Computer Law & Security Review Volume 25, Issue 2, 2009, Pages 115-122,
http://dx.doi.org/10.1016/j.clsr.2009.02.008

[Page 115]

Data Protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention

Gerrit Hornung, Christoph Schnabel[1]

University of Kassel, Germany

ABSTRACT

This year, the population census decision of the German Federal Constitutional Court (Bundesverfassungsgericht) will celebrate its 25th anniversary. The celebration is a good reason to take a look back at this groundbreaking decision, which has lost none of its topicality and validity. It is also an occasion to examine the wave of new Bundesverfassungsgericht decisions, stemming from the beginning of 2008, on governmental surveillance and data protection, in particular the "online-searching" decision, the decision on license plate scanning, and the interim injunction to partly stop the enactment of the European data retention directive in Germany. This article is an attempt at helping overcome the language barrier that has prevented much of the world from understanding the depth and value of German legal theory on data protection (This article is thus following an appeal made by J. A. Cannataci, "Lex Personalitatis & Technology-driven Law", *scripted*, Volume 5, Issue 1, April 2008, p. 3, via http://www.law.ed.ac.uk/ahrc/script-ed/vol5-1/editorial.asp). In Part I of this paper, published in [2009] CLSR 84-88 we examined the population census decision and the German concept of informational self-determination. Part II below now deals with the aforementioned new decisions.

The fear that has grasped the USA following the attacks of 11th of September, 2001 has not left Germany untouched. Although Germany has not yet been successfully hit by terrorists with an Islamic motivation, the German federal parliament (Bundestag) has enacted a long list of security laws to provide police and intelligence agencies with effective weapons for the "war on terror".[2] Most of these laws bear heavy impacts on the freedom rights of German citizens.

From February to March 2008, the German Federal Constitutional Court (Bundesverfassungsgericht) handed down three judgments that severely restricted both Acts

---

[1] The authors are researchers at the University Kassel/Germany and members of the "Project group for constitutionally compatible technology design (provet)". Disclaimer: The authors were among the 34,000 citizens that filed the lawsuit against data retention in Germany which led to the third decision of the Bundesverfassungsgericht (see below 3).

[2] An overview on the activities of the Bundestag from September 2001 to July 2006 to fight terrorist activities, provided by the scientific service of the German Bundestag, can be found at: http://www.bundestag.de/wissen/analysen/2007/terrorismusbekaempfung.pdf.

of Parliaments, and undertakings by the German federal and state police, and the German intelligence services. The reasonings of the three decisions are based on the groundbreaking population census decision which was explained in part one of this article.[3] The Bundesverfassungsgericht was rather explicit in its criticism. The acts controlled in these decisions suffered from severe procedural deficits, and they were drafted in much too general a manner to meet the requirements the Bundesverfassungsgericht has set up for security laws which have a heavy impact on the freedom rights of German citizens.

[Page 116]

1 Online-searching of Computers

On February 27th, 2008, the Bundesverfassungsgericht delivered its decision in a case concerning an act on the online searching of computers, enacted by the state of Nordrhein-Westfalen.[4] The new act authorised the Office for the Protection of the Constitution of the State (internal intelligence authorities) to, *inter alia*, "secretly access information technology systems through the use of technical means". The fact that no further indications were given regarding the mode of access gave rise to speculations on the potential technical approach. Possibilities include one-time online access to the data on the computer, continuous surveillance to tape-record any change of such data, and the observation of further operations (such as keyboard entries or VoIP calls).[5]

Following a heated debate on the subject within the political and scientific[6] communities, the Bundesverfassungsgericht held the Act as being unconstitutional. This was of no surprise since the aforementioned provisions did not entail any further substantial or procedural privacy safeguards, which are mandatory according to the population census decision.[7] However, the Court did not take the easy way to annul the act simply because of these deficiencies, since there was a discussion on introducing online-searches of computers as a general means in the federal police act, as well as in several acts of the state police. Instead, the Bundesverfassungsgericht established a new "fundamental right to confidentiality and integrity of information technology systems" in the reasons given for the judgment.[8]

