CFR entered into force through the Lisbon treaty.[56] Proportionality in the case law of the CJEU is very much characterised by the balancing of the interests and rights concerned.[57] With regard to data protection, derogations can only apply when strictly necessary.[58] Hence, there is a new, combinatory power through the correlation of the CFR, fundamental rights, data protection and the principle of proportionality driven through strict necessity, as well as based on the already existing doctrine on proportionality.

---

[51] Joined Cases C-96/03 and C-97/03 *Tempelman and van Schaijk v Directeur van de Rijksdienst voor de keuring van Vee en Vlees* ECLI:EU:C:2005:145, para 47.

[52] Hans D Jarass, *GRCh* (3rd edn, CH Beck 2016) art 52 - 'Tragweite und Auslegung der Rechte und Grundsätze' 501, para 36.

[53] *Digital Rights Ireland* (n 34) para 45f; *Tele2 Sverige AB* (n 29) para 96.

[54] Kingreen (n 43) art 52 GRCh, 2984, para 70; Rumler-Korinek and Vranes (n 47) art 52 GRCh 755, para 16.

[55] Johannes Saurer, 'Die Globalisierung des Verhältnismäßigkeitsgrundsatzes' (2012) 51 Der Staat 3, 9; Florian Becker, 'Grundrechtliche Grenzen staatlicher Überwachung zur Gefahrenabwehr' (2015) 34 NVwZ 2015 1335, 1336.

[56] Steve Peers and Sacha Prechal, 'Article 52 – Scope and Interpretation of Rights and Principles' in Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward (eds), *The EU Charter of Fundamental Rights* (Nomos, CH Beck, Hart Publishing 2014) art 52 CFR, 1482, para 52.70.

[57] Joined Cases C-468/10 and C-469/10 *Asociación Nacional de Establecimientos Financieros de Crédito and Federación de Comercio Electrónico y Marketing Directo v Administración del Estado* ECLI:EU:C:2011:777 paras 43, 47f; *Volker und Schecke* (n 13) para 77, 86.

[58] *Volker und Schecke* (n 13) paras 77, 86; Kingreen (n 39) art 8 GRCh, 2809, para 16.

To stay focused, proportionality here is analysed on the grounds of the two decisions in *Digital Rights Ireland* and *Tele2 Sverige*, both decisions made on the issue of data retention. In both decisions, laws on data retention were deemed not to conform to the fundamental right of data protection (art 8 CFR) and proportionality as a general principle of law now codified in article 52(1) CFR. This provision serves as the cornerstone of justification in the field of fundamental rights. Other general principles of law, such as legal certainty or confidence, serve as further standards of verification. As the CJEU did in its decisions later, the ECtHR emphasised the need for clear, precise laws on data retention. Thereby, the ECtHR strengthens the principle of proportionality through the principle of legal certainty. The ECtHR increases the requirements of proportionality in the field of data protection.[59] In accordance with article 8(2) ECHR, the ECtHR demands strict necessity for justification. For sure, the case law of the ECtHR served as support, as clearly shown by the CJEU in referencing essential cases of the ECtHR.[60] Thus, the Court declared the Data Retention Directive invalid. As far as the decision in *Tele2 Sverige* deviates from *Digital Rights Ireland* or emphasises specific elements, these selected elements will be explained as such.

4.1 Legitimate objective test

The CJEU admits that the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest and argues that the same is true of the fight against serious crime in order to ensure public security.[61] But the Court criticises that it remains unclear what in specific terms a serious crime is.[62] Under strict necessity, the CJEU describes the insufficient regulation of serious crime. The CJEU demands that the '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'.[63] The Court states further that such

> data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, 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.[64]

---

[59] *Leander v Sweden* (n 9) para 60ff.

[60] For instance expressly *Digital Rights Ireland* (n 34) paras 35, 47, 54; Bäcker (n 1) 1273.

[61] *Digital Rights Ireland* (n 34) para 42.

[62] ibid, para 60.

[63] ibid, para 61.

[64] *Digital Rights Ireland* (n 34) para 27.

For its part, the German CC emphasises the principle of legal certainty supporting the requirements of proportionality. Access is not restricted to the objective of serious crimes and is not subject to a court decision requirement.[65] Crimes which may be able to justify the extent and weight of interference need to be clearly and precisely determined.[66] Although the law should have served the legitimate objective of fighting terrorism, this goal may not be generally used as a justification.[67] In the light of proportionality in the narrow sense – which may be translated as an element of strict necessity in the language of the CJEU – it is not enough to justify restrictions of fundamental rights by an abstract legitimate objective. State authorities need concrete facts of suspicion.[68] The prognosis of danger has to reach a certain degree of likelihood, but occasional behaviour or simple assumptions may not serve as justification.[69] The CJEU here goes in the same direction, but more abstractly:

> 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. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime.

If this is true, the legitimate objective is already a hurdle in fulfilling the requirements of the proportionality test. Thus, the CJEU could have clarified the invalidity of the directive even at this stage.[70] Such a clear structure does not prevent the detection of further elements of disproportionality.[71] However, the Court examines all these thoughts under the umbrella of strict necessity mixed together with other facts, aspects, elements and explanations. Access to 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.[72] For the Court, the element of legitimate objective seems not to be the right place for deeper examination of such an objective. This simple affirmation is questionable because chronologically and logically

---

65 BVerfG (n 31) para 247ff.

66 ibid, para 228.

67 ibid, para 250ff.

68 ibid, paras 228, 261, 289: the German CC speaks of concrete facts constituting suspicion or sufficient initial suspicion.

69 Florian Becker,'Grundrechtliche Grenzen staatlicher Überwachung zur Gefahrenabwehr' (2015) 34 NVwZ 2015 1335, 1336.

70 Also in Lorin-Johannes Wagner, *Der Datenschutz in der Europäischen Union* (Jan Sramek Verlag 2015) 86.

71 Peers and Prechal (n 56) art 52 CFR, 1482, para 52.71.

72 *Digital Rights Ireland* (n 34) para 61.

the element of legitimate objective is prior to (strict) necessity, as an own element.[73]

From the perspective of the outcome of the ruling, it is remarkable and only consistent that strict necessity already refers to the legitimate objective considering the relevant arguments under this umbrella. The content of strict necessity proves that it is not just a necessity test. This conclusion is hidden in the extensive balancing within the reasonableness test.

4.2 Appropriateness test

The CJEU examines appropriateness in *Digital Rights Ireland* by stating that data which must be retained pursuant to the Data Retention Directive allow the national authorities which are competent for criminal prosecutions to have additional opportunities to shed light on serious crime and, in this respect, the data are a valuable tool for criminal investigations.[74] It is common legal understanding that the appropriateness test is not very strict, as it is enough that a measure aims to support the legitimate objective.[75] With regards to market freedoms, the CJEU usually requires only that it is not 'manifestly inappropriate'.[76] In order to prove this standard, even a rather vague argumentation is sufficient. The Court could have at least questioned the supportive power of data retention. For instance, data retention may be misleading or misused. Subjects could use false IPs, names, other Wi-Fi access or hotspots anonymously.[77] However, in *Tele2 Sverige* the CJEU did not examine this step or repeat the rather simple examination of *Digital Rights Ireland*. Even if in result this may be correct, it is an integral part of the proportionality test. It ensures the logic of examination, self-reflection and legal discipline. All together, normative structures have to correspond to an asystematic, coherent approach, and to follow clear objectives avoiding contradictions, in particular in the area of equality.[78]

4.3 Necessity test

There is no universal doctrine on necessity. This is understandable given the different legal systems and cultures. Different views and

---

[73] Margit Bühler, *Einschränkung von Grundrechten nach der Europäischen Grundrechtecharta* (Duncker & Humblot 2005) 104.; Kingreen (n 43) art 52 GRCh, 2985, para 71; Jarass (n 52) art 52 GRCh 501, para 36, 503, para 41.

