THE GERMAN CONSTITUTIONAL COURT JUDGMENT ON DATA RETENTION: PROPORTIONALITY OVERRIDES UNLIMITED SURVEILLANCE (DOESN'T IT?)[1]

Katja de Vries, Rocco Bellanova, Paul De Hert & Serge Gutwirth

1. Introduction

On 15 March 2006, the Data Retention Directive, demanding the retention of telecommunications data for a period of six months up to two years, was adopted.[2] Since then, this seemingly straightforward directive has 'generated' quite an impressive number of court judgments. They range from the European Court of Justice[3] (ECJ) to the administrative (e.g. Germany[4] and Bulgaria[5]) and constitutional courts (e.g. Romania[6]) of some Member-States.

In particular, the judgment of the German Federal Constitutional Court,[7] delivered on 2 March 2010, has already caught the attention of several commentators, from civil society, lawyers, journalists and politicians (cf. infra, section 4). In the judgment, the Court annuls the German implementation laws of the Data Retention Directive.

This paper has two main goals. On the one side, it aims at offering a first critical overview of this important judgment, highlighting some of the key features of the ruling and its main similarities and divergences with other similar judgments. On the other side, given the relevance of the issues at stake, it aims at contextualizing the judgment in the wider framework of European data processing and protection debates, assuming a critical posture on the increasing emphasis on proportionality as the "golden criterion" to assess and limit surveillance practices.

---

[1] Earlier versions of this article have been published on the 23rd of March 2010 at the TILT Weblog for Law and Technology (http://vortex.uvt.nl/TILTblog/?p=118) and on the 18th of May 2010 in the CEPS Liberty and Security in Europe - publication series (http://www.ceps.eu/book/proportionality-overrides-unlimited-surveillance). The authors want to thank Patrick Breyer (*AK Vorratsdatenspeicherung: German Working Group against Data Retention*) and Caspar Bowden (*Microsoft*) for their salient comments.

[2] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC OJ L105, 13.04.2006. Hereinafter: Data Retention Directive. Available at: http://eur-lex.europa.eu/ LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

[3] Judgment of the Court (Grand Chamber) of 10 February 2009 - Ireland v European Parliament, Council of the European Union (Case C-301/06) *(Action for annulment - Directive 2006/24/EC - Retention of data generated or processed in connection with the provision of electronic communications services - Choice of legal basis)*. Available at: http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=EN&Submit=rechercher& numaff=C-301/06

[4] Administrative Court of Wiesbaden, 27 February 2009, file 6 K 1045/08.WI. See Commentary in English: http://www.vorratsdatenspeicherung.de/content/view/301/79/lang,en/

[5] Decision no. 13627, Bulgarian Supreme Administrative Court ('Върховния административен съд'), 11 December 2008. Original text available at: http://www.econ.bg/law86421/enactments/article153902.html. Commentary in English: http://www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention

[6] Decision no.1258, Romanian Constitutional Court, 8 October 2009. Published in the Romanian Official Monitor, no. 789, 23 November 2009. English translation (unofficial): http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf

[7] *Vorratsdatenspeicherung* [Data retention] BVerfG 2 March 2010, 1 BvR 256/08. Available at: http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.htmll. Hereinafter: the judgment or the German Court judgment.

2. The 2 March 2010 judgment

2.1. Background

In its judgment of 2 March 2010 the German Federal Constitutional Court abrogated the national implementation of the data retention directive: Art.113a and 113b of the *Telekommunikationsgesetz*[8] (TKG), i.e., the Telecommunications Law, and Art. 100g, paragraph 1 sub 1, of the *Strafprozeßordnung*[9] (StPO), i.e., the Criminal Procedural Code, in combination with the aforementioned Art 113a TKG. This legislation, which was originally passed by the Bundestag on 9 November 2007 and entered into force on 1 January 2008, imposed the retention of information about all calls from mobile or landline phones for six months, including who called whom, from where and for how long. In 2009, the law was extended to include the data surrounding e-mail communications as well. This being said, the law did forbid authorities from retaining the contents of either form of communication.

Since its adoption, the German national implementation law had met considerable resistance. On 31 December 2007 on the eve of its entry into force, the German privacy group *Arbeitskreis Vorratsdatenspeicherung* (AK Vorrat: Working group on data retention) filed a constitutional complaint with the German Federal Constitutional Court. The complaint was backed by more than 30,000 people, and requested, *inter alia*, the immediate suspension of the law.[10] The judgment of 2 March 2010 is the outcome of this complaint.

2.2. The main findings: a proportionality check

The case could have been tricky and threatening for EU law, but the German Court did not criticize the EU directive itself, arguing that the problem lay instead with how the German Parliament chose to interpret it. The German legislation was found to breach art. 10 paragraph 1 of the German Constitution (*Grundgesetz*[11]) which ensures the privacy[12] of correspondence and telecommunications (the so-called "Fernmeldegeheimnis" or "Telekommunikationsgeheimnis"). The text of the German Constitution protects communication in what might be termed an old-fashioned way. Article 10 of the German Basic Law seems to suggest that we still communicate by writing letters, but through the activity of the Court the protection goes well beyond the paper medium. All forms of (tele)communications are in fact protected, and this protection does not only cover the content of the communication, but it reaches also out to the data about this communication.[13] In the judgment of 2 March 2010, the Court stated that: "the protection of communication does not include only the content but also the secrecy of the circumstances of the communication, including especially if, when and how many times some person (…) contacted another or attempted to." (section 189)

---

[8] Available in German at the "Juristische Informationsdienst": http://dejure.org/gesetze/TKG/113a.htm, and http://dejure.org/gesetze/TKG/113b.html

[9] Available at http://dejure.org/gesetze/StPO/100g.html, ibid.

[10] Available in English at the website of the "Arbeitskreis Vorratsdatenspeicherung": http://www.vorratsdatenspeicherung.de/content/view/184/79/lang,en/

[11] Available in German at the website of the German Bundestag: http://www.bundestag.de/dokumente/rechtsgrundlagen/grundgesetz/gg_01.html

[12] Privacy is not mentioned in the German Constitution, but the German Court has developed a broad right to privacy and "informational self-determination" ("das Recht auf informationelle Selbstbestimmung") as tenets of the right to human dignity in Article 1 of the Constitution in its famous 1983 "Census Decision". BVerfG [Judgments of the Federal Constitutional Court] 15 December 1983, (*Volkszählung*), *BVerfGE* 65, 1. The plaintiffs in the German data retention case also claimed that the national implementation laws infringed both their right to informational self-determination and their privacy of telecommunication (art 10 GG), but the annulment of the Court was only based on the infringement upon the latter.