The Bundesverfassungsgericht has taken the recent developments in the area of information and communication technology as a starting point. Much emphasis is placed on the major role played by these forms of technology in today's life and their ever increasing influence on the self-development of citizens. As the new technology depends largely on the processing of personal data, it has become obvious that there is a strong need for the protection of privacy. The Court did not consider the existing German system of fundamental rights to be sufficient in this respect. Secrecy of telecommunications, as protected in Article 10 of the Grundgesetz, did not cover online searching of computer systems. The Court considered secrecy of telecommunications as being applicable only if the authorities aim at the surveillance of VoIP

---

3 See G. Hornung/C. Schnabel, "Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination", [2009] CLSR 84-88.

4 Available via http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html (in German).

5 See in more detail U. Buermeyer, "Die Online-Durchsuchung", *HRR-Strafrecht* 2007, pp. 154 ff., available at http://www.hrr-strafrecht.de/hrr/archiv/07-04/index.php?sz=8.

6 See e.g. G. Hornung, "Ermächtigungsgrundlage für die 'Online-Durchsuchung'?", *Datenschutz und Datensicherheit* 2007, pp. 575 ff., available at http://www.uni-kassel.de/fb7/oeff_recht/publikationen/pubOrdner/publikation_2007_hornung_online_durchsuchung.pdf; J. Rux, "Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden", *Juristenzeitung* 2007, pp. 285 ff.; S. Schlegel, "Warum die Festplatte keine Wohnung ist", *Goltdammer's Archiv für Strafrecht* 2007, pp. 648 ff.

7 G. Hornung/C. Schnabel (above n. 3), p. 86 f.

8 On the judgment, see G. Hornung, "Ein neues Grundrecht", *Computer und Recht* 2008, pp. 299 ff.

systems, and the method of the surveillance (e.g. a Trojan horse or similar malware) is technically restricted to the telecommunications, i.e. searching of the system is not possible.

Regarding the sanctity of the home, there was a debate on whether the respective provision of the Grundgesetz (Article 13) applies in the case of the online searching of an IT system which is based in the home of the person affected. While there are solid arguments that this is the case,[9] the Bundesverfassungsgericht responded negatively, arguing that the location of the system is not usually apparent for the authorities, and that the fundamental right in Article 13 of the Grundgesetz has to be construed with regard to the modalities of the access. Lastly, the Bundesverfassungsgericht deemed the right to informational self-determination, developed in the population census decision,[10] as not covering the peculiarities of IT systems and their relevance for citizens' everyday lives.

Importantly, the inapplicability of the conventional fundamental rights in the German Constitution did not leave the plaintiffs unprotected. Building on earlier decisions, the Bundesverfassungsgericht emphasised what it calls the "gap-closing function of the general personality right". From there, it was only a small step to the creation of a "new"[11] fundamental right. This fundamental right protects "IT systems that may – as such, or within a network – store personal data to an extent that the searching of the system could disclose important parts of the conduct or life of a person or even a significant image of his/her personality".[12] Besides computers, mobile phones, PDAs and similar systems are also included "if they feature a wide range of functions and store and process personal data of different kinds". Crucially, it is not decisive whether the system actually stores or processes personal data to that extent, but whether the system is capable in that respect.

The system will only be protected if, given the concrete circumstances, the person affected can assume that he/she is able to control the system, whether alone or with other authorised persons. Arguably, this also includes online hard drives.

There are two aspects of the new right, namely, the confidentiality and the integrity of the system. The first aspect covers personal data and is thus largely congruent with the right to informational self-determination, although the requirements for interventions are much higher.[13] It applies if data is collected by public authorities from "outside" the system. The second aspect is described by the Bundesverfassungsgericht to protect against the unauthorised use of the system regarding its capacities, functions and memory contents. In this respect, it is irrelevant whether personal data of any kind is involved. This enhances the protection of the person affected.

[Page 117]

As to the limits of the fundamental right, the Bundesverfassungsgericht explained that secret online searching may be justified if there is "factual evidence indicating a concrete threat for an object of legal protection of utmost importance, such as the physical condition, life or freedom of a person, the fundaments or continuance of the state or the basis for the existence of humans".[14] Thus, there is no need to prove the existence of the concrete threat itself, but

---

[9] See G. Hornung (above n. 6), pp. 577 f. with further references.

[10] G. Hornung / C. Schnabel (above n. 3), p 85 f.

[11] Arguably, the "fundamental right to confidentiality and integrity of information technology systems" is not an independent fundamental right in itself, but a new subgroup of the general personality right. As this also holds true for the right to informational self-determination, the two are closely interrelated, albeit separated by different limits to legal restraints (see below).