[74] *Digital Rights Ireland* (n 34) para 49.

[75] Rumler-Korinek and Vranes (n 33) art 52 GRCh, para 16; Raschauer and Riesz (n 47) art 8 GRCh, 119, para 33; Jarass (n 52) art 52 GRCh 502, para 37f.

[76] Eg Case C-491/01 *British American Tobacco (Investments) Ltd and Imperial Tobacco* ECLI:EU:C:2002:741, para 123.

[77] BVerfG (n 31) para 207.

[78] Kingreen (n 43) art 52 GRCh, 2984, para 68.

intensity of examination may lead to varying or finally different results. But necessity is broadly recognised as an integral part of proportionality and has to be examined as the step subsequent to appropriateness and before proportionality in the narrow sense.[79] This cannot explain the inconsistencies in the examination of necessity. It is difficult to distinguish necessity from proportionality in the narrow sense if balancing or normative assessment is done within the frame of necessity.[80] It may function as a rather neutral, scientific filter before appropriateness. Hence, necessity is deemed as an essentially fact-oriented examination if a milder means could have been used to achieve the same success.[81] This view provoked the thesis that necessity may doctrinally be the most secure part of proportionality.[82] According to the CJEU 'as far as when there is a choice between several appropriate measures, recourse must be had to the least onerous'.[83] The necessity test requires the search for alternative means.[84] An alternative in the area of data retention may be the so-called 'quick freeze' of data. According to 'quick freeze', operators are obliged to retain data relating only to specific individuals suspected of criminal activity as from the date of the preservation order issued by a court[85] or another competent authority. This means that data are retained in single cases, not in a widespread manner from all people and means of communication, and are immediately frozen in the case of concrete suspicion. This could be a milder procedure because it is not necessary to retain data for weeks, months or years without any reason.

It is remarkable that the CJEU in *Digital Rights Ireland* and *Tele2 Sverige* skipped the necessity test completely. Perhaps the Court deemed the test too easy or unimportant, although the Advocate General Cruz Villalón referred to the necessity test, specifically to the alternative of quick freeze.[86] It cannot be disregarded that 'quick freeze' is the option

---

[79] Rumler-Korinek and Vranes (n 33) art 52 GRCh, 755, para 16; Raschauer and Riesz (n 47) art 8 GRCh, 119, para 33; Ladenburger and Krämer (n 46) Art 52 GRCh, 789, para 49; Hans D Jarass, *GRCh* (3rd edn, CH Beck 2016) art 8 -'Schutz personenbezogener Daten' GRCh 106, para 14.

[80] Benjamin Rustenberg, *Der grundrechtliche Gewährleistungsgehalt* (Mohr Siebeck 2009) 223; Kingreen (n 43) Art 52 GRCh, 2984, para 69ff.

[81] Philipp Reimer, '… und machet zu Jüngern alle Völker'?; Von 'universellen Verfassungsprinzipien' und der Weltmacht der Prinzipientheorie der Grundrechte' (2013) 52 Der Staat 27, 33.

[82] Christoph Möllers, 'Wandel der Grundrechtsjudikatur, Eine Analyse der Rechtsprechung des Ersten Senats des BVerfG' 59 (2005) NJW 1973, 1975.

[83] Joined Cases C-37/06 and C-58/06 *Viamex Agrar Handels and Zuchtvieh-Kontor v Hauptzollamt Hamburg-Jonas* ECLI:EU:C:2008:18, para 35.

[84] Ladenburger and Krämer (n 46) Art 52 GRCh, 789, para 49; Jarass (n 79) art 8 GRCh 106, para 14.

[85] Commission, 'Evaluation report on the Data Retention Directive (Directive 2006/24/EC)' COM (2011) 225 final 5.

[86] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* (n 34) Opinion of AG Cruz Villalón, para 142.

chosen by article 16 of the Budapest Convention on Cybercrime adopted by the Council of Europe 2001 which is in force in the EU Member States. This is also referred to not only by the Advocate General, but also by the Evaluation Report on the Data Retention Directive issued by the Commission in 2011.[87] The report also elaborates on the method of 'quick freeze plus'. This model goes beyond data preservation in that a competent authority may also grant access to data which have not yet been deleted by the operators.[88] In most cases this will at least be the data already stored for one month for the purpose of justifying the bill issued by the telecommunication operators. The same alternative means was discussed by the German CC in its decision on data retention.[89] However, if there is any explanation possible for the CJEU skipping the necessity test, all of the previously mentioned came to the conclusion that 'quick freeze' cannot effectively replace data retention. The AG did so by simply stating that 'the idea that the data in question must remain accumulated for a period of time is one of the key aspects of a measure intended to make the public authorities better able to respond to certain forms of serious crime'.[90] The German CC did not do much more or much better, simply arguing that 'such a procedure that encompasses data from the date before the preservation order issued by the authority only insofar as they are still available, is not as effective as a continuous storage that ensures a complete availability of data from the past six months'.[91] Or, in other words, the purpose of data retention cannot be achieved if there are no data retained. Both miss the point that the legitimate objective is the fight against specific serious crimes, and data retention is not the purpose in itself. A study by the German Max Planck Institute on the number on criminal cases where data have been requested by German authorities before the obligation of data retention was introduced by law shows that, for example, only in 0.01% of annual criminal investigations in Germany in 2005[92] were the requested data already deleted.[93] This may lead to the conclusion that in 99% of cases quick freeze was even an effective measure.[94] Of course, on the other hand, it needs to be taken into consid-

---

87 Commission (n 85) 5.

88 ibid.

89 BVerfG (n 31) para 208.

90 Opinion of AG Cruz Villalón (n 86) para 142.

91 BVerfG (n 31) para 208.

92 Christian DeSimone,'Pitting Karlsruhe Against Luxembourg? – German Data Protection and the Contested Implementation of the EU Data Retention Directive' (2010) 11 German Law Journal, 291, 311.

93 Overall analysis of legal practice Hans-Jörg Albrecht, Adina Grafe and Michael Kichling, *Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO: Forschungsbericht im Auftrag des Bundesministeriums der Justiz* (Duncker & Humblot 2008).

94 DeSimone (n 92) 11.

eration that the decision of the authorities to request data is influenced by the fact regarding whether or not the data are stored.[95] Anyhow, the discussion seems to deserve a more thorough analysis from both courts.