[13] This is indeed fully in line with the case law of the Strasbourg Court: ECrtHR, *Malone vs. UK*, 2 August 1984

Hence, the German Constitution also applies to the data that are the object of the retention measures. But this does not necessarily mean that the implementation law is unconstitutional. So how did the German Court come to the conclusion that the implementation law, doing no more than implementing EU legislation, breaches Article 10 of the Constitution?

As also remarked by Mohini, the Court bases its analysis on a "privacy test" similar to the one developed by the European Court of Human Rights.[14] From Strasbourg's point of view, the "privacy test" as contained in the second paragraph of Article 8 of the European Convention on Human Rights (ECHR),[15] not only requires a check of the quality of the legal basis,[16] but also of the legitimate aim and proportionality of the proposed initiative. We will see in the following that the German Court follows this scheme and carries out a check of the three requirements. It is however useful to observe that the European Court sees minimum safeguards with regard to data (e.g. safeguards on duration; storage conditions; usage, access by third parties and preserving the integrity of data) as being part of the first requirement (legality requirement),[17] whereas the German Court sees these safeguards as elements of the third requirement (proportionality). We will come back to this. Now let us turn to the privacy check by the German Court in the judgment of 2 March 2010.

As all the transposition laws were made with the proverbial German accuracy, the first requirement (legality) was not the problem. With regard to the second (legitimacy) the German Court found that a six-month retention period can be legitimate in principle: firstly because under the current laws the data are stored in a dispersed manner by private actors (section 214). Secondly, such data retention is in accordance with the challenges posed by the current era:

> "Storage of telecommunication traffic data for the period of six months is also not a measure which aims at the complete interception ("eine Totalerfassung") of the communication and activities of citizens as a whole. Much more it ties in, in a rather restrained manner, to the special significance of telecommunications in the modern world and it reacts to the specific potential danger which it brings along. The new means of telecommunication overcome time and space in a way which is incomparable to other forms of communication and basically exclude public observation. Thus these new means make it easier for criminals to communicate and act in a hidden way and enables dispersed groups of a few persons to find each other and effectively collaborate with each other […] Thus precisely the reconstruction of connections by means of telecommunication is of special significance for effective criminal prosecution and the prevention of dangers". (section 216)

---

[14] Mohini, (2010), 'On the BVG ruling on Data Retention: "So lange" – here it goes again…', 13 April, available at http://afsj.wordpress.com/2010/03/05/so-lange-here-it-goes-again/.

[15] Article 8 of the European Convention on Human Rights states: "Everyone has the right to respect for his private and family life, his home and his correspondence" (first paragraph); "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others" (second paragraph).

[16] The legality principle is expressly laid down in Articles 2, 5, 6 and in the second paragraphs of Articles 8 to 11. Interferences by the executive with the rights and freedoms of the individual should not be permitted unless there is a clear legal basis to do so. By the same token, individuals should be able to predict with reasonable certainty when and under what conditions such interferences may occur. Hence the need for a legal basis to be accessible and foreseeable are key features of the first requirement of the privacy check

[17] The Court recalls in its well established case-law that the wording "in accordance with the law" requires the impugned measure both to have some basis in domestic law and to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus be adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual – if need be with appropriate advice – to regulate his conduct. For domestic law to meet these requirements, it must afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise" (ECtHR, *Case of S. and Marper versus the United Kingdom*, Application nos. 30562/04 and 30566/04, Strasbourg, 4 December 2008, § 95 with ref. to ECtHR *Malone v. the United Kingdom*, 2 August 1984, *Series A* no. 82, §§ 66-68; ECtHR *Rotaru v. Romania* [GC], no. 28341/95, *ECHR* 2000-V, § 55; and ECtHR, *Amann v. Switzerland* [GC], no. 27798/95, *ECHR* 2000-II, § 56).

However, while the Court holds that the current legislation is in principle legitimate and not contrary to the German Constitution, it also notes that this would not be the case for more all-encompassing and intrusive legislation:

> "In contrast the retention of telecommunication traffic data should not be understood as a stepping stone towards a legislation which aims at a potentially blanket measure of preventive data retention which stores all data which could be useful for the prosecution of crime or prevention of dangers. Such legislation would be, irrespective of the regulations concerning its usage, would be a priori incompatible with the Constitution". (section 218)

Yet, even though the Court deemed the contested national data retention laws not to be unconstitutional in principle, it did acknowledge that these measures do constitute a heavy infringement ("schwerwiegender Eingriff", section 212) . Such measures:

> "largely increase the risk of citizens to be the subject of further investigations, although they did not do anything wrong. It is enough to be at a wrong time (…) contacted by a certain person (…) to be under an obligation to provide justifications", [and further in the judgment that the preventive collection of data] which "can establish a feeling of permanent control" [and] "diffuse threat" ("diffuse Bedrohlichkeit"). (sections 212 and 242)

Because of the heavy infringements that such data retention can bring along, the major problem with the German implementation laws was that they did not satisfy the third requirement of proportionality. This requirement involves, at least in the German Court's understanding, that the transposition laws should contain regulations that are in accordance with all requirements of *legality* ("normenklare Regelungen"). Thus, contrary to Strasbourg's interpretation, proportionality is not directly discussed as part of the more sensitive criterion of *necessary in a democratic society*. Following the proportionality check the Court concludes that, while the idea underlying data retention is not "absolutely incompatible with Art.10 of the German Constitution (protecting the privacy of telecommunications)*"* (section 205), its application in national law did not meet the constitutional need for proportionality, which can be subdivided into four criteria:

(i) proportional data security standards. Given that data retention is a very heavy infringement, the threshold for those standards should be set very high;

(ii) proportional purpose limitation. When direct use of data is sought, and thus the possibility to create very detailed behavioral profiles is at stake, these standards should be very high (only in case of "schwerwiegende Straftaten", i.e. heavy crimes). However, the Court assesses indirect use (as in the case of requests to a service provider for the identifying information that belongs to an IP-address) as a less intrusive practice, and thus the standards concerning purpose limitation can be more lenient (no need for an exhaustive catalogue);

(c) transparency. This criterion aims at counter-acting the feeling of "diffuse threat" (discussed in section 242): using data without knowledge of the involved should only be allowed if the purpose of the investigation would become jeopardized otherwise, and if the involved people are at least notified afterwards. This criterion applies both to direct and indirect use of the data;

(d) judicial control and effective legal remedies. Proportionality requires that in case of direct use there should be judicial control, while in the case of indirect use this is not necessary.