[12] Para. 203 of the judgement.

[13] On the requirements for interventions into the right of informational self-determination, see G. Hornung / C. Schnabel (above n. 3), p. 86 f.

[14] Para. 247 of the judgement.

only for the facts indicating it. On the other hand, the Court made clear that there has to be a firm establishment of the factual evidence in a specific case, indications that the threat will turn into severe damage for public security[15] in the near future and the connection to individual persons responsible for the threat. It is of utmost importance that these requirements apply to intelligence agencies as well. Thus, there is no possibility for such authorities to use secret online searches of computers for the general gathering of information.

Even if the aforementioned requirements are met, the interference can only be justified if it is warranted by a judge or a body of equal legal and personal independence. Furthermore, the legal basis for the measure has to provide safeguards to prevent any infringements of the "core of personal privacy". The Court had specified this idea in its decision on acoustic surveillance of private homes,[16] requiring the surveillance to be interrupted if there are indications that it will affect, *inter alia*, expressions of innermost feelings or sexuality. In the current case, the Bundesverfassungsgericht considered it impossible to analyse the data, in this respect, at the time of collection. According to the technical experts in the court session, there are no technical means which would absolutely exclude data belonging to the core of personal privacy from the transfer to the authorities. In this situation, the judges demanded that the data is subsequently examined in this respect and deleted if it pertains to this sphere. However, there are neither indications in the judgment as to the body responsible for the examination, nor to the time within which the examination must take place. The legal provisions in a new act for the measure will need to address both questions, because it is both crucial that the body is independent from the authority responsible for the surveillance, and that the examination of the data proceeds within reasonable time.

Altogether, the Bundesverfassungsgericht specified rather high requirements for the secret online searching of IT systems, yet it is likely that politicians in the Bundestag, and in at least some of the state parliaments, are determined not to waste any time. Within the German federal government and the coalition in the Bundestag, a proposed federal law on the same subject has provoked a heated debate throughout the last year. While the Christian Democrats and their Minister of the Interior, Wolfgang Schäuble, claim that this measure is essential in combating organised crime and terrorism, many Social Democrats, such as the Minister of Justice, Brigitte Zypries, are rather sceptical. It is apparent from recent statements that the latter will nevertheless agree to a narrow provision in compliance with the new demands set by the Bundesverfassungsgericht. In any case, Mr Schäuble will have to re-draft his proposal on the issue, as it does not meet these constitutional requirements

The opinion of the Bundesverfassungsgericht delivers guidelines not only for the online searching of computer systems, but also for other surveillance measures. Hence, the ruling is widely recognised as the most important decision on privacy and constitutional law in Germany within recent years, arguably even since the famous census case of 1983.[17] There are numerous open questions to be addressed in future cases and in the scientific debate.[18] These include, *inter alia*, the consequences for open searches of IT systems (e.g. in the context of house searches), further dimensions of the new fundamental right in regards to the

---

[15] In German police law, this includes individuals' rights, facilities and activities of the state, and the legal order as such.

[16] Bundesverfassungsgericht, decisions volume 109, p. 279 (pp. 311 ff.).

[17] See part I of this article, G. Hornung / C. Schnabel (above n. 3), p. 84 ff. The former Minister of the Interior G. Baum stated that the court has finally arrived in the IT age and that the decision will have an impact on "the history of law", cf. Frankfurter Rundschau 14th of April, 2008.

[18] See G. Hornung (above n. 8).

effects between private parties,[19] and the issue of online searching of IT systems within criminal proceedings, which was not addressed by the Court in the current decision.

2 Automatic number plate recognition

Automatic number plate recognition (ANPR) is a technique[20] that can be used for different purposes. One of the most famous examples is the collection of the city toll of London's Congestion Charge Zone (CCZ). This example, however, demonstrates the usability for security purposes as well, as police forces were also given access to the data in the summer of 2007.[21] There is no distinct legal basis for this in England,[22] and there are plans to expand the ANPR system to store the details of up to 50 million recordings per day for up to five years.[23] In France, the same technique is used for the prevention and persecution of terrorism-related crimes,

[Page 118]

organised crime and customs violations.[24] As regards Australia, there were plans of state and federal police forces unveiled in September 2008 to install 5.000 cameras around the country to collect full-frontal images of vehicles, including the driver and front passenger, that are clear enough for identification purposes and usable as evidence in court.[25]