What we can now say for sure is that in *Digital Rights Ireland* and *Tele2 Sverige* 'strict necessity' was not examined as a 'stricter' necessity test. On the contrary, the CJEU did not examine necessity at all. In its decision in *Volker and Schecke* the Court proved legal discipline by thinking about the alternative of a milder means in the spirit of necessity when stating that

> there is nothing to show that, when adopting (...), the Council and the Commission took into consideration methods of publishing information on the beneficiaries concerned which would be consistent with the objective of such publication while at the same time causing less interference with those beneficiaries' right to respect for their private life in general and to protection of their personal data in particular...[96]

Therefore, no conclusion should be drawn that the 'strict necessity' test excludes the regular necessity test. In the *Volker and Schecke* judgment, the CJEU applied 'strict necessity' as a form of stricter necessity.[97] It did so by lowering the standard for the necessity test. The CJEU used the following argumentation:

> derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (*Satamedia*, para 56) and that it is possible to envisage measures which affect less adversely that fundamental right of natural persons and which still contribute effectively to the objectives of the European Union rules in question

With regard to the legitimate objective, the effects of an alternative means do not have to reach the same or similar effect. The CJEU lowers the second part of the definition of necessity to 'a still effective contribution'. This opens a broader field for alternative necessity and makes it more difficult for the legislator to adopt the most effective measure. Hence, apart from the methodological inconsistencies, it is astonishing that the CJEU in *Digital Rights Ireland* and *Tele2 Sverige* did not apply the necessity test to strengthen the strict necessity standard.

---

[95] Hans-Jörg Albrecht, Adina Grafe and Michael Kichling, *Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO: Forschungsbericht im Auftrag des Bundesministeriums der Justiz* (Duncker & Humblot 2008) 214.

[96] *Volker und Schecke* (n 13) para 81.

[97] ibid, paras 83 and 86.

4.4 Test of proportionality in a narrow sense summarised by the CJEU under the umbrella of strict necessity

The Court focuses all its power on strict necessity within the reasonableness test, combining different elements under this umbrella.[98] Thereby, this element of proportionality receives strong reinforcement. But it remains unclear if every element of strict necessity leads to disproportionality or only cumulatively (widespread retention of all data, of all means of communication, of all people, retention for a period up to twenty-four months, missing a precise, clear definition of serious crimes, lack of technical, organisational protection and security measures).[99] There is a difference of impact of consequences if every element itself is already not proportionate.[100] It could be argued that, if only the power of all elements together cause disproportionality, the legislator may achieve conformity by the amendment of single elements.[101] The breach may appear less harmful but depends on the metal effect of the elements. Besides other questions, the fundamental tenor of the decision is of leading importance for future legislation on data retention as a whole. In both decisions, the CJEU stresses that 'having regard to all of the foregoing', the right to data protection is disproportionally interfered with. If we put enough weight on this rather usual phrase at the end of a legal assessment of a single preliminary question, we would conclude that only all of the elements together constitute a breach.[102] The *Schrems* judgement does not provide a clear answer either, as again the CJEU evaluated the elements together and concluded that they do not fulfil the requirements of strict necessity.[103]

The following aspects of strict necessity are represented in a comparison of the case law of the CJEU on data retention with the essentials of the case law of the German CC. It is remarkable that the judgments show the main convergences, but there are divergences in detail, intensity of requirements, impact on legislation and general principles of law. It is also remarkable that the ECtHR after so many years started to use the strict necessity test again. In its decision in *Szabó and Vissy v Hungary* of 2016, the ECtHR expressly refers to *Digital Rights Ireland*. In the area of data protection, the ECtHR demands that "'necessity in a democratic

---

98 Kingreen (n 39) art 8 GRCh, 2809, para 16; Kingreen (n 43) art 52 GRCh, 2984, para 69ff.

99 Reinhard Priebe, 'Reform der Vorratsdatenspeicherung – strenge Maßstäbe des EuGH' (2014) 25 EuZW, 456, 457.

100 Kühling (n 2) 683f.

101 Bäcker (n 1) 1269.

102 Kühling considers the elements to be cumulatively required. Kühling (n 2) 683.

103 The CJEU did not have to make any precise conclusion in *Schrems*, as the essence of the right to private life was found to be violated. *Schrems* (n 35) paras 93 and 94.

society" must be interpreted in this context as "strict necessity"'.[104] The ECtHR explained:

> A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation.

Commensurately with the CJEU and the German CC, the ECtHR requires intense proportionality on data protection, in particular if the people concerned are not aware of surveillance. The Court does not allow this developing technology, with all its power or smartness, to override the law. Not everything that is possible is allowed.[105] In the same way, general or public interests cannot serve as abstract justification for using any technology possible.

4.4.1 Data retention is not excluded a priori as a legislative instrument

Digital Rights Ireland was a rather scathing verdict on data retention. Although the German CC stated that state authorities are not allowed to retain all data possible without any reason, including the content and knowledge of internet pages used by individuals, data retention was deemed permitted under strict necessity requirements.[106] Such opinions and the unanswered questions in *Digital Rights Ireland* in particular at the level of the Member States forced a second judgment. In *Tele2 Sverige* in 2016, it became clear that data retention under the conditions of strict necessity was not deemed in itself a forbidden legal approach.[107] EU law, in particular article 15(1) of Directive 2002/58, does not prevent Member States from preventive legislative measures on data retention for the purpose of fighting serious crime, limited to what is strictly necessary. In *Digital Rights Ireland*, the CJEU did not mention the clear lawfulness of data retention. Instead, the Court intensively elaborated a dozen elements leading to disproportionality. After its judgment on data retention, the CJEU was raised as a guardian of data protection, a true constitutional or fundamental rights court.[108] At least it was seen as essential proof on the way towards a fully respected CFR and to the position of a functional fundamental rights court. Instead of delivering a scathing

---

[104] *Szabó and Vissy v Hungary* App no 37138/14 (ECtHR, 12 January 2016) paras 73.

[105] Kühling (n 2) 685.

[106] BVerfG (n 31) para 183ff.

[107] *Digital Rights Ireland* (n 34) para 109.

[108] Kotzur (n 2) 592; Kühling (n 2); Kingreen (n 43) art 52 GRCh, 2985, para 71; Friederike Lange, 'Verschiebungen im europäischen Grundrechtssystem?' 33 (2014) NVwZ 169, 173; Jürgen Schwarze, 'Die Abwägung von Zielen der europäischen Integration und mitgliedstaatlichen Interessen in der Rechtsprechung des EuGH' 48 (2013) EuR 253.

verdict, the German CC from the beginning deemed data retention as a lawful legal instrument for security concerns. The way taken by the German court was to link the strict requirements of justification to a legislative approach on data retention without obstructing the legislative path.

4.4.2 Widespread retention of data of all means of communication and all people without distinctions, limitations or exceptions

The CJEU brandishes the scathing criticism that '… the directive covers all subscribers and registered users. It therefore entails an interference with the fundamental rights of practically the entire European population',[109] and further emphasises that it '… covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception …'.[110] This seems to be a recurring theme through the case law of the CJEU on data protection. In its *ASNEF* case, the Court emphasises the need to consider the concerned rights linked to the processing of data: '… excluding, in a categorical and generalised manner, the possibility of processing certain categories of personal data, without allowing the opposing rights and interests at issue to be balanced against each other in a particular case'. A proportionate consideration of the rights concerned is needed in the case of processing data without the knowledge of people. If people do not know who has control of their data and what happens to personal data, this leads to a sense of constant surveillance of private life with the consequence of restriction, less freedom and curtailed actions.[111] The German CC broadly speaks of a deterrent or intimidation effect.[112] Considering the importance of data protection as a paramount fundamental right, it is understandable to apply a stricter proportionality test than in other cases. The more data protection is restricted, the more strictly proportionality has to be verified. Having the Snowden knowledge in mind, the CJEU demanded data to be retained on the territory of the EU.[113] The German CC was not as demanding. The retention of data could have an effect on the use of means of electronic communication and, consequently, on its exercise by the users thereof. After an evaluation of the effects of interference, the Court again explains its expectation of national legislation to conform to the CFR and the general principles of primary law:

> national legislation must, first, lay down clear and precise rules governing the scope and application of such a data retention measure

[109] *Digital Rights Ireland* (n 34) para 56.

