RANKED AMONG THE WORLD'S TOP 10 THINK TANKS
CEPS Liberty and Security in Europe
CENTRE FOR EUROPEAN POLICY STUDIES

Proportionality overrides Unlimited Surveillance

The German Constitutional Court Judgment on Data Retention

Katja de Vries, Rocco Bellanova & Paul De Hert

May 2010

ISBN 978-94-6138-010-4
Available for free downloading from the CEPS website (http://www.ceps.eu)

CONTENTS

PROPORTIONALITY OVERRIDES UNLIMITED SURVEILLANCE

THE GERMAN CONSTITUTIONAL COURT JUDGMENT ON DATA RETENTION

CEPS 'LIBERTY AND SECURITY IN EUROPE'/MAY 2010

KATJA DE VRIES, ROCCO BELLANOVA & PAUL DE HERT*

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.[1] Since then, this seemingly straightforward directive has 'generated' quite an impressive number of court judgments. They range from the European Court of Justice[2] (ECJ) to the administrative (e.g. Germany[3] and Bulgaria) and constitutional courts (e.g. Romania) of some member states.

In particular, the judgment of the German Constitutional Court,[4] delivered on 2 March 2010, has already caught the attention of several commentators, from civil society, lawyers, journalists and politicians. In the judgment, the court says 'no' to the German implementation laws of the Data Retention Directive.

In this paper we wish to highlight some of the key features of the ruling and its main similarities and divergences with similar judgments. Then, given the relevance of the issues at stake, we contextualize the judgment in the wider framework of EU data processing and protection debates, outlining some elements of reflection for further discussion.

---

* Katja de Vries is a PhD researcher in the interdisciplinary group on Law, Science, Technology and Society (LSTS) at the Vrije University Brussel (VUB); Rocco Bellanova is a researcher at the LSTS-VUB, and researcher and assistant at the Centre de Recherche en Science Politique (CReSPo) of the Facultés universitaires Saint-Louis, Paul De Hert is Professor at the faculty of law at VUB, member of the LSTS-VUB and Associated Professor at the University of Tilburg. The authors would like to thank the Tilburg Institute for Law, Technology, and Society (TILT), who hosted a shorter version of this article on their TILT Weblog Law & Technology: http://vortex.uvt.nl/TILTblog/?p=118. The authors would also like to thank Sergio Carrera and an external anonymous reviewer for their comments.

[1] 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

[2] 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

[3] 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/

[4] *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 FCC judgment.

Background

In its judgment, the German Federal Constitutional Court (FCC) abrogated the German national implementation of the data retention directive (Art.113a and 113b of the TKG,[5] i.e., the Telecommunications Law, and Art. 100g, paragraph 1 sub 1, of the StPO,[6] i.e., the Criminal Procedural Code, in combination with the aforementioned Art 113a TKG). This legislation on data retention, implementing the similar EU Directive, was passed by the Bundestag on 9 November 2007 and entered into force on 1 January 2008. The law allows 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 all contact via e-mail. The law forbids authorities from retaining the contents of either form of communication.

Since its adoption, the German national implementation law has met with considerable resistance. On 31 December 2008, 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 at the Federal Constitutional Court. The complaint was backed by more than 30,000 people, and requested, *inter alia*, the immediate suspension of the law.[7] The judgment of 2 March 2010 is the outcome of this complaint.

The main findings: A proportionality check

The case could have been a tricky one for EU law, but the German Court upheld the EU directive, saying the problem lay instead with how the German Parliament chose to interpret it. The German legislation was not upheld but found to breach the German Constitution (*Grundgesetz*[8]) and the rights of privacy, ensuring the "security and integrity" of communications by post and telephone. Privacy is not mentioned in the German Constitution, but the Court has developed a broad right to privacy and "informational self-determination" as tenets of the right to human dignity in Article 1 of the Constitution in its famous 1983 "Census Decision" (*Volkszählungsurteil*).[9] 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 mainly by writing letters, but through the activity of the Court the protection goes well beyond the paper medium. All telecommunication and communication is protected. In the judgment of 2 March 2010, the court states 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."

Hence, the Constitution applies.