In nine of the German states, the respective police acts were changed in recent years to introduce the same technique.[26] In general, ANPR works as follows: Video cameras scan number plates of passing vehicles and, using special software, recognise the figures and letters. The recognised number plate is then matched against the police's wanted list for people and vehicles. If there is no match, the picture with the number plate and the recognised number plate are to be immediately deleted. If there is a match on the wanted list, a success notification is displayed and stored together with the time and place of the successful recognition. The police are then able to take follow-up measures, like following and stopping the car and arresting the driver.[27]

---

[19] See A. Roßnagel / C. Schnabel, "Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht", *Neue Juristische Wochenschrift* 2008, forthcoming. In German theory of fundamental rights, it is widely recognised by courts and scholars that the rights enshrined in the constitution not only protect the individual against the state, but also affect the construction of private law. This applies particularly to general clauses and terms which are open to valuation processes.

[20] For the technical basics of ANPR, see http://www.cctv-information.co.uk/constant3/anpr.html.

[21] A. Travis, "'Big Brother' plan for police to use new road cameras", Guardian 17th of July, 2007, via http://www.guardian.co.uk/uk/2007/jul/18/humanrights.terrorism.

[22] Cf. Office of Surveillance Commissioners, *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2006-2007*, 2007, pp. 3, 16 f., via http://www.surveillancecommissioners.gov.uk/docs1/OSC%20Annual%20Rpt%202006-07%20final%20version.pdf.

[23] Cf. P. Lewis, "Fears over privacy as police expand surveillance project", Guardian 15th of September, 2008, via http://www.guardian.co.uk/uk/2008/sep/15/civilliberties.police.

[24] Cf. Conseil Constitutionnel, Decision of 19th of January, 2006 – No 2005-532 DC, in English via http://www.conseil-constitutionnel.fr/decision/2006/2005532/2005532endc.htm.

[25] Cf. K. Dearne, "Privacy concerns on speed cameras", via http://www.australianit.news.com.au/story/0,24897,24387179-15306,00.html; see also the background paper of Information Integrity Solutions Pty Ltd, http://www.privacy.org.au/Papers/ANPR-Background-Paper.doc.

[26] These German states were Bayern, Brandenburg, Bremen, Hamburg, Hessen, Mecklenburg-Vorpommern, Rheinland-Pfalz, Schleswig-Holstein and Niedersachsen. Additionally, there were legislative procedures in Sachsen and Baden-Württemberg to enact similar laws.

[27] On the legal issues in Germany, see e.g. A. Roßnagel, *Kennzeichenscanning*, München 2008 (a short version of the expertise is available via http://www.uni-

After the state police acts of two states (Hessen and Schleswig-Holstein) were challenged before the Bundesverfassungsgericht, the court released its decision on ANRP on March 11th, 2008.[28] It ruled that both state provisions that allowed for ANPR[29] were unconstitutional and thus void.

The Bundesverfassungsgericht acknowledged that ANPR constitutes an intervention in the concerned individual's right to informational self-determination if the number plate is not unhesitatingly matched against the wanted list and immediately deleted afterwards, without further evaluation. Due to the huge potential for electronic data processing, which allows for huge amounts of data to be processed within milliseconds, the related protection of fundamental rights must be adjusted to the degree of danger to the right to informational self-determination. Therefore, it is of no relevance that the number plates are publicly visible. On the other hand, ANPR does not interfere with the right to informational self-determination if the data is deleted without a trace, and without the possibility of being restored in the case of no matches on the wanted list, and if this is guaranteed by legal and technical safeguards.[30]

However, the right to informational self-determination is not granted without any restrictions. Interventions into this right are possible when they are based on an enabling act that is, in itself, constitutional. The requirements for the safeguards depend on the intensity of the intervention in the concerned basic right, and apply to the proportionality criterion and the basic principles of clarity and certainty of the act.