[110] ibid, paras 57, 63; *Tele2 Sverige AB* (n 29) para 51.

[111] BVerfG (n 31) para 212.

[112] Bäcker (n 1) 1267; Markus Oermann and Julia Staben, 'Mittelbare Grundrechtseingriffe durch Abschreckung?' (2013) 52 Der Staat 630.

[113] Bäcker (n 1) 1269.

> and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. That legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary ….[114]

In the light of the principle of proportionality, widespread retention of data is not acceptable, in particular due to the exceptional law principle. Both the CJEU and the German CC doctrinally agree on the importance of this principle. It would be a paradox to generally allow data processing and to make data protection the exception. According to the CJEU, exceptions have to be limited to what is strictly necessary,[115] while the German CC declares that widespread data retention of all people and all means of communication are exceptions which should not serve as a model for surveillance. Surveillance or a police state, as illustrated in George Orwell's *1984*, is to be avoided, not enabled. Processing of data to protect against danger is only permitted if real indications exist for believing that a concrete danger to life, limb or freedom exists.[116] In addition, the German CC requires that further surveillance measures have to be put on the surveillance balance sheet to avoid the state converting itself into a surveillance state.[117] Such an idea allows quantitative evaluations, comparisons and assessments. The inaccuracies of such a balance sheet are not a hindering factor because it only serves as a verification test for the relations of the exceptional-law-principle. It must not be used for precise mathematical calculations.

The CJEU deems interference with data protection through widespread data retention to be extensive and particularly severe. The fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.[118] Analogously, the German CC pronounced that the secrecy of interference strengthens and causes a sense of constant surveillance and diffuse danger.[119] It is an interference of extraordinary weight and depth.[120] Remarkably, the courts describe the seriousness of

---

[114] *Tele2 Sverige AB* (n 29) para 109ff.

[115] *Digital Rights Ireland* (n 34) para 52.

[116] BVerfG (n 31) para 230ff.

[117] ibid, para 218, 228f.

[118] *Digital Rights Ireland* (n 34) para 37.

[119] BVerfG (n 31) para 212, 241f; cf further decisions of the court on interference in Bäcker (n 1) 1267.

[120] BVerfG (n 31) para 210f.

interference by the feelings and subjective view of the people potentially concerned. Objective proof is not needed, and, in any case, it would actually be difficult to prove scientifically or empirically such a subjective view.[121] Already the noticeable reluctance to exercise rights of freedom may be deemed as a limitation of fundamental rights.[122] From the past, it is known that people behave differently in repressive systems. From the point of view of primary law, new doctrinal paths may appear. If the subjective view on fundamental rights has any influence, this may change the examination of interference with fundamental rights and at the same time increase the requirements of justification. Clearly, both courts emphasise that the level of strict necessity or proportionality is stricter in cases where more paramount rights such as data protection are concerned. For state authorities, this means that the legal basis used for interference has to be implemented or applied more thoroughly. Actions have to be better justified, explained and prepared.

4.4.3 Substantive conditions and objective criteria that are clear and precise

Both courts demand more precise, clear conditions and criteria to be set by legislation on data retention. But the clarity and intensity of the specifications of legislation differ between the courts and the different judgments. Although only two years lie between the CJEU judgments in *Digital Rights Ireland* and *Tele2 Sverige*, an extended tonality is given by the Court. The CJEU states in *Digital Rights Ireland* that the Data Retention Directive fails to lay down any objective criteria by which to determine the limits of access to data and their subsequent use.[123] According to the Court, the directive also fails to lay down objective criteria by which the number of persons authorised to access and subsequently use data is limited to what is strictly necessary.[124] Again, the CJEU in *Digital Rights Ireland* criticises the legislator without stipulating minimum requirements. In contrast, the German CC demands the German legislator to define serious crimes in a catalogue. Accordingly, the processing of data is to be allowed only in cases of concrete danger to life, limb or freedom.[125] In its *Tele2 Sverige* decision in 2016, the CJEU describes the need for substantive conditions and objective criteria on justification in a more intense tonality.[126] Accordingly, such conditions may vary with reference to the nature of the measures in question. The Court speaks

[121] Kühling (n 2); Bäcker (n 1) 1267.

[122] Oermann and Staben (n 112) 630.

[123] *Digital Rights Ireland* (n 34) para 60.

[124] ibid, para 62.

[125] BVerfG (n 31) para 230ff.

[126] *Tele2 Sverige AB* (n 29) para 110; for rather strong comments on the advancement in *Tele 2 Sverige* in contrast to *Digital Rights Ireland*, see Alexander Roßnagel, 'Vorratsdatenspeicherung rechtlich vor dem Aus?' (2017) 70 NJW 2017, 696, 697.

not only of serious crime, but of measures for the purposes of prevention, investigation, detection or prosecution. In particular, such conditions should in practice describe the extent of such measures with the public affected. Hence, national legislation must be based on objective evidence to justify a link between data retention and fighting serious crime.[127] Data retention has to contribute to this objective. The Court allows access to data only with regard to individuals suspected of planning, committing or having committed a serious crime or of being implicated one way or another.[128] In this context, the CJEU expressly refers to the decision of the ECtHR in *Zakharov v Russia*.[129]

The question of serious crime essentially has to be dealt under the legitimate objective. According to the CJEU and the German CC, interference with data protection has to be based on such a legal basis. Instead of widespread retention of data, concrete facts of suspicion may serve as a proportionate approach to data protection. What a serious crime is and what degree of suspicion is needed are traditional questions of criminal law. In German legislation, the law of data retention is implemented through the Telecommunications Act and the Code of Criminal Procedure. This shows that the field of data protection is additionally determined by correlating legal fields. Complex thinking is needed to cope with increasing globalisation in all essential areas of law, technology and the economy. This also apparently applies to the principle of proportionality.[130] All these developments require more holistic, hermeneutic approaches from a universal scholarly perspective than fragmented solutions.

It seems that the CJEU is rather cautious concerning other state powers in *Digital Rights Ireland*. Perhaps this is a result of the criticism on its innovative character and the national tendencies within the Member States.[131] *Digital Rights Ireland* left several questions unanswered, creating doubts on the application of EU and national legislation on data retention.[132] The German CC deemed that a new law on data retention was justified.[133] This was a clear message to the German legislator. At the same time, the German CC requires strict limits, minimum requirements and guarantees in particular on organisational and technical means. For its detailed elaborations and governance, the court was criticised on the

[127] *Tele2 Sverige AB* (n 29) para 111.

[128] ibid, para 119.

[129] ibid.

[130] Saurer (n 55) 9; Benedikt Schneiders, *Die Grundrechte der EU und die EMRK* (Nomos 2010) 203.

[131] Schwarze (n 108) 254. For further explanations of fundamental rights, see Werner Schroeder, 'Neues zur Grundrechtskontrolle in der Europäischen Union' (2011) 22 EuZW 462, 466.

[132] Bäcker (n 1) 1265; Kühling (n 2) 683.

[133] BVerfG (n 31) para 183ff.

grounds of separation of powers.[134] From a fundamental rights perspective, the demand for guarantees is a great stride forward in advancing the functions of fundamental rights within primary law.