None of these requirements were met. Seven out of eight judges (section 308) therefore agreed that the national transposition laws infringed upon art. 10, paragraph 1, of the German Constitution. After suspending the law several times during interim proceedings, the Court

annulled[18] it in its final judgment. All data already collected by carriers and providers had to be deleted.

2.3. The German Court on access and use and the role of private companies

According to the Constitutional Court it is important to distinguish between the mere retention and the actual access and use of data. In practice this difference is expressed by the fact that the data are not directly accessible as they are stored by a multiplicity of private companies (telecommunications services and providers). Although the complaints concerning the excessive economic burden of data retention on these companies were not accepted, their remarkable consolation prize was that the court assigned them the constitutionally pertinent and important role of incorporators of the distinction between storage and access. The private and dispersed nature of the collection and retention of data was thus welcomed by the German Federal Constitutional Court as something very positive. The fact that the obligation to retain data rests with private service-providers even became a "decisive element" for the assessment of the "non-unconstitutionality" of the principle of data retention. In fact, "when the data are stored, they are not gathered in one place, but they are scattered over many private companies and thus they are not at the State's disposal as a total collection. More importantly the State does not have (…) direct access to the data" (section 214 of the judgment).

Thus, while clearly stating that "the retention of telecommunication traffic data should not be understood as a step towards a legislation that aims at a potentially blanket measure of preventive data retention" (section 218), the Constitutional Court seems to identify a fundamental guarantee in the two-step procedure: a general but dispersed retention by private actors followed by a justified direct or indirect use by public actors. However, following up on the judgment of the German Federal Constitutional Court , the German Federal Commissioner for Data Protection, Peter Schaar, said in an interview with the *Focus* magazine that the data retention practised by private companies such as Google and Facebook should also be limited: "After all, private data collections of large companies, such as Google, are much more precise, extensive and more meaningful than that what is captured by a retention that was ordered by a state".[19] This raises not only the question of how large private actors can be without endangering the dispersed character of the retention, but also of the relativity of the notion of "dispersion" given the existence and availability of powerful data mining and aggregative software tools

Another important elaboration by the German Federal Constitutional Court with regards to the use of the retained data is the distinction between 'direct' and 'indirect' use of data by law enforcement authorities and secret services. On the one hand, direct use is particularly sensitive and needs stronger safeguards, because it can lead to the construction of behavioural and mobility profiles. In particular, stricter rules have to apply to secret services. On the other hand, indirect use, namely the possibility for officials to request of service providers that they inform them of the holders of connections with specific IP addresses, requires "less strict guidelines". Because the Court deems the indirect use of data to be a relatively light infringement, the purpose limitation for such requests is proportionally light: "the production of such requests for

---

[18] Judge Schluckebier wrote an extensive dissenting opinion in which he argues that the retention of mere location and traffic data, particularly when executed by private companies and not by the state itself, does not infringe upon art. 10,1, GG. According to Schluckebier data retention cannot be compared to truly intrusive infringements such as the acoustic surveillance of private premises or remote searches of information technical systems (section 314). Moreover he points at the need for judicial self-restraint in order to give the legislator more room to create regulations which it deems necessary. However, while the majority of the judges agreed that the transposition laws infringed upon the German Constitution, the question whether the law should be declared nullified (which implied that all stored data had to be erased immediately) or whether the legislator should get the opportunity to adapt the laws during a set period of time in which the data would be kept, was a harder question: with four out of eight judges in favor of the latter (section 309), it was a really close call that the transposition laws were completely nullified.

[19] Online Focus (2010, 06.03.2010). Bundesdatenschutzbeauftragter: Google, Facebook & Co. Reglementieren. *Online Focus*, from http://www.focus.de/digital/internet/bundesdatenschutzbeauftragter-google-facebook-und-co-reglementieren_aid_487099.html

information is independent of an exhaustive catalogue of legal interests or criminal offences, and can be allowed more widely than the request and the use of telecommunication traffic data themselves." (section 254)

2.4. Other important findings

As widely discussed by journalists, the German Federal Constitutional Court stresses that what should be prevented at all costs is the creation of an opaque, blanket and centralised data retention that can engender a 'feeling of unease' with the citizens. In the words of the Court:

> "a preventive general retention of all telecommunications traffic data (…) is, among other reasons, also to be considered as such a heavy infringement because it can evoke a sense of being watched permanently (…). The individual does not know which state official knows what about him or her, but the individual does know that it is very possible that the official does know a lot, possibly also highly intimate matters about him or her" (section 241).

This is why such a "diffuse threat" should be "counteract[ed] (…) by effective rules of transparency" (section 242). The Court's posture on "unease" is quite a strong official acknowledgment of the potential perverse effects of wide, even if soft, surveillance measures on individuals' lives.[20]

The Constitutional Court also underlines (section 238) that "as a product of the principle of proportionality" there has to be "a fundamental prohibition of transmission of data, at least for a narrowly defined group of telecommunications connections which rely on particular confidentiality"[21]. The Court continues that these "might include, for example, connections to persons, authorities and organisations in the social or ecclesiastical fields which offer advice in situations of emotional or social need, completely or predominantly by telephone, to callers who normally remain anonymous, where these organisations themselves or their staff are subject to other obligations of confidentiality in this respect".

Notwithstanding the attempt of the German Constitutional Court to keep national and EC matters separate from each other (cf. infra, section 3.1), the judgment also provides some reflections that can give food for thought on the EC level. In particular this is the case with regard to the question of whether location and traffic data that have to be stored according to the Data Retention Directive (2006/24/EC) should be considered personal data as defined in Art. 2(a) of the Data Protection Directive 95/46/EC:

> "'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

Although the German Federal Constitutional Court does not make any explicit reference to the notion of personal data in the Data Retention Directive, it recognises that location and traffic data also deserve protection, because technologies can extract from their processing important, and sometimes even sensitive, personal data. Because the Court was reluctant to pose a preliminary question to the ECJ and underlined the importance of Germany's constitutional identity, it also let the opportunity pass to take a stance with regard to how its judgment relates to similarly important questions within the EU directive. Even though it is understandable that