The Bundesverfassungsgericht recognised different aspects to assess the intensity of the intervention, which are reflected by the relevance for the personality of the concerned individual. In the case of ANPR, this depends on the additional information that is gathered with the number plate match, such as the place and time of the filming of the number plate. Since some ANPR cameras are mobile, the intensity of the intervention varies, depending on where the individual has been filmed by the police and whether this allows for concluding details not only on the individual's movement, but also on further details of his/her lifestyle.[31] According to the Bundesverfassungsgericht, ANPR has a heavy impact on the right to informational self-determination due to the fact that it takes place without the concerned individual giving any reason for the procedure, and it can thus affect anybody. This could have an intimidating effect on citizens and as a result on the democratic constitutional state as a whole. In addition to the impact on the concerned individual's right to informational self-determination, there is the secrecy of ANPR, which may lead to factual restrictions on the possibility of legal remedies.

Due to the heavy impact on informational self-determination, there are high requirements as to the principles of clarity and certainty regarding the enabling act. The Bundesverfassungsgericht has already explained in the population census decision that the higher the impact on the freedom of the individual the higher are the demands to the principles of clarity and certainty regarding the enabling act and that the standards to be met

---

kassel.de/fb7/oeff_recht/gutachten_kennzeichenerfassung_2008_01_29.pdf); C. Arzt, "Voraussetzungen und Grenzen der automatisierten Kennzeichenerkennung", *Die Öffentliche Verwaltung* 2005, pp. 56 ff.

[28] Bundesverfassungsgericht, 11.3.2008 - 1 BvR 2074/05 and 1 BvR 1254/07, via http://www.bundesverfassungsgericht.de/entscheidungen/rs20080311_1bvr207405.html; on the decision, see A. Roßnagel, "Verfassungsrechtliche Grenzen polizeilicher Kfz-Kennzeichenerfassung, *Neue Juristische Wochenschrift* 2008, pp. 2547 ff.

[29] Sec. 14, para. 5 of the police act of Hessen and Sec. 184, para. 5 of the police act of Schleswig-Holstein.

[30] Bundesverfassungsgericht, 11.3.2008 - 1 BvR 2074/05 and 1 BvR 1254/07, para. 68; see also Bundesverfassungsgericht, decisions volume 100, p. 313 (p. 366); volume 107, p. 299 (p. 328); volume 115, p. 320 (p. 343).

[31] Bundesverfassungsgericht, 11.3.2008 - 1 BvR 2074/05 and 1 BvR 1254/07, para. 87.

by the enabling act are even higher when the intervening act itself is done secretly.[32] The state legislators could have known all of this by taking into account the population census decision.

The enabling acts did not meet these requirements, as they neither defined the preconditions for the use of ANPR, nor specified the purpose for which the collected data could be used.[33] Another problem was the absence of any legal definition of the "wanted list". Thus, ANPR could be used to investigate both capital crimes and minor misdemeanours. It was also unclear whether the systems could be used for long-term observations and for creating tracking profiles. Since the enabling acts did not clearly specify the purpose of ANPR, they were held as unconstitutional.[34]

According to the Bundesverfassungsgericht, the enabling acts also violated the principle of proportionality. As per this

[Page 119]

principle, every exercise of jurisdiction that intervenes with basic rights must follow a legitimate goal and must be adequate for achieving this goal. Furthermore, there must not be any equally adequate way of achieving the goal with methods that bear less of an impact on the basic rights of the concerned citizens, and the impact on basic rights must not be out of proportion compared to the goal and the probability of success.[35] The last aspect is the most critical one. It demands from the legislator to find a balance between two poles: first, the nature and intensity of the interferences into basic rights, and second, the importance of the Rechtsgut to be protected by the measure.[36]

The enabling acts for ANPR did not meet these high standards. Their purpose was broad and they allowed for area-wide filming of number plates of citizens who had not shown any reason for such a measure to be directed against them. The court stressed that these measures also convey the feeling of constant surveillance with all of its subsequent, negative effects. The legislators had not made use of any possibility to alleviate the impact on basic rights by, for example, restricting the use of ANPR to certain places, like border areas or places with high criminality rates. They had also not restricted the use of the collected data. Due to these extreme deficiencies, the enabling acts were declared unconstitutional and are thus void.