Digital Rights Ireland may be seen as respectful proceedings of the Court towards the legislator which bases its power very much on democratic legitimation and governmental expertise. The critical, but cautious, judgment of the Court is an expression of respect or judicial self-restraint. The question of *Rechtsfortbildung* (development of law by judicial decisions) v *Kontrolldichte* (density of judicial scrutiny) reflects the dialectic of different general principles of law, mainly democratic legitimation, separation of powers and rule of law.[135] The case law on strict necessity unavoidably leads to an increased *Kontrolldichte* of the court over legislation.[136] This is understandable and necessary in respect of the requirements of coherence by positive law such as article 52(3) CFR. The CJEU can hardly afford to fall below the protection level of data protection recognised by the ECtHR and its Member States.[137] Moreover, there is a question if the CJEU is obliged to increase the level of protection in the spirit of article 52 III 2 CFR after its own clarifications on the paramount importance of data protection. As far as the CJEU stipulates minimum or clear requirements, the Court narrows the freedom of the legislator, and provides governance or direction. But this is a natural dialectic between state powers. In full awareness of the need to protect fundamental rights and ensure an appropriate protection level in the spirit of the rule of law, the CJEU states that the margin of the legislator is limited or reduced by the rights of data protection together with the general principles of law such as proportionality and legal certainty.[138] This is also remarkable, because the CJEU usually provides the legislator with a broad margin of appreciation.

With its clarity in *Tele2 Sverige*, the CJEU provokes a debate on the aforementioned general principles of law such as the separation or balance of powers. But this does not mean that the Court did anything essentially wrong. Overall, the statements are not really new in comparison to *Digital Rights Ireland*, but in *Tele2 Sverige* the Court answers differ-

---

[134] Bäcker (n 1) 1273.

[135] Weiß (n 50) 290; Matthias Klatt and Moritz Meister 'Der Grundsatz der Verhältnismäßigkeit' (2014) 54 JuS 193; Aharon Barak, *The Judge in a Democracy* (Princeton University Press 2006) 164; Ladenburger and Krämer (n 46) art 52 GRCh, 800, para 55; Jarass (n 52) art 52 GRCh 505, para 45ff.

[136] Schroeder (n 131) 462; referring also to other EU institutions, see Andreas Wehlau and Niels Lutzhöft, 'Grundrechte-Charta und Grundrechts-Checkliste – eine dogmatische Selbstverpflichtung der EU-Organe' (2012) EuZW 45.

[137] Weiß (n 50) 290.

[138] *Digital Rights Ireland* (n 34) para 47f; Jarass (n 52) art 52 GRCh 498, para 27.

ent open questions in a clearer tone.[139] In legal literature, *Tele 2 Sverige* is seen more as a decision in terms of legal policy. The Court provided clearer governance regarding a *political and legal* discourse that has now been unfurling for over a decade.[140]

4.4.4 Technical and organisational measures of protection and security

The CJEU demands the Member States to adopt appropriate technical and organisational measures against accidental or unlawful destruction, accidental loss or alteration of data.[141] Irrespective of the content itself, communication data may allow conclusions on the private lives of the people concerned.[142] The ECtHR, in its decisions such as *Leanders* and *Aman*, had already required appropriate data protection through governance, control or conformity.[143] For instance, the legislator may specify conditions of access, storage or destruction. Technical and procedural causality are directly linked to the content of data enabling access or knowledge. Technical procedures may enable restrictions and conclusions on private lives. It would be unjustifiable to formally separate data content from data conditions and to deem the conditions as unimportant procedural issues. The German CC is stricter by claiming that external circumstances may allow conclusions on behaviour and content of communication.[144] To obtain insights into essential parts of privacy or to be able to draw a picture of personality touches on data protection.[145] What else should be the sense of profiling or other communication analysis? The legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and impose minimum safeguards so that the persons whose data have 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.[146] The need for such safeguards is deemed all the greater where personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data.[147] Overall, the Court demands that the protection and security of the data in question be governed in a clear and strict manner in order to ensure their full integrity and confidentiality.[148] Thereby the Court clarifies that

[139] Roßnagel (n 126) 697.
[140] Roßnagel (n 26) 533.
[141] *Digital Rights Ireland* (n 34) para 40.
[142] BVerfG (n 31) para 211.
[143] *Leander v Sweden* (n 9) para 60ff; *Amann v Switzerland* (2000) 30 EHRR 843, para 76ff.
[144] BVerfG - 1 BvR 370/07 of 27 February 2008, para 326.
[145] ibid, para 314.
[146] *Digital Rights Ireland* (n 34) para 54.
[147] ibid, para 55.
[148] BVerfG (n 144) para 313.

single security rules may not be sufficient. The legislator has to ensure the principles of integrity and confidentiality. This is more expressed as a guarantee, an obligation to ensure a certain level of protection preventively and effectively, eg by minimum standards, as a technical or organisational mechanism. This understanding has already been established by the ECtHR in the area of data protection.[149]

In 2008 the German CC made a decision on online searches, the *Online Durchsuchungen* case. To complete data protection through fundamental rights, the German court established the right to the confidentiality and integrity of IT systems.[150] The court deems data security as a framework requirement of data protection. Technical and organisational means as guarantees of a high protection and security level may not depend on economic considerations.[151] The court believes that data protection may be restricted not only content-wise, but also through technical, organisational means. In the digitalised era, infrastructure, devices or other media are gates to data. Hence, the way to data requires complementary protection and guarantees to the content of data itself.

By referring to guarantees, both courts touch on the essentials of fundamental rights functions.[152] The functions and scope of such rights in a contemporary society are no longer seen as narrowed rights of individuals in relation to physical breaches through state authorities. On the other hand, fundamental rights are not accepted as competences to change all democratic, social or economic behaviour, or as legitimation or rules for redistribution or equality. Thus, the question is to what extent state authorities have to protect fundamental rights functionally, preventively or effectively. Traditionally, fundamental rights serve as *status negativus* rights.[153] But it would be insufficient to protect data rights only from direct, serious attacks. Data protection may more effectively be seen from its effects, not from predefined classifications such as physical ones or otherwise, private ones or otherwise.[154] Fundamental rights demand state powers to be active, to ensure the functionality of fundamental rights, for

[149] Robert Uerpmann-Wittzack, 'Die Bedeutung der EMRK für den deutschen und den unionalen Grundrechtsschutz' (2014) 36 JA 916, 917.

[150] Lewinski (n 18) 96, paras 36, 101 para 55; Florian Becker, 'Grundrechtliche Grenzen staatlicher Überwachung zur Gefahrenabwehr' (2015) 34 NVwZ 2015 1335, 1336.

[151] BVerfG (n 31) para 224f.

[152] Margit Bühler, *Einschränkung von Grundrechten nach der Europäischen Grundrechtecharta* (Duncker & Humblot 2005) 462, 467; Hans D Jarras, 'Funktionen und Dimensionen der Grundrechte' in Detlef Merten and Hans-Jürgen Papier (eds), *Handbuch der Grundrechte II* (CF Müller 2006) § 38, 632 para 15ff.

[153] Lewinski (n 18) 103, para 61, 118, para 112; fundamentally Michael Sachs, 'Abwehrrechte' in Detlef Merten and Hans-Jürgen Papier (eds), *Handbuch der Grundrechte II* (CF Müller 2006) § 39, 655ff.