---

[20] For a critical overview of the shift towards a "soft surveillance" approach in law-enforcement, cf. Marx, G. T. (2006)., 'Soft Surveillance. The Growth of Mandatory Volunteerism in Collecting Personal Information - "Hey Buddy Can You Spare a DNA?'. In T. Monahan (Ed.), *Surveillance and Security. Technological Politics and Power in Everyday Life*. New York/London: Routledge.
[21] Press release in English: http://www.bverfg.de/pressemitteilungen/bvg10-011en.html

the court did not want to get its fingers burned, it would have been interesting if the Court had taken the debates on the European level into consideration more explicitly. Thus, for instance, it could have been interesting if the Court would have taken into account the Working Party (WP) 29 Opinion (2007) on the definition of personal data. In this, not uncontested, opinion[22] the Working Party stated that dynamic IP addresses should be treated as personal data, unless the ISP can establish with "absolute certainty that the data correspond to users that cannot be identified": but in practice this is almost impossible to ascertain. Also, the Court did not take into account Directive 2002/58/EC, the so-called e-Privacy Directive, that provides for a distinctive protection of traffic and location data. The rationale of this protection is that these data can threaten privacy even if they are not personal data (which implies that "privacy" and "data protection" cannot be reduced one to the other, although they do surely overlap).[23]

3. The German Constitutional Court judgment and Europe

3.1. Fundamental rights and data retention

In order to get to the 'core of the problem' the plaintiffs who addressed themselves to the German Federal Constitutional Court had hoped that the Court would pose a preliminary question about the constitutionality of the Data Retention Directive to the ECJ. However, the Constitutional Court did not deem such a preliminary question necessary. The questions we want to consider here are the following: When is the constitutionality of the data retention legislation part of the jurisdiction of the German Federal Constitutional Court and when is it part of the powers of ECJ? And what is the difference between mere retention and actual access to the data?

The German Court has on several occasions shown a reluctance to accept an unconditional and full supremacy of EC law. In the Solange II case[24] it famously stated that "as long as" ("so lange") the EC "ensured an effective protection of fundamental rights" that were "substantially similar" to that of the fundamental rights safeguarded by the German Constitution, the German Court would "no longer exercise its jurisdiction to decide on the applicability of secondary Community legislation". Recently, in the complex and controversial Lisbon Judgment, the German Court took an even more outspoken stance and showed its constitutional teeth towards EC law.[25] In this judgment it held that the primacy of Community law could never infringe upon the constitutional identity of the Member-States (identity review, section 240) and should not transgress its competences (*ultra vires* review, section 240).[26] Even though it is difficult to say whether the judgment should be characterised as a triumph of nationalist euroscepticism or of constitutionalism, it has in any case become clear once more that the relationship between EC law and the German Constitutional Court C is far from an unequivocal given.

If we keep this in mind, and return to the data retention judgment of 2 March 2010, it is noteworthy to stress how the German Federal Constitutional Court avoids referring the case to

---

[22] Article 29, Data Protection Working Party (2007). *Opinion 4/2007 on the concept of personal data*. Brussels. Available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

[23] Cf. Gonzales-Fuster, G. & Gutwirth, S., 'Privacy 2.0 ?', *Revue du droit des Technologies de l'Information*, Doctrine, 2008, 349-359.

[24] *Solange II - Wünsche Handelsgesellschaft*, 22 October 1986, BVerfGE 73, 339, 2 BvR 197/83. English translation: *Wünsche Handelsgesellschaft* [1987] 3 CMLR 225.

[25] BVerfG 30 June 2009, 2 BvE 2/08 (*Lisbon*). A preliminary English translation: http://www.bundesverfassungsgericht.de/entscheidungen/es20090630_2bve000208en.html See also: Steinbach, A. (2010). The Lisbon Judgment of the German Federal Constitutional Court – New Guidance on the Limits of European Integration? *German Law Journal, 11*(4), 367-390; Lanza, E. (2010). Core of State Sovereignty and Boundaries of European Union's Identity in the Lissabon – Urteil *German Law Journal, 11*(4), 399-418.

[26] *Ultra vires* review is a concept that has already been around for a while in the case law of the German Court, the identity review was a new concept which was forwarded in the *Lisbon* judgment.

the ECJ with a preliminary question. In the sections 80-83 the Court briefly discusses the European legal context: it gives some bibliographical references to articles that raise doubts about the compatibility of Directive 2006/24 with European fundamental rights and refers to case C-301/06, 10 February 2009. In this case the ECJ rejected the claims that the Directive should be annulled because of its adoption within the first pillar (i.e., Art. 95 EC Treaty) instead of the more appropriate third pillar: according to the ECJ the first pillar is the correct legal basis. The way in which the German Court uses this judgment as an argument to avoid and circumvent a preliminary question to the ECJ is ingenious. After the general observation that Directive 2006/24 only ordains the storage of data for a period of at least six months, and does not give any prescriptions regarding the access and use of the data (section 186) it points out that this leaves a large margin of appreciation ("einen weiten Entscheidungsspielraum") to the national legislator. Looking at the ECJ judgment, this large margin of appreciation seems only natural to the German Court: after all, if the Directive has rightly been construed as a first pillar measure its main object is the establishment and functioning of the internal market, whereas its applicability with regards to the detection, investigation, and prosecution of crime has to be considered as the responsibility of individual Member-States. Henceforth, the regulations of the Directive do

> "neither harmonise the question of access to data by the competent national law enforcement authorities nor the question of the use and exchange of this data between these authorities (cf. ECJ, C-301/06, 10 February 2009, section 83). Based on the minimal requirements of the Directive (Articles 7 and 13 of Directive 2006/24/EC), the Member States are the ones who have to take the necessary measures to ensure data security, transparency and legal safeguards" (section 186).

Even more telling is section 218 of the 2 March 2010 judgment, wherein the Court refers again to the notion of "constitutional identity" of its own Lisbon Judgment:

> "That the free perception of the citizen may not be completely captured and subjected to registration, belongs to the constitutional identity of the Federal Republic of Germany (cf. on the constitutional proviso with regard to identity, Judgment of the second senate, 30 June 2009 - 2 BvE 2/08 etc. -, section 240) and the Federal Republic has to devote itself to guarantee this in a European and international context. By a preventive retention of telecommunications traffic data the room for other blanket data collections, also by means of the European Union, becomes considerably smaller".

Thus, especially when read together, the ECJ judgment of 10 February 2009 and the German judgment of 2 March 2010 seem to indicate the emergence of a very important demarcation within data retention: on the one hand there is the question of the storage and retention of data, which is regulated by Directive 2006/24/EC, and on the other there is the question of the use of and access to these data, which fall under the competency of the individual Member-States. It is striking that the UK Home Office uses the same distinction to brush aside the human rights concerns that the UK implementation law of the Data Retention Directive could lead to a disproportionately large "acquisition of communications data by the police, law enforcement agencies the security and intelligence agencies".[27] According to the Home Office, the critics overlook the difference between mere retention and access: "It is important to state that access to communications data is governed by the Regulation of Investigatory Powers Act 2000 (RIPA) and no changes to the safeguards set out in that Act are planned".[28]

In the judgment of the German Federal Constitutional Court this distinction between retention and access is further elaborated upon by the importance that is assigned to the fact that the

---

[27] Home Office (2009). *Government Response to the Public Consultation on the Transposition of Directive 2006/24/EC*. Available at http://www.homeoffice.gov.uk/documents/cons-2008-transposition-dir/cons-2008-transposition-response?view=Binary.