The ANPR-decision of the Bundesverfassungsgericht sparked the least controversy of the three new decisions. One of the reasons for this is the fact that there were very few successes to be named and it was difficult to establish a connection between the use of ANPR and the "war on terror", even for security politicians. Also, the biggest German Automobile Club (ADAC) had released an expert opinion on all the ANPR-state acts just a few weeks before the decision of the Bundesverfassungsgericht.[37] The expert opinion came to the devastating result that nearly all of the acts were unconstitutional and its presentation received great media attention.[38] When the Bundesverfassungsgericht took the same view as the expert

---

[32] See G. Hornung / C. Schnabel (above n. 3), p. 86.
[33] Bundesverfassungsgericht, 11.3.2008 - 1 BvR 2074/05 and 1 BvR 1254/07, para. 98.
[34] Bundesverfassungsgericht, 11.3.2008 - 1 BvR 2074/05 and 1 BvR 1254/07, para. 93.
[35] Cf. Bundesverfassungsgericht, decisions volume 109, p. 279 (pp. 335 ff.).
[36] Bundesverfassungsgericht, 11.3.2008 - 1 BvR 2074/05 and 1 BvR 1254/07, para. 169.
[37] A. Roßnagel, (above n. 27); A. Roßnagel, "Verdachtslose automatisierte Erfassung von Kfz-Kennzeichen", *Deutsches Autorecht* 2008, pp. 61 ff.
[38] See T. Hillenbrand, "Nummernschild-Scanning verstößt gegen Verfassung", Spiegel-Online 29th of January, 2008, via http://www.spiegel.de/auto/aktuell/0,1518,531451,00.html; S. Schulz, "Bürgerrechte auf der Autobahn", taz 29th of January, 2008, via http://www.taz.de/1/debatte/kommentar/artikel/1/buergerrechte-auf-der-autobahn/?src=AR&cHash=fbb4fe582f; A. Berger, "Big Brother fährt mit", Financial Times Deutschland 29th of January, 2008, via http://www.ftd.de/politik/deutschland/:Big%20Brother/309348.html; "ADAC: Scannen von Auto-Kennzeichen verfassungswidrig", heute.de 29th of January, 2008, via http://www.heute.de/ZDFheute/inhalt/25/0,3672,7152729,00.html.

advice just a few weeks later, the level of surprise was limited. Also, the Bundesverfassungsgericht did not rule ANPR to be unconstitutional in any event, but, rather, declared the acts at hand to be unconstitutional due to their severe legislative-technical deficiencies. Following the legal practice of the Bundesverfassungsgericht, ANPR can be introduced in Germany if certain privacy safeguards are foreseen.

3 Data retention

The idea to preserve all data referring to the circumstances of every act of telecommunication, without a given suspicion, is not new. German security politicians have repeatedly tried to enact a provision forcing data retention on access providers and telecommunication operators. The Bundestag has always rejected this idea[39] and named the strict legal practice of the Bundesverfassungsgericht as one of the main reasons why such an undertaking could not be successful in Germany. Another reason is that such an undertaking would be out of proportion since it would affect both suspected criminals and completely innocent citizens.

3.1 The route via Europe

At first, a European-wide retention of data was planned to be enacted as a framework decision. When it was made evident that the required unanimity could not be achieved, the decision was made to enact it as a directive. Despite the concerns over privacy violations repeatedly uttered by all the political parties in the Bundestag, the Christian Democratic and the Social Democratic members of the European parliament have voted for the plans of data retention initiated by France, Great Britain[40], Ireland and Sweden.

Therefore, at some point in 2005, German security politicians must have considered ordering data retention as an act of European law as a clever way of avoiding the strict legal practice of the Bundesverfassungsgericht. The reason for this lies in the structure of the European Union and the complicated relationship between the European Court of Justice and the Bundesverfassungsgericht. Until the middle of the 1980s, the Bundesverfassungsgericht reserved itself the right to check every legal act of the European Community which affected the basic rights of German citizens and the right to annul it if the legal act proved to be incompatible with the German constitution. The Bundesverfassungsgericht explicitly ruled this out in 1974 with the "as-long-as-I" decision.[41] In 1986, the "as-long-as-II" decision came into effect, and has remained valid until this day.[42] It states that the Bundesverfassungsgericht will practice judicial self-restraint and will not decide any case filed against legal acts coming from the European Community or Union.

> *„As long as the European Community, especially the jurisdiction of the European Court of Justice, provides an effective protection of basic rights against the acts of the Community in general, that does not fall below what is deemed as indispensable by the Grundgesetz, (…),the Bundesverfassungsgericht will not*

[Page 120]

---

[39] Remarkably, the last rejection took place on the 27th of February, 2005; cf. Bundestags-Drucksache 15/4597, p. 3 (available at http://dip.bundestag.de/btd/15/045/1504597.pdf).