[154] Oermann and Staben (n 112) 632.

instance through procedures or guarantees. In other words, this dimension of fundamental rights may be described by positive obligations.[155] In the area of data protection, organisational and technical means of protection and security are needed to ensure data security. This includes, for example, the obligations of information, disclosure or deletion.[156] Such knowledge is a precondition to effectively exercise fundamental rights, including defence rights. In this sense, both courts speak of sufficient guarantees to protect fundamental rights effectively.[157] Thereby, the courts set higher and higher limits of data protection. In the light of a general right of privacy, every individual has to be free and self-determined in decisions about the release and processing of personal data.[158] The ECtHR derives obligations of protection and guarantee on data protection (German: *Schutz- und Gewährleistungspflichten*).[159]

4.4.5 Retention periods

It is incomprehensible that data may be retained for a period of at least six months without any distinction being made between categories of data on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned.[160] Furthermore, the period is set at between a minimum of six months and a maximum of twenty-four months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.[161] The AG here correctly stipulates that the retention period should also be assessed from the perspective of a regular necessity test, rather than reasonableness.[162] Namely, the question is not whether, from the point of view of the prevention of serious criminal activities, a longer retention and availability period is preferable to a shorter period, but whether, in the context of an examination of its proportionality, there is a specific need for it.[163] The German CC

[155] BVerfG (n 31) para 321; Jarass (n 79) art 8 GRCh 106, para 14; Lewinski (n 150) para 63; Florian Becker, 'Grundrechtliche Grenzen staatlicher Überwachung zur Gefahrenabwehr' (2015) 34 NVwZ 2015 1335; Schroeder (n 131) 464; Christian Calliess, 'Schutzpflichten' in Detlef Merten and Hans-Jürgen Papier (eds), *Handbuch der Grundrechte II* (CF Müller 2006) § 44, 963ff.

[156] Florian Becker, 'Grundrechtliche Grenzen staatlicher Überwachung zur Gefahrenabwehr' (2015) 34 NVwZ 2015 1335.

[157] *Digital Rights Ireland* (n 34) para 54; *Tele2 Sverige AB* (n 29) paras 82, 109, 122.

[158] BVerfG - 1 BvR 209/83 of 15 December 1983, 41ff.

[159] Jens Meyer-Ladewig and Martin Nettesheim in Jens Meyer-Ladewig and Martin Nettesheim and Stefan von Raumer, EMRK (4th edn, Nomos 2017) art 8 - 'Recht auf Achtung des Privat- und Familienlebens' 319, para 3.

[160] *Digital Rights Ireland* (n 34) para 63.

[161] ibid, para 64.

[162] Opinion of AG Cruz Villalón (n 86) para 143.

[163] ibid.

is here more precise because the court precisely refers to a period of six months, not allowing a broader timeframe.[164] Expressly, the court states:

> Actually, a retention period of six months is, due to the extent and significance of the retained data, very long and at the absolute limit of what is justifiable according to proportionality. But after the retention period each individual concerned can rely on the destruction of data and that such data are not reconstructable for anybody, except of such data already accessed due to serious reasons.

The German court is rather definite in its requirements and imposes these obligations on state authorities without the need for individuals to provide reasoned requests. There is no room for extensions of retention time, and data have to be irreversibly destroyed.

4.4.6 Prior court or administrative review of access to data

The CJEU makes criticism that access by competent national authorities to data retained is not made dependent on a prior review carried out by a court or by an independent administrative body.[165] It is remarkable that the Court deems an administrative body in the sense of article 8(3) CFR equivalent to a prior review carried out by a court. Of course, article 8(3) CFR itself offers such a perspective by its wording. But, if data protection is deemed a paramount right, it is hardly enough to allow the processing of data by the approval of an administrative authority. In such a case, one state authority would provide an approval to another state authority. This understanding does not reflect the idea of the principle of separation of powers. According to the wording of article 8(3) CFR, an independent authority is needed. But a view into legal literature shows that this wording is interpreted in the light of the paramount importance of data protection.[166] The requirements are directed more to a totally independent authority that is institutionally, functionally and materially independent.[167] The CJEU itself deemed it necessary to emphasise in *Commission v Austria* in 2012:

> The Court has already held in its judgment in *Commission v Germany*, paragraph 30, that the words 'with complete independence' in the second subparagraph of Article 28(1) of Directive 95/46 must be interpreted as meaning that the supervisory authorities for the protection of personal data must enjoy an independence which allows them to perform their duties free from external influence. The Court also stated in that judgment that those authorities must remain free

[164] BVerfG (n 31) para 205, 208ff.

[165] *Digital Rights Ireland* (n 34) para 62.

[166] Raschauer and Riesz (n 7) art 8 GRC, 115, para 25.

[167] ibid, art 8 GRC, 115, para 26.

> from any external influence, direct or indirect, which is liable to have an effect on their decisions …'.[168]

Only such an understanding supports the idea of such an authority as a guardian of fundamental rights.

The German CC demands a court decision. Administrative bodies are not considered at all. The ECtHR supports this requirement of a judicial review which cannot be substituted through an administrative decision:

> the Court notes the absence of prior judicial authorisation for interceptions … This safeguard would serve to limit the law-enforcement authorities' discretion in interpreting the broad terms of 'persons concerned identified … as a range of persons' by following an established judicial interpretation of the terms or an established practice to verify whether sufficient reasons for intercepting a specific individual's communications exist in each case … A central issue common to both the stage of authorisation of surveillance measures and the one of their application is the absence of judicial supervision. The measures are authorised by the Minister in charge of justice upon a proposal from the executives of the relevant security services …. For the Court, this supervision, eminently political … but carried out by the Minister of Justice who appears to be formally independent of both the TEK and of the Minister of Home Affairs – is inherently incapable of ensuring the requisite assessment of strict necessity with regard to the aims and the means at stake. In particular, although the security services are required, in their applications to the Minister for warrants, to outline the necessity as such of secret information gathering, this procedure does not guarantee that an assessment of strict necessity is carried out …[169]

4.4.7 Economic interests as an influencing factor of protection and security

The German CC clearly states that the protection and security level to be granted must be independent of economic considerations.[170] Independence indicates that any interpretation has to be free of economic reasons. Hence, safety requirements cannot easily be adapted to increasing costs or market challenges. This understanding is not clearly expressed by the CJEU. The Court criticises that the Data Retention Directive does not ensure that a particularly high level of protection and security is applied by those providers by means of technical and organisational measures, but permits those providers in particular to have regard to economic

[168] Case C-614/10 *Commission v Austria* ECLI:EU:C:2012:631, para 41.
[169] *Szabó and Vissy v Hungary* App no 37138/14 (ECtHR, 12 January 2016) paras 73, 75.
[170] BVerfG (n 31) para 224f.

considerations when determining the level of security which they apply, as regards the costs of implementing security measures.[171]

On the other hand, it is remarkable to see how precise and demanding the German CC is towards legislation. With respect to the fundamental rights of the service providers obliged by the legislator on data retention, the German CC requires a consideration of the costs and efforts of providers caused by data retention. Indeed, the German legislator already reacted in its new legislation on data retention in 2015. For specific providers, compensation of damages is foreseen. However, the regulation is questionable with regard to the preconditions of compensation and equal treatment.