Now, how did the court come to the conclusion that the implementation law, doing no more than implementing EU legislation, breaches Article 10 of the Constitution?

---

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

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

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

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

[9] BVerfG [Judgments of the Federal Constitutional Court] 15 December 1983, (*Volkszählung*), *BVerfGE* 65, 1.

As also remarked by other authors,[10] the court based its analysis on a privacy test similar to the one developed by the European Court of Human Rights. It not only checks the quality of the legal basis, but also looks at the legitimate aim and proportionality of the proposed initiative. Germans are good at making laws, so the first requirement was not the problem. With regard to the second (legitimacy), the court found that a six-month retention period can be legitimate, in principle, but only if recognised as an exception ("dass diese eine Ausnahme bleibt"). Such a measure:

> "largely increases the risk of citizens to be the subject of further investigation, 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] "can establish a feeling of permanent control" [and] "diffuse threat" ("diffuse Bedrohlichkeit").

The major problem with the German implementation law was that it did not satisfy the third requirement of proportionality. While the idea underlying data retention is not "absolutely incompatible with Art.10 of the German Constitution (protecting the privacy of telecommunications)" (§ 205 judgment), its application in national law did not meet this constitutional need for proportionality that the Court subdivided into four criteria: purpose limitation, data security, transparency and control against misuse. All these criteria were left unmet. The court found that the law failed to set the bar high enough to allow investigators access to the data and failed to ensure sufficient data encryption should the information be stolen. "The disputed instructions neither provided a sufficient level of data security, nor sufficiently limited the possible uses of the data", the court said.

After suspending the law several times during interim proceedings, the court annulled it in its final judgment. All data already collected by carriers and providers had to be deleted.

Fundamental rights and data retention

The questions to consider here are: when is it the jurisdiction of the Federal Constitutional Court (FCC) and when of the ECJ? And what is the difference between mere retention and actual access to the data?

The German FCC has on several occasions shown a reluctance to accept an unconditional and full supremacy of EC law. In the Solange II case (*Wünsche Handelsgesellschaft* [1987] 3 CMLR 225) 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 FCC would "no longer exercise its jurisdiction to decide on the applicability of secondary Community legislation". Recently, in the complex and controversial Lisbon Judgment, the FCC took an even more outspoken stance and showed its constitutional teeth towards EC law.[11] 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). Even though it is difficult to say whether the judgement should be characterised as a triumph of

---

[10] Among others, 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/.

[11] BVerfG 30 June 2009, 2 BvE 2/08 (*Lisbon*). 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.

nationalist euroscepticism or of constitutionalism, in any case it has become clear once more that the relationship between EC law and the German Constitutional Court 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 how the FCC avoids the need to refer to the ECJ with a preliminary question. In the beginning of the Data Retention Judgment (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: 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 negate the necessity of a preliminary question to the ECJ is rather 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. 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, wherein the court refers back to the notion of "constitutional identity" in 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, FCC, 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 FCC Judgment of 2 March 2010 seem to indicate the emergence of a new 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 hand there is the question of the use and access to these data, which falls 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 data retention could lead to a disproportionately large "acquisition of communications data by the police, law enforcement agencies and the security and intelligence agencies".[12] According to the Home Office, the critics overlook the difference between mere

[12] 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.

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".[13]

In the judgement of the FCC this distinction between mere retention and access is further elaborated upon by the importance that is assigned to the fact that the retention is carried out by private companies instead of governmental bodies and by the introduction of the notions of 'direct' and 'indirect use'.

The FCC's access and use of the data; the role of private companies and direct and indirect use

According to the FCC, the difference between retention and access is also 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 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 FCC as very positive. The fact that the obligation to retain data rests with private service-providers becomes even a "decisive element" for the assessment of the non-unconstitutionality of the principle behind 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" (§ 214 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" (§ 218 judgment), the Court seems to identify in the two-step procedure, general but dispersed retention by private actors, and justified direct or indirect use by public actors, a sort of fundamental guarantee. However, following up on the judgment of the FCC, the German Federal Commissioner for Data Protection, Peter Schaar, said in an interview with the *Focus* magazine that also the data retention practised by private companies such as Google and Facebook should 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".[14] This raises the question of how large private actors can be without endangering the dispersed character of the retention.