[28] Ibid., p. 27.

retention is carried out by private companies instead of governmental organs and by the introduction of the notions of 'direct' and 'indirect use' (cf. supra, section 2.3).

3.2. Affinities and differences among judgments

As said before, the German judgment is not the first to rule on the topic of data retention[29]. Apart from the ECJ ruling on the legal basis of the directive itself, it is important to note that two other important judgments were formulated by the Romanian Constitutional Court,[30] on 8 October 2009, and by the Bulgarian Administrative Court,[31] on 11 December 2008. It is interesting to compare these two judgments, which are relatively concise, with the much more elaborated 2 March 2010 judgment of the German Federal Constitutional Court. Though certain similar elements can be discerned in the three judgments, in the Romanian case the differences are most striking, while in the Bulgarian case a focus on similarities is more enlightening.

First, we will take a closer look at the differences between the German and the Romanian decisions. The question that differentiates these judgments is whether, given that there are enough legal and technological safeguards, constitutional data retention could be possible, or whether such an idea is a categorical contradiction in terms. Is 'constitutional data retention' as unthinkable as a square circle? Both the German and the Romanian judgments subject the national implementation of Directive 2006/24 to similar tests, which concern the legality, the legitimate purpose, and proportionality of the measures. Yet, the criticisms forwarded by the German Court focus on the *use* and *access* of the data. It does not deem the data *retention* in itself, as required by the Directive, to be necessarily unconstitutional (section 205). On the other hand, the Romanian Court underlines that the *use* of data can be lawful and proportional in certain circumstances:

> "the Constitutional Court does not deny […] that there is an urgent need to ensure adequate and efficient legal tools, compatible with the continuous process of modernization and technical upgrading of the communication means, so that the crime phenomenon can be controlled and fought against. This is why the individual rights cannot be exercised *in absurdum*".

However, while there might be circumstances wherein the *use* may be justified, the Court considers the *blanket retention* of data to be disproportional by nature:

> "The Constitutional Court underlines that the justified use, under the conditions regulated by law 298/2008, is not the one that in itself harms in an unacceptable way the exercise of the right to privacy or the freedom of expression, but rather the legal obligation with a continuous character, generally applicable, of data retention. This operation equally addresses all the law subjects, regardless of whether they have committed penal crimes or not or whether they are the subject of a penal investigation or not, which is likely to overturn the presumption of innocence and to transform *a priori* all users of electronic

---

[29] The Bulgarian, Romanian and German judgments discussed in this section are not the only constitutional challenges which have been raised against the implementation of the Retention Directive. A decision regarding a constitutional complaint directed towards Hungarian Telecom Data Retention Regulations is still pending before the Hungarian Constitutional Court: http://tasz.hu/en/data-protection/constitutional-complaint-filed-hclu-against-hungarian-telecom-data-retention-regulat. In a similar case (Record No. 2006/3785P) pending before the High Court of Ireland the presiding judge decided on the 5th of May 2010 to refer the case to the ECJ. This means the ECJ will finally have to give a substantive decision on the constitutionality of Directive 2006/24/EC. We will return to this important development later in this paper.

[30] Decision no.1258, Romanian Constitutional Court, 8 October 2009. Published in the Romanian Official Monitor, no. 789, 23 November 2009. English translation (unofficial): http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf

[31] Decision no. 13627, Bulgarian Supreme Administrative Court ('Върховния административен съд'), 11 December 2008. Original text available at: http://www.econ.bg/law86421/enactments/article153902.html. Commentary in English: http://www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention

> communication services or public communication networks into people susceptible of committing terrorism crimes or other serious crimes".

Contrary to the German Court, the Romanian Court considers the use of the data to be a less radical threat than the blanket storage as such, as only the latter creates a situation where the infringement on "the right to private life and freedom of expression, as well as processing personal data" is no longer the exception but the rule:

> "The legal obligation that foresees the continuous retention of personal data transforms though the exception from the principle of effective protection of privacy right and freedom of expression, into an absolute rule. The right appears as being regulated in a negative manner, its positive role losing its prevailing role".

Because the focus of the German Constitutional Court is on access and use, its criticisms are mainly aimed at the national implementation law. Moreover its criticisms are a matter of proportionality. Given the right safeguards not only retention, but also use and access can be constitutional. The Romanian focus, on the other hand, is on data retention as such and therefore the judgment is not only a frontal attack on national law 298/2008, but also on the Directive itself. Clearly, the Court considers ubiquitous and continuous retention for a period of six months to be intrinsically in opposition with Art 8 ECHR (right to respect for private and family life). Thus, the Romanian Court takes a particularly strong stance, and states that:

> "the obligation to retain the data, established by Law 298/2008, as an exception or a derogation from the principle of personal data protection and their confidentiality, empties, through its nature, length and application domain, the content of this principle".

In Bulgaria the Supreme Administrative Court (judgment of 11 December 2008) annulled Art. 5 of *Regulation # 40 on the categories of data and the procedure under which they would be retained and disclosed by companies providing publicly available electronic communication networks and/or services for the needs of national security and crime investigation*, which partially transposed Directive 2006/EC, for being unconstitutional. Article 5 stated that "the data would be retained by the providers and a directorate within the Ministry of Interior (MoI) would have a direct access via a computer terminal"[32] and specified not only that the MoI would have "passive access through a computer terminal" but also that "security services and other law enforcement bodies" would have access "to all retained data by Internet and mobile communication providers"[33] without needing court permission. The constitutional aversion to centralised storage and direct access without any court control is very similar to the reasoning found in the German judgment. In 2009, the Bulgarian government tried to reintroduce a law that would give direct access to the Ministry of Internal Affairs to all data held by the providers, but the law was rejected by Bulgaria's Parliament. On 17 February, Parliament "approved the second reading of amendments to the Electronic Communications Act, but only after serious concessions".[34] One of the concessions made by the Ministry of Interior was that it had to renounce to its

> "demand to have permanent, direct access to personal communication data. From now on, mobile phone and internet operators will have to supply requested communication data within 72 hours and not, as Interior Minister Tsvetan Tsvetanov wanted, in two hours. The Interior Minister, or his representative, would have the right to set a different

---

[32] Access to Information Programme (AIP) Foundation, available at http://www.aip-bg.org/documents/data_retention_231209eng.htm

[33] Digital Civil Rights in Europe, available at http://www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention

[34] The Sofia Echo, available at http://sofiaecho.com/2010/02/17/860017_bulgarias-parliament-approves-eavesdropping-act

deadline, shorter or longer, in exceptional cases and depending on the severity of the case."[35]

4. The politics "around" the judgment of 2 March 2010

4.1. The reactions to the German judgment

It is noteworthy that the German judgment attracted much more attention than either the Bulgarian or Romanian one. This is probably due to a set of different reasons, among which are: the strong civil society participation behind the plaintiffs, namely 34,000 persons which were mostly mobilised by the *Arbeitskreis Vorratsdatenspeicherung*[36] (Working Group on Data Retention); and the timing of the very extensive and substantial judgment, just in the midst of EU debates on transatlantic data-sharing agreements.