4.5 Consequences for the methodology and future application of strict necessity

The intense discussion on proportionality confirms the increasing meaning of, and the need to cope with and apply, this principle.[172] Article 52(1) CFR clearly demands an examination of proportionality as the backbone of justification of fundamental rights. Perhaps the CFR was underestimated, but its effects are enormous and the seriousness of the CJEU confirms its responsibilities concerning fundamental rights.[173] It is not by chance that in the meanwhile there has been a globalisation of the principle of proportionality through constitutionalisation, codification and jurisdiction.[174] This does not mean that only one logic or one means of interpretation or application applies. Although we may see the international reception of proportionality, this does not mean that a universal legal doctrine has been established.[175] Codification and jurisdiction do not automatically accept or design one universal doctrine. Different views exist on how this principle should be structured and applied. As long as the main idea is respected, cultural or other specific requirements of the respective legal system may demand its own interpretation or application.[176] Apparently, proportionality is a rather challenging general principle of law.[177]

Without doubt, proportionality is supported by the case law of the CJEU. The Court clearly states that it is necessary to verify the

---

[171] *Digital Rights Ireland* (n 34) para 67.

[172] Kingreen (n 43) art 52 GRCh, 2985, para 71.

[173] Schroeder (n 131) 462; Weiß (n 50) 287; Daniel Sarmiento, 'Who Is Afraid of the Charter? The Court of Justice, National Courts and the New Framework of Fundamental Rights Protection in Europe' (2013) 50 CMLR 1267.

[174] Saurer (n 55) 9; Schneiders (n 130) 203ff.

[175] Reimer (n 81) 53.

[176] Saurer (n 55) 13.

[177] Florian Becker,'Grundrechtliche Grenzen staatlicher Überwachung zur Gefahrenabwehr ' (2015) 34 NVwZ 1335, 1336.

proportionality of interference to data protection and points out that according to the settled case law of the Court, the principle of proportionality requires that EU actions are appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives.[178] Specifically for data protection, the Court refers to the recitals of Directive 2002/58 pointing out that measures of this kind must be strictly proportionate to the intended purpose.[179] In *Digital Rights Ireland* and *Tele2 Sverige* we can identify a structure or power of proportionality as required in article 52(1) CFR.[180] But the way the Court applies proportionality is not fully comprehensible, logical and consistent.[181] We have shown that the strict necessity of the CJEU in the two analysed judgments is equivalent to a reasonableness test concerning elements of justification. Comprehensibly, the Court starts to examine the essence of data protection and the legitimate objective. But the Court skipped the examination of the elements of appropriateness in *Tele2 Sverige* and necessity in both judgments. Instead, the next element of strict necessity summarises different elements of proportionality under one umbrella. This is a method the CJEU developed for strict necessity even before the *Digital Rights Ireland* and *Tele2 Sverige* judgments and seems to have become established practice for this test.[182] Proportionality in a strictly technical sense expresses the proportion of the single elements of appropriateness, necessity and proportionality in the narrow sense or reasonableness with regard to the legitimate objective.[183] It is clearly a concept of several steps, layers or dimensions, and not free, widespread balancing. The CJEU itself distinguishes between necessity and reasonableness. Necessity chronologically, systematically and teleologically is the first of the two to be examined. Even if the next step is named differently, it is the next and last step of proportionality. There is no need to mix up these elements. It leads to the danger of not examining every single step of the proportionality test to the proper extent, leaving uncertainty for future legislative activities.[184] As shown, necessity is a more scientific, empirical test without the need to be burdened with elements of balancing or normative assessment. There is

[178] *Digital Rights Ireland* (n 34) para 45f; *Tele2 Sverige AB* (n 29) para 96.

[179] *Tele2 Sverige AB* (n 29) para 95.

[180] Kingreen (n 43) Art 52 GRCh, 2985, para 71.

[181] Saurer (n 55) 9; O Koch, *Der Grundsatz der Verhältnismäßigkeit in der Rechtsprechung des Gerichtshofs der Europäischen Gemeinschaften* (Duncker & Humblot 2003) 494ff.

[182] See already in the CJEU judgment in *Volker and Schecke* (n 13); J Kühling and M Klar (2010) Transparenz vs Datenschutz – erste Gehversuche des EuGH bei der Anwendung der Grundrechtecharta (2011) 33 Jura 771, 775.

[183] Reimer (n 174) 41.

[184] Kühling and Klar (n 181) 775.

no need to query legal discipline and confidence through methodological arbitrariness.[185]

Reasonableness or proportionality in the narrow sense is not free of balancing rights.[186] Finally, proportionality in the case law of the CJEU on data protection seems to be very much a question of fair balance with regard to the understanding of the ECtHR.[187] In its case *Volker and Schecke*, the Court expresses the closer link of balance to proportionality by speaking of a proper balance.[188] The balancing character of reasonableness may be more anchored in the spirit of article 52(1) CFR by the logic of proportionality. Instead of pure balancing, the German CC is very much focused on the content of each single right, its proportion towards the legitimate objective and the correlations among the concerned rights.[189] Additionally, proportionality consists of a logic in sequences. First, rights may be examined generally, and, second, each individual case treated individually.[190] This may lead to differing results. Ultimately, balancing is only a consequence of legal reasoning, not a simple weighing and defining of the content, limits or significance of fundamental rights.[191] Often, balancing is used to criticise proportionality, while proportionality is often used as a knockout argument to blur clarity and precision.[192] But the logic followed here shows that, before balancing, the different elements of proportionality serve to achieve a more neutral, logical, scientific and legal view on justification, even if balancing may finally be needed. The formal structure and logic has to be distinguished from the external factors with their impact on the different rights concerned.[193]

---

[185] Thomas von Danwitz, 'Der Einfluss des nationalen Rechts und der Rechtsprechung der Gerichte der Mitgliedsataaten auf die Auslegung des Gemeinschaftsrechts' (2008) 7 ZESAR 57, 61.

[186] Konrad Hesse, *Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland* (20th edn, CF Müller 1995) 317; Klatt and Moritz (n 133) 194; Werner Schroeder, *Das Gemeinschaftsrechtsystem* (Mohr Siebeck 2002) 281; Reimer (n 174) 35.

[187] Case C-275/06 *Promusiciae* ECLI:EU:C:2008:54, para 68; Joined Cases C-468/10 and C-469/10 *ASNEF* ECLI:EU:C:2011:777 paras 43, 47f; Jarass (n 52) art 52 GRCh 500, para 33, 503, para 41, 510, para 59ff.

[188] *Volker und Schecke* (n 13) paras 77, 86.

[189] BVerfG (n 31) para 320.

[190] Andreas Wehlau and Niels Lutzhöft, 'Grundrechte-Charta und Grundrechts-Checkliste – eine dogmatische Selbstverpflichtung der EU-Organe' (2012) 23 EuZW, 45, 48; for instance, concretely on the legitimate objecive within the frame of proportionality, see Sebastian Kluckert, 'Die Gewichtung von öffentlichen Interessen im Rahmen der Verhältnismäßigkeitsprüfung' (2015) 55 JuS 116.

[191] Reimer (n 174) 33.

[192] Klatt and Moritz (n 133) 195; Florian Becker, 'Grundrechtliche Grenzen staatlicher Überwachung zur Gefahrenabwehr' (2015) 34 NVwZ 2015 1335, 1336; Reimer (n 174) 27, speaking of proportionality as a ghost, as a standard argument, as a plasticiser or conditioner.

[193] Klatt and Moritz (n 133) 198.