[40] For Home Office plans of a 12-month long retention of phone and e-mail data in a central data base, see R. Ford, "Big Brother's database for phones and e-mails", Times 20th of May, 2008, via http://business.timesonline.co.uk/tol/business/industry_sectors/telecoms/article3965033.ece.

[41] Bundesverfassungsgericht, decisions volume 37, pp. 271 ff.

[42] Bundesverfassungsgericht, decisions volume 73, pp. 339 ff.

exercise its jurisdiction on national acts derived from Community law, (…) and will not check these laws against the basic rights of the Grundgesetz; such lawsuits following Article 100, para. 1 of the Grundgesetz will be considered inadmissible."[43]

This practice has been repeatedly confirmed, lastly in the banana-market decision from 2000.[44]

The Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (Directive 2006/24/EC) was enacted by the European Parliament and the Council on the 15th of March, 2006.[45] It was the fastest legislative procedure in the history of the European Union.[46] The Directive 2006/24/EC obliges Internet service providers and telecommunication operators to store the communication data of all their users and subscribers for a period of 6 to 24 months. "Data" means traffic and location data and the related data necessary to identify the subscriber or user, according to Article 1, para. 2 of the Directive 2006/24/EC. Any data referring to the content of the communication is excluded from the ambit of the directive. Article 5 of the Directive 2006/24/EC defines in detail the types of data to be stored. This data is destined by Directive 2006/24/EC for the investigation, detection and prosecution of serious crime. Providers are obliged to store only data generated or processed in the process of supplying their communications services. If the data is not already generated by the provider in the process of supplying their communications services, there is no obligation to collect and retain it.[47]

When the public became aware of the existence of Directive 2006/24/EC and the plans for its transposition, a heated public debate was sparked. The criticism from legal scholars in Germany was intense and sometimes devastating.[48] A former Minister of Justice from the liberal party (FDP) even accused the government of provoking a constitutional crisis by driving the Bundesverfassungsgericht to review its present legal practice and thus endangering the European process of integration.[49] At the European level, the European Data Protection Supervisor Peter Hustinx accused the European Union of using terrorism as an excuse for privacy breaches.[50] The Advocate General Juliane Kokott also doubted the compatibility of data retention with European fundamental rights.[51] The Article 29 Working Party had strong reservations about data retention, since it would constitute a change of

---

[43] Bundesverfassungsgericht, decisions volume 73, p. 387.

[44] 7.6.2000 - 2 BvL 1/97, via http://www.bverfg.de/entscheidungen/ls20000607_2bvl000197.html (in German).

[45] Official Journal L 105, 13.4.2006, p. 54, via http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2006/l_105/l_10520060413en00540063.pdf.

[46] For details on the legislative procedure see A. Alvaro, "Die Richtlinie zur Vorratsdatenspeicherung", *Datenschutz Nachrichten* 2/2006, pp. 52 ff.; see also O. Leistert, "Data Retention in the European Union: When a Call Returns", *International Journal of Communication* 2008, pp. 925 ff.

[47] Cf. Recital 23 Directive 2006/24/EC.

[48] R. Gitter / C. Schnabel, "Die Richtlinie zur Vorratsspeicherung und ihre Umsetzung in das nationale Recht", *MultiMedia und Recht* 2007, pp. 411 ff., via http://www.uni-kassel.de/fb7/oeff_recht/publikationen/pubOrdner/mmr07-07_Gitter_Schnabel.pdf; D. Westphal, "Die neue EG-Richtlinie zur Vorratsdatenspeicherung", *Europäische Zeitschrift für Wirtschaftsrecht* 2006, pp. 555 ff.; J. Rauhofer, Legislative developments in relation to the mandatory retention of communications data in the European Union, (2006) 3:4 *SCRIPTed* 322, via http://www.law.ed.ac.uk/ahrc/script-ed/vol3-4/rauhofer.asp.

[49] S. Leutheusser-Schnarrenberger, "Vorratsdatenspeicherung – Ein vorprogrammierter Verfassungskonflikt", *Zeitschrift für Rechtspolitik* 2007, pp. 9 ff.

[50] Quoted via http://www.theregister.co.uk/2006/09/19/terrorism_privacy_breaches; in the hearing of the ECJ on data retention, Hustinx surprisingly supported the enactment of data retention at least as far as choosing a directive as a legal basis is concerned, much to the shock of data protection activists.