In Germany, the reactions to the judgment came from three types of actors in particular: the privacy group that promoted and supported the complaint; the Federal Criminal Police and the government. It is particularly interesting that in the aftermath of the publication of the Court's decision, several international media focused on the contrast between the respective positions of the Justice Minister and the Interior Minister.[37] On the one side, the Justice Minister, an FDP party member of the opposition at the moment of the adoption of the German legislation and amongst the plaintiffs as a private citizen, publicly welcomed the judgment. On the other side, the Interior Minister, member of the CDU, expressed a thinly veiled criticism, and underlined the need for a quick redrafting of the law to fill the "legislative gap" created by the Court's judgment. A similar posture has been taken by the Federal Criminal Police[38] which not only urged German politicians to come up with new legislation as soon as possible, but also sent out an open letter to Chancellor Angela Merkel wherein it reproaches the German Constitutional Court their naïve outlook.[39]

The reaction of the AK Vorrat deserves particular attention. First, they criticised the reasoning of the Court, and one of their members stated in a press release that:

> "[the Court's] decision proclaiming the recording of the entire population's behaviour in the absence of any suspicion compatible with our fundamental rights is unacceptable and opens the gates to a surveillance state".[40]

Then, in the same press release, they already announced a double move: the continuation of the "legal fight" against data retention in Germany to avoid the re-enacting of the implementation law;[41] as well as a sort of "Europeanization" of their fight at the EU level, planning an EU-wide campaign based on the preparation of a European Citizens' Initiative concerning data

---

[35] The Sofia Echo, ibid.

[36] Stoppt die Vorratsdatensspeicherung! [Stop data retention!], available at http://www.vorratsdatenspeicherung.de/content/view/355/55/lang,en/

[37] See, among others: Q. Peel & S. Pignal (2010), 'Germany's top court overturns EU data law', *Financial Times*, 2 March, available at http://www.ft.com/cms/s/0/563e0fc8-25f6-11df-b2fc-00144feabdc0.html; and H. Mahony (2010), "German court strikes blow against EU data-retention regime", *euobserver.com*, 3 March, available at http://euobserver.com/9/29595.

[38] Online Focus (2010, 02.03.2010). BKA will schnell ein neues Gesetz. *Online Focus*, from http://www.focus.de/politik/deutschland/vorratsdatenspeicherung-bka-will-schnell-ein-neues-gesetz_aid_486040.html

[39] Original text of the letter available at http://www.bdk.de/kommentar/artikel/vakuum-bei-der-kriminalitaetsbekaempfung-im-internet-ist-ein-hochrisiko-fuer-die-sicherheit-der-buerger-sondersitzung-der-imk-und-jumiko-zur-schadensbegrenzung-unverzichtbar/5920af02d045433601f31c9d0dde1180/?tx_ttnews[year]=2010&tx_ttnews[month]=03

[40] Arbeitskreis Vorratsdatenspeicherung (2010), After data retention ruling: Civil liberties activists call for political end to data retention. Available at http://www.vorratsdatenspeicherung.de/content/view/355/79/lang,en/

[41] Arbeitskreises Vorratsdatenspeicherung (2010). Kampagne: Stoppt die Vorratsdatenspeicherung 2.0! Retrieved 16.04.2010, http://www.vorratsdatenspeicherung.de/static/portal_de.html

retention.[42] This double move reflects their focus on the linkage between the national and the European (and even international) level. Indeed, they also invited the German government to refrain from agreeing to a new international agreement on data exchange, and they advised the Justice Minister to liaise at EU and international level with the EU Commissioner of Justice, Fundamental Rights and Citizenship and with the other Member-States that have not yet passed data retention implementation laws, in order to repeal data retention.

Finally, it is noteworthy that the telecom and internet providers, while playing such a crucial role in data retention, have not been a subject of much attention in the reactions of the first commentators. However, according to some news sources, both Deutsche Telekom and Vodafone immediately complied with the German Constitutional Court's order to delete all already stored data.[43]

4.2. From the EU perspective

As stated above, the interest and impact of the German judgment at European level are also due to the timing of the decision. Indeed, the judgment arrived in the midst of European and international debates on the next moves in data-sharing and protection, and, in particular, just weeks after the rejection of the so-called 'SWIFT agreement by the European Parliament'.[44] The judgment brought back emphasis on the issue of the implementation of the data retention directive. In fact, several Member-States have still not implemented the directive or are still in the course of passing the relative implementation law.[45] The slowness of the process is partly due to several and different layers of resistance (national political and juridical debates) and partly due to other less direct reasons (e.g. election schedules). Two months after the decision of the German Court, the High Court of Ireland has finally done what everybody has been hoping for: in its decision of the 5th of May 2010 (Record No. 2006/3785P) it refers the case to the ECJ. This is an important breakthrough because it means getting to the core of the matter, which is the constitutionality of Directive 2006/24/EC itself, rather the constitutionality of the national implementation legislation.

At present, the most official reaction from the Commission has been the decision to schedule a "Proposal for a review of [the Data Retention] Directive" in the Commission Work Programme 2010.[46] Indeed, the official motivation of this decision states that:

> "[f]ollowing an evaluation of the existing Data Retention Directive and recent judgments of MS constitutional courts, a review of the Directive is aimed at better matching data retention obligations with law enforcement needs, protection of personal data (right to privacy) and impacts on the functioning of the internal market (distortions)".[47]

---

[42] AK Vorratsdatenspeicherung is lobbying to get directive 2006/24/EC rejected or at least amended, so that Member-States can opt out of data retention: http://www.vorratsdatenspeicherung.de/content/view/362/79/lang,en/ and http://www.vorratsdatenspeicherung.de/images/antworten_kommission_vds_2009-11-13.pdf

In a phone interview held on 30 April 2010, Patrick Breyer of the AK Vorrat told the authors that AK Vorrat was waiting for the adoption of the relevant European Citizens' Initiative legislation to launch their citizens' initiative campaign. The European Commission has already presented a first proposal: European Commission (2010), *Proposal for a regulation of the European Parliament and of the Council on the citizens' initiative*.