The doctrine of proportionality serves as a framework and limitation of free balancing of opinions and interests. It is crucial that reasonableness fully respects the different general principles of law and follows the recognised legal methodology. Symbolically, Sweet and Mathews speak of proportionality balancing.[194] Balancing by people can hardly be assessed as purely objective. People, including judges, are by nature subjective. But this does not mean to support personal opinions, decisionism or conceptual jurisprudence.[195] Different elements have to be considered on the basis of general principles of law and recognised legal methodology. For example, the principle of proportionality is framed and strengthened by the principle of legal certainty.[196] Repeatedly, the CJEU requires clear, precisely defined regulations. Thereby, the Court within strict necessity refers to the principles of legal certainty.[197] Balancing is framed by positive law, rights and general principles. It cannot be determined by any interest. Factual and legal arguments have first to be hermeneutical evaluated according to positive law and the factual circumstances.[198] Thus, elements of necessity have to be examined in a state-of-the-art approach without normative assessment. In this sense of legal technique, balancing is primary not a question of objectivity, but of legal assessment.

5 Reaction of the German legislator: conformity to proportionality and data protection in EU law?

In light of the judgments on data retention, it is worth seeing the new legislation on data retention by the German legislator in 2015.[199] Following the German CC, the legislator foresaw rather high, detailed justification needs for data retention in this new law.

The state-of-the-art approach with regard to organisational and technical means is a recurring theme through the new legislation, in particular expressed in § 113 d of the Telecommunications Act. Pursuant to § 113 b VIII of the Telecommunications Act, providers are obliged to destroy data irreversibly as soon as possible after the end of the data retention period, at the latest within one week. The destruction has to be done according to the state of the art of the technology, as indicated in §

---

[194] Alec Stone Sweet and Jud Mathews,'Proportionality Balancing and Global Constitutionalism' (2008) 47 Columbia Journal of Transnational Law 72.

[195] Reimer (n 174) 34.

[196] cf comments on legal certainty on the grounds of Art 52(1) CFR, Jarass (n 52) art 52 GRCh 498, para 27; Florian Becker, 'Grundrechtliche Grenzen staatlicher Überwachung zur Gefahrenabwehr' (2015) 34 NVwZ 2015 1335, 1336.

[197] Becker (n 195) 1335, 1336.

[198] Reimer (n 174) 48.

[199] 'Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten' BGBl I 2015, 2218; Roßnagel (n 126) 697f; Roßnagel (n 26) 534.

113 f. Further, § 113 e I of the Telecommunications Act demands meeting minutes for each destruction. According to § 113 d-g of the Telecommunications Act, organisational and technical means have to be state of the art to guarantee data security and protection. Specific encryption methods have to be used, access has to be granted only by a four-eyes principle and data have to be stored in the intranet separately from data processing systems. Minutes have to record each access to or processing of data (§ 113 e).

Other essential amendments were made in the Code of Criminal Procedure to enable the processing of data for prosecutions. This shows that the German legislator thinks in two directions: the preventive, urgent averting of danger, and repressive prosecution.

Two regulations of the new German law hardly conform to the judgment in *Digital Rights Ireland*.

Firstly, the legislator limited the privilege of professional secrecy only to people belonging to the scope of § 99 II of the Telecommunications Act instead of protecting all professional bearers of secrets.[200] This scope only captures activities in the area of the church or social professions. But the German CC only referred to § 99 II of the Telecommunications Act as an example.[201] Moreover, the court pronounces that professional secrecy in this context has to be deemed as an expression of the principle of proportionality. Now, other people, such as lawyers or doctors, obtain protection of professional secrecy when prosecution authorities start with the enforcement of a law. This is already clarified by § 53 I of the Code of Criminal Procedure. Here the CJEU was much more protective. The Court required a privilege for all professional bearers of secrets.

Secondly, the main criticism refers to the general permission on data retention. Only subsequent use of data follows specific, strict requirements. But it is worrying that the German legislator takes the judgment of the German CC literally and did not align its legislation in 2015 with the main message given by the CJEU on data retention in *Digital Rights Ireland* in 2014. The new German law allows the retention of traffic data for ten weeks without any reason, and location data from mobile communication for four weeks. In such a general, widespread manner, data retention does not conform to the spirit of *Digital Rights Ireland*.[202] Such a widespread approach is not really what is strictly necessary.[203] Even

[200] Julia Kleen and Andreas Riegler, 'Big Brother lässt grüßen – Vorratsdatenspeicherung die Zweite!' (2017) 14 Ad Legendum, 59, 65; Nachbaur (n 40) 216; Roßnagel (n 126) 698; Roßnagel (n 26) 538.

[201] BVerfG (n 31) para 238.

[202] Roßnagel (n 126) 698; Roßnagel (n 26) 538.

[203] Nachbaur (n 40) 216.

the German CC indicated that the widespread, preventive retention of all data cannot be the goal of legislation.[204] The restriction of data protection must remain an exception.

6 Conclusion

Direct access to the content of communication compromises the essence of the right to private life, as fundamentally concluded by the CJEU in *Schrems*. In addition, permitted access needs to be on a generalised basis. Indirect knowledge of the communication content, by the retention of other communication data that allow very precise conclusions on the private life of the people concerned, does not compromise the essence of the right to private life. This is the conclusion drawn from *Digital Rights Ireland* and *Tele2 Sverige*.

The strict necessity test applies to all elements of the proportionality test: the legitimate objective, appropriateness, necessity and reasonableness. The importance of the right to data protection requires that all of these elements are examined more strictly. Strict necessity is not just a stricter necessity test. In *Digital Rights Ireland* and *Tele2 Sverige* the CJEU did not examine necessity at all. Although 'quick freeze' and 'quick freeze plus' were worth examining as being possibly less onerous, the CJEU skipped the test. This was an opportunity missed, considering that the CJEU in the *Volker and Schecke* judgments applied 'strict necessity' in the form of stricter necessity. It lowered the standard for the necessity test by not requiring the alternative means to be equally effective, but just a 'still effective contribution'. Such a lower standard makes it much harder for the legislator to pass the necessity test for data retention. Strict necessity further requires the legitimate objective to be restricted to preventing and detecting precisely defined serious offences, and not just any serious crime.

The case law on strict necessity unavoidably leads to increased *Kontrolldichte* of the Court over legislation. The critical, but still cautious, judgments of the CJEU in *Digital Rights Ireland* and *Tele2 Sverige* are an expression of judicial self-restraint. The German CC, with different democratic legitimation, goes further. The German legislator, with its new legislation on data retention in 2015, still gets it wrong. By allowing data retention in a general manner, it goes against the spirit of the *Digital Rights Ireland* judgment.

Each element of proportionality has to be seen individually within a logical structure, not as a mass under an umbrella. Although the CJEU supports the idea of proportionality following positive law in article

[204] BVerfG (n 31) para 218.

52(1) CFR, the Court unnecessarily raises questions through its general approach on proportionality. It seems that if one or more elements are disproportionate, then this is sufficient. But then the Court evokes confusion on legal discipline and confidence. The power of proportionality lies in its logic and sequences. Proportionality may firstly be approached generally, looking at the significance and weight of each element, and, secondly, at the individual case where the significance and weight may change. In the end, we have the link of doctrinal and case law approaches. Pure or summarised balancing is not the intended purpose.[205] The abstract testing of rights should be independent and followed by a test in each individual case. Rights may have another weight or intensity in a specific case. Instead of simple balancing, the necessity test requires a state-of-the-art approach based on the best possible knowledge and empiricism to ensure effectiveness. This is not a question of normative assessment, but of fair or proportional balancing in the spirit of practical concordance. Reasonableness in the spirit of practical concordance requires the maximum preservation of rights in the light of the principle of coherence. Instead of summarised balancing, it should be clear which elements of proportionality cause disproportionality or invalidity, and to what extent. This is the basis of legal security and of the legal system as a whole.

[205] Reimer (n 81) 36.