Another important elaboration by the FCC with regards to use 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". Indeed, "the production of such requests for information is independent of an exhaustive catalogue of legal interests or criminal offences, and can be

---

[13] Ibid., p. 27.

[14] 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

allowed more widely than the request and the use of telecommunication traffic data themselves." (§ 254 judgment).

Transparency to prevent the feeling of diffuse threat

As widely discussed by journalists, the FCC 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" in 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" (§ 241 judgment).

This is why such a "diffuse threat" should be "counteract[ed] (…) by effective rules of transparency" (§ 242 judgment). 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.

Are location and traffic data personal data? Parallels between the position of the FCC and the debate about "personal data" in Data Protection Directive 95/46/EC

Notwithstanding the attempt of the FCC to keep national and EC matters separate from each other, the judgment also provides some reflections to 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 FCC 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 the court did not want to get its fingers burned, it would have been interesting if the court had more explicitly taken the debates at European level into consideration. 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[15] the Working Party stated that dynamic IP addresses should be treated as personal data, unless the ISP can establish with "absolute

[15] 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

certainty that the data correspond to users that cannot be identified": but in practice this is almost impossible to ascertain.

Affinities and differences among judgments

As said before, the German judgment is not the first intervention on the topic of data retention. 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,[16] on 8 October 2009, and by the Bulgarian Administrative Court,[17] on 11 December 2008. It is interesting to compare these two judgments, which are relatively concise, with the much more differentiated German case. Though certain similar elements can be discerned in all of these 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 cases. 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 it is an absolute 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 of 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). The Romanian court also underlines that the use of data should be proportional and lawful. However, while the court holds that the use of data may be justified 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*").

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

---

[16] 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

[17] 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

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 could 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 the Bulgarian case the administrative court annulled Art. 5 of the law (*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, as 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"[18] 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"[19] 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".[20] One of the concessions made by the Ministry of Interior was that it had to renounce 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 deadline, shorter or longer, in exceptional cases and depending on the severity of the case."[21]

The reactions to the German judgment

It is noteworthy that the German judgment has 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, 34,000 persons, mostly mobilised by

---

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

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

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

[21] The Sofia Echo, ibid.

the *Arbeitskreis Vorratsdatenspeicherung*[22] (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, reactions to the judgment came from three types of actor in particular: the privacy group that promoted and supported the complaint; the Federal Criminal Police and the government. It is particularly interesting to note that in the aftermath of the publication of the Court's decision, several international media focused on the contrast between the Justice Minister and the Interior Minister.[23] On the one side, the Justice Minister, an FDP party member of the opposition at the moment of the adoption of the DE 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,[24] 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 in which they reproach the German Constitutional Court for their naïve outlook.[25]

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".[26]

Then, in the same press release, they announced a double move: the continuation of the "legal fight" against data retention in Germany to avoid the re-enacting of the implementation law;[27] as well as a sort of "Europeanisation" of their fight at the EU level, planning an EU-wide campaign based on the preparation of a European Citizens' Initiative concerning data retention.[28] This double move reflects their focus on the linkage between the national and the

---

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

[23] 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.

[24] 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

[25] 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

[26] 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/

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

[28] 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

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 an important actor of data retention, namely telecom and internet providers, have not attracted the main interest of the first commentators. According to some news sources, both Deutsche Telekom and Vodafone had already started to comply with the FCC order to delete already stored data.[29]

For an EU perspective: guidelines for the future?

As stated above, the interest raised by the FCC Judgment at European level is 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'.[30] 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.[31] 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).

At present, the most official reaction from the Commission has been the decision to insert the tabling of a "Proposal for a review of [the Data Retention] Directive" in the Commission Work Programme 2010.[32] 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)".[33]

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*.

[29] Die Presse.com (2010, 04.03.2010), "Deutsche Telekom vernichtet 19 Terabyte an Vorratsdaten" [German Telekom destroyed 19 terabytes of data storage]. *Die Presse.com*, from http://diepresse.com/home/techscience/internet/544115/index.do?from=gl.home_tech

[30] 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

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

[32] 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*.