[43] Die Presse.com (2010, 04.03.2010). Deutsche Telekom vernichtet 19 Terabyte an Vorratsdaten. *Die Presse.com*, from http://diepresse.com/home/techscience/internet/544115/index.do?from=gl.home_tech

[44] Among the main reasons behind the massive rejection of the new "Swift Interim Agreement" were the European Parliament's requests for increased data protection guarantees and further inter-institutional cooperation to ensure proper parliamentary control. See European Parliament website: http://www.europarl.europa.eu/news/expert/background_page/019-68530-032-02-06-902-20100205BKG68527-01-02-2010-2010-false/default_en.htm

[45] In particular, Belgium and Luxembourg have not yet passed the implementation laws.

[46] European Commission (2010), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Commission Work Programme 2010 – Time to act*.

[47] Idem, p. 18 (annex).

In fact, the said evaluation was already planned in the very text of the Data Retention Directive itself.[48] According to the directive, such evaluation is supposed to be released to the public not later than 15 September 2010.[49] It has been already planned in the Action Plan Implementing the Stockholm Programme, which also mentions the possibility, if 'necessary', of following the evaluation with a "proposal for revision".[50]

Apart from the issues concerning the future of the Data Retention Directive itself, the German judgment will probably prove to be very important in the numerous debates surrounding data protection and processing. The analysis of the German Constitutional Court judgment takes a position on important issues such as the definition of personal data; the recourse to commercial data for security purposes (and thus the relations with private entities, and the legal framework to adopt); the adoption of technological instruments to limit data use and abuse; the effects of diffuse surveillance on personal and social behaviour, even when surveillance takes the form, or relies, on the 'mere' retention of data.

5. Provisional conclusions

Even if it is still completely uncertain what the future will bring, and what will be the effective contribution of the German judgment to the evolution and solution of the current tensions and issues, it is already possible to advance some final considerations. In particular, it seems important to advance a more critical approach to the increasing emphasis on proportionality.

(i) The 'proportionality check' approach of the German Constitutional Court confirms the relevance of this bundle of criteria in assessing the acceptability of privacy and data protection derogations for the benefit of security measures. It not only enriches the case-law on privacy and data protection, but also pays specific attention to the technological features of the measures and the need for adequate technological solutions (data security, control against misuse, encryption).

(ii) However, even an enhanced 'proportionality test' of this kind does not substitute political and social choices concerning data retention, or data processing for security purposes at large. The reaction of the AK Vorrat, as well as the tensions within the German government, seem to confirm the increasing request for having 'politics' back into these debates, and not merely "around" them. The posture taken by the European Parliament in the discussions concerning transatlantic data sharing and processing could be partially read in this sense.

(iii) Moreover, there is no unanimous vision of what "the" proportionality test is, since the methods and criteria do not only vary from jurisdiction to jurisdiction, but also from case to case. The German Federal Constitutional Court, the European Court of Human Rights and the European Court of Justice, to name just these three, have a distinct understanding of what a proportionality test should comprise, and they all seem to apply the test in a strict and in a more lenient way, depending on the case. In his study on the use of the proportionality principle by the European Court on Human Rights, Sébastien van Drooghenbroeck deplores the lack of reflexivity from the side of the judges. There are no leading cases and very little can be distilled about the scope and impact of the

---

[48] Art. 14(1) Data Retention Directive.

[49] A draft version of this document has recently been leaked (https://docs.google.com/fileview?id=0B2Rh7x7YpF3KNTZlNTU0NDAtZjgwMS00YzJkLWFiODktMDQwNTUxMjE3MTcz&hl=en). See also: Karlin Lillington "Leaked report reveals big surge in call data requests", *Irish Times*, 14 May 2010, online available at: http://www.irishtimes.com/newspaper/finance/2010/0514/1224270357547.html

[50] European Commission (2010), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Delivering an area of freedom, security and justice for Europe's citizens, Action Plan Implementing the Stockholm Programme*, p. 30.

requirement.[51] Nothing in European case law comes close to the three-tiered approach to scrutiny developed by the U.S. Supreme Court over recent decades under the Equal Protection Clause (rational basis review, middle-tier scrutiny and strict scrutiny).[52] It is clear that the European Court of Human Rights reaches a similar result through acknowledging to state authorities a 'margin of appreciation'. This margin and the standard of scrutiny will vary according to the context of the case.[53] However, there is no guidance in case law about this margin. Looking back at the Court's case law on security issues, one *can* observe that the Court is prepared to accept the legitimacy of the fight against crime and terrorism as well as to acknowledge the need to take effective measures. Without going as far as to say that the Court gives full discretion to Member States it is clear that almost always less strict scrutiny of the proportionality requirement is applied, especially when the bulk of the litigation is (only) on privacy, and not on other human rights enshrined in the Convention. This careful approach of sensitive issues by the European judges explains, so we believe, a tendency to concentrate on the first requirement (legality) of the privacy check.[54] This explains why the European Court studies the presence of safeguards to avoid abuse of data as elements of the legality requirement, rather than elements of the proportionality requirement, as the German Court in its judgment of 2 March 2010. There might be good reasons for both approaches. Like the German Court, Sébastien van Drooghenbroeck, seems to consider that safeguards against abuse are part of the proportionality requirement, but they are, and this deserves some emphasis, to be considered as the more formal aspects of this requirement. The other half of the requirement of proportionality, the substantive part, consists of balancing the interests at stake.[55] A fixation on the formal requirements of proportionality by the judges, might allow them to avoid the more sensitive, but necessary, substantive proportionality test. A bit of this is lurking in the German judgment and raises the question whether this judgement is really to be understood as a break-through in the European case law.

(iv) The foregoing shows that the existence as such of a proportionality test is not automatically a warrant for a strong protection of human rights and liberties. It all depends on the strictness of the test applied by the judges.[56] Will the judges address the substantive issues of the requirement or will they only concentrate on the formal issues? Even when they do address substantive questions regarding proportionality, it remains to be seen how this is done. A weak proportionality test, consisting of a mere balancing of a fundamental right and another interest – for example: privacy and crime control – does in fact not offer any guarantee for the preservation of that fundamental right, since the

---

[51] S. van Drooghenbroeck, *La proportionalité dans de le droit de la convention européenne des droits de l'homme*, Brussels, Bruylant, 2001, 777p.