[51] Opinion of the Advocate General, 18 July 2007, C-275/06, Promusicae vs. Telefónica de España, para 82, via http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=EN&Submit=Rechercher$docrequire=alldocs&numaff=C-275/06&datefs=&datefe=&nomusuel=&domaine=&mots=&resmax=100.

paradigm from collecting and processing as little data as possible to storing the communication data of every citizen within the European Union, which is not considered compatible with the principles of privacy and democracy as enshrined in the European Charta of Human Rights, the European constitution, and the constitutions of the Member States.[52]

At the same time, data protection became a topic in a societal debate. The plans of the German government led to the foundation of new NGOs, like the "Arbeitskreis Vorratsdatenspeicherung"[53] and others, that massively campaigned against the transposition of Directive 2006/24/EC. All this public debate culminated in the biggest class-action suit the Bundesverfassungsgericht has ever been faced with: More than 34,000 citizens filed an individual lawsuit against the implementation of Directive 2006/24/EC as it was planned.[54]

In the meantime, Ireland had filed an action of nullity before the European Court of Justice to annul Directive 2006/24/EC because of a lack of competence of the legislating bodies, namely the European Parliament and the Council.[55] Since the main or predominant purpose of the directive is to facilitate the investigation, detection and prosecution of serious crime, including terrorism, it can be argued, the only permissible legal basis for the measures contained in the directive is Title VI of the Treaty on European Union, in particular Articles 30, 31(1)(c) and 34(2)(b). Thus, the correct legal basis for data retention would be a framework decision, just like the Council had originally intended.[56] However,

[Page 121]

Advocate General Ives Bot invited the Court to dismiss Ireland's action.[57] He argued that the Directive 2006/24/EC is intended to improve the conditions for the establishment and functioning of the internal market and is therefore correctly based on Article 95 EC. The European Court of Justice recently announced its decision on the 10 February 2009. It rejected Ireland's action of nullity, which means Directive 2006/24/EC remains valid and is applicable law.

3.2 The decision of the Bundesverfassungsgericht

Consequently, Germany implemented the directive into the Federal Telecommunications Act. The new provisions entered into force on the 1 of January, 2008. On the 11 March, 2008, the Bundesverfassungsgericht granted an injunction and temporarily prevented the application of the new provisions transposing Directive 2006/24/EC.[58] It was decided that the telecommunications operators and internet service providers still have to store the data, but they are not allowed to transfer the data to law enforcement agencies unless the conditions of Section 100a of the Code of Criminal Procedure are met. Section 100a of the Code of Criminal Procedure was composed for wiretapping and is only applicable when there is suspicion that a serious crime has been committed (like murder, rape, violation of the

---

[52] Article 29 Data Protection Working Party, Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council 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, March 2006 via http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp119_en.pdf.

[53] Via http://www.vorratsdatenspeicherung.de/index.php?lang=en.

[54] The German procedure law does not recognise class-action suits. Technically, these had to be considered as 34,000 single lawsuits. Among the complainants were former Ministers of Justice and the Interior.

[55] Official Journal C 237, 30.09.2006, p. 5, via http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:237:0005:01:EN:HTML.

[56] See above.

[57] Cf. Press Release No 70/08, 14.10.2008, via http://curia.europa.eu/en/actu/communiques/cp08/aff/cp080070en.pdf.

[58] Bundesverfassungsgericht, 11.3.2008 - 1 BvR 256/08, via http://www.bundesverfassungsgericht.de/entscheidungen/rs20080311_1bvr025608.html.

narcotics law, or a similarly severe crime). In addition, the federal government was ordered to report to the Bundesverfassungsgericht on the practical impact of the data retention. The Bundesverfassungsgericht also considered it necessary to order the German states and the Federal Public Prosecutor to supply the federal government with the information necessary to deliver their report to the Bundesverfassungsgericht.[59]

First, the Bundesverfassungsgericht had to decide about the admissibility of the interim injunction. It stuck to its "as-long-as" legal practice and decided not to stop or even check legal acts of the European Community. However, due to the fact that Ireland had filed an action of nullity against Directive 2006/24/EC to the European Court of Justice, it could not be ruled out that the directive might be annulled. In that case, the Bundesverfassungsgericht would be able to check all of the changes made in the Federal Telecommunications