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

In fact, the said evaluation was already planned in the very text of the Data Retention Directive itself.[34] According to the Directive, it is supposed to be released no later than 15 September 2010 and should be made public. 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".[35]

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 points highlighted in the analysis of the FCC judgment, mirror, and take 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.

Even if it is still completely uncertain what the future will bring, and what will be the effective contribution of the FCC judgment to the evolution and solution of these tensions, we can already highlight some considerations and invite all interested actors to consider them.

(i) The 'proportionality check' approach of the FCC confirms the relevance of this criterion in assessing the acceptability of privacy and data protection derogations 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 check' could 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, seems to confirm a growing demand to put 'politics' back into these debates. The posture taken by the European Parliament in the discussions concerning transatlantic data sharing and processing could be partially read in this sense.

(iii) 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.

(iv) In the context of a debate already underway on the possible revision of the Data Protection Directive, the FCC 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.

(v) The FCC 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 decried the 'mere', but not time-limited, retention of personal data of

---

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

[35] 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.

acquitted or discharged people.[36] 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 'preventive' accumulation of commercial and non-commercial data of a great number of people.[37]

(vi) Finally, the FCC Judgment takes an interesting stance on the role of private companies, praising their participation in 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. Nevertheless, given the aforementioned modifications to the nature of security systems, this issue nonetheless deserves careful attention.

[36] 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.

[37] 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 », in *Cultures & Conflits*, No.76, pp.101-114, l'Harmattan, Paris.

About CEPS

Founded in Brussels in 1983, the Centre for European Policy Studies (CEPS) is among the most experienced and authoritative think tanks operating in the European Union today. CEPS serves as a leading forum for debate on EU affairs, but its most distinguishing feature lies in its strong in-house research capacity, complemented by an extensive network of partner institutes throughout the world.

Goals

- To carry out state-of-the-art policy research leading to solutions to the challenges facing Europe today.
- To achieve high standards of academic excellence and maintain unqualified independence.
- To provide a forum for discussion among all stakeholders in the European policy process.
- To build collaborative networks of researchers, policy-makers and business representatives across the whole of Europe.
- To disseminate our findings and views through a regular flow of publications and public events.

Assets

- Complete independence to set its own research priorities and freedom from any outside influence.
- Formation of nine different research networks, comprising research institutes from throughout Europe and beyond, to complement and consolidate CEPS research expertise and to greatly extend its outreach.
- An extensive membership base of some 120 Corporate Members and 130 Institutional Members, which provide expertise and practical experience and act as a sounding board for the utility and feasability of CEPS policy proposals.

Programme Structure

CEPS carries out its research via its own in-house research programmes and through collaborative research networks involving the active participation of other highly reputable institutes and specialists.

Research Programmes

Economic & Social Welfare Policies
Energy, Climate Change & Sustainable Development
EU Neighbourhood, Foreign & Security Policy
Financial Markets & Taxation
Justice & Home Affairs
Politics & European Institutions
Regulatory Affairs
Trade, Development & Agricultural Policy

Research Networks/Joint Initiatives

Changing Landscape of Security & Liberty (CHALLENGE)
European Capital Markets Institute (ECMI)
European Climate Platform (ECP)
European Credit Research Institute (ECRI)
European Network of Agricultural & Rural Policy Research Institutes (ENARPRI)
European Network for Better Regulation (ENBR)
European Network of Economic Policy Research Institutes (ENEPRI)
European Policy Institutes Network (EPIN)
European Security Forum (ESF)

CEPS also organises a variety of activities and special events, involving its members and other stakeholders in the European policy debate, national and EU-level policy-makers, academics, corporate executives, NGOs and the media. CEPS' funding is obtained from a variety of sources, including membership fees, project research, foundation grants, conferences fees, publication sales and an annual grant from the European Commission.

E-mail: info@ceps.be
Website: http://www.ceps.be
Bookshop: http://shop.ceps.be

CENTRE FOR EUROPEAN POLICY STUDIES

Place du Congrès 1 • B-1000 Brussels
Tel: 32(0)2.229.39.11 • Fax: 32(0)2.219.41.51