[52] K. Henrard, *Mensenrechten vanuit international en nationaal* perspectief, The Hague, Boom, 2007, p. 258. See also Beth A. Deverman, 'Fourteenth Amendment - Equal Protection: The Supreme Court's Prohibition of Gender-Based Peremptory Challenges', *Journal of Criminal Law and Criminology*, Vol. 85, 1995

[53] On the nature of the Court's review see, e.g., ECtHR, Handyside, *Series A-24*, §§ 49-50 and ECtHR, Olsson, *Series* A-130, §§ 67-69 Relevant factors include the nature of the Convention right in issue, its importance for the individual and the nature of the activities concerned. If the Court finds that one or more of these factors are present, e.g. the right at stake is crucial to individual's effective enjoyment of intimate or key rights, then the state has a narrow margin of action. If they are not the state's action will be assessed against a wider margin of appreciation. See E. Guild, 'Global Data Transfers: The Human Rights Implications', *Inex policy brief* no. 9, May 2009, 10p., (http://www.ceps.eu/ceps/download/3400)

[54] P. De Hert, 'Balancing security and liberty within the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11', *Utrecht Law Review*, 2005, Vol. 1, No. 1, 68-96 (http://www.utrechtlawreview.org/publish/articles/000005/article.pdf).

[55] S. van Drooghenbroeck, *La proportionalité dans de le droit de la convention européenne des droits de l'homme*, Brussels, Bruylant, 2001, p. 728.

[56] See on this more in detail: P. De Hert, 'Balancing security and liberty within the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11', *Utrecht Law Review*, 2005, Vol. 1, No. 1, 68-96 (http://www.utrechtlawreview.org/publish/articles/000005/article.pdf). See on the strict proportionality test in the *Marper* judgment: E. Guild, 'Global Data Transfers: The Human Rights Implications', *Inex policy brief* no. 9, May 2009, 10p., (http://www.ceps.eu/ceps/download/3400)

approach itself assumes that preserving the one per definition implies weakening the other, and vice versa. It excludes the possibility that both interests can be fostered and protected together. Such a proportionality test is doomed to weigh one interest *against* the other, and makes impossible the search of a *composition* in which the different interests at stake are all preserved in an optimal way. Such criticisms however do not apply to stronger proportionality tests that include the possibility to decide that some measures are inacceptable from a constitutional point of view – an exercise known to the Strasbourg court as the "necessary in a democratic state" test – since they encompass the possibility to refuse a measure because it harms the essence of a fundamental right or of the constitutional order, even if it can be shown that this measure can effectively realise another legitimate interest. The issue at stake then is not a "balancing" between two values, but an answer to the questions "How much erosion of a fundamental right is compatible with the democratic constitutional state in which fundamental rights are a constitutive element" or "In which society do we want to live?". Another aspect of a stronger proportionality test is indeed the obligation to explore if there are alternative measures that allow for the realisation of the legitimate interest in a way that does not affect the fundamental rights in the same way as the proposed measure. That is, in other words, answering the question: "Is there a way to protect and enforce both values without loss at the fundamental rights' side ?"

(v) Also noteworthy is the growing interest of national civil liberties groups to articulate their campaign at European level, and take advantage of the capacity to operate on different layers. This seemed to be mainly a prerogative of other actors, and in the field of security measures, of Interior Ministries and, to a certain degree, data protection authorities.[57]

(vi) In the context of a debate already underway on the possible revision of the Data Protection Directive, the German Constitutional Court judgment's concern for traffic and location data is particularly precious. In particular, the decision to assess the level of data protection on the base of data processing technology has to be welcomed. This should offer some guidance when discussing the possible, and most adequate, regulations for 'data mining' and other 'risk assessment' tools.

(vii) The German Constitutional Court judgment highlights the idea that even 'mere' data retention is not a trivial measure, but a measure that has concrete consequences on societies and thus must undergo a severe check. This echoes the Strasbourg Court decision on the so-called Marper case, that criticized the 'mere', but not time-limited, retention of personal data of acquitted or discharged people.[58] This posture is particularly important in the face of a continuous shift in the nature of security and surveillance measures, heading towards systems based on the 'proactive' or random accumulation of commercial and non-commercial data of a great number of people.[59]

---

[57] Such ability of some Interior Ministries to operate along several layers to shape in a specific way security measures based on data exchange, and foster their adoption at European and international levels, was particularly evident in the case of the Prüm measure, dealing with exchange of DNA, fingerprints and vehicle registration data. For an analysis of the re-shaping of power relations, cf. Bellanova, R. (2008), 'The 'Prüm Process': The Way Forward for Police Cooperation and Data Exchange?', in E. Guild & F. Geyer (Eds.), *Security vs. Justice? - Police and Judicial Cooperation in the European Union* (pp. 203-221). Aldershot: Ashgate.

[58] European Court of Human Rights, *Case of S. and Marper versus the United Kingdom*, Application nos. 30562/04 and 30566/04, Strasbourg, 4 December 2008.

[59] Bellanova, R., & De Hert, P. (2009), 'Le cas S. et Marper et les données personnelles: l'horloge de la stigmatisation stoppée par un arrêt européen'. *Cultures & Conflits*, 76, 101-114 ; De Beer D., De Hert P., Gonzalez Fuster G. & Gutwirth S. (2010), 'Nouveaux éclairages de la notion de la notion de « donnée personnelle » et application audacieuse du critère de proportionnalité. Cour européenne des droits de l'homme Grande Chambre *S et Marper c. Royaume Uni*, 4 décembre 2008', *Revue Trimestrielle des Droits de l'Homme*, 81, 141-161 and Gonzalez Fuster G., P. De Hert, E. Ellyne & S. Gutwirth (2010) *Huber, Marper and Others: Throwing new light on the shadows of suspicion*, INEX Policy Brief No. 11, 2010 Centre for European Policy Studies (CEPS), 9 p. via http://www.ceps.eu/book/huber-marper-and-others-throwing-new-light-shadows-suspicion

(viii) Finally, the German Constitutional Court judgment takes an interesting stance on the role of private companies, praising their participation to data retention as an important guarantee against possible excess of state surveillance. However, the role and the responsibilities of private actors in the setting of security measures based on data processing is still far from being clear, or from achieving political consensus. The principle that crime fighting and guaranteeing public security by means of legitimate restrictions of fundamental rights and liberties is the exclusive prerogative of the democratic constitutional state certainly deserves to be reanimated during this debate. Given the aforementioned modifications to the nature of security systems, the issue of the "privatisation" of security and crime-fighting deserves crucial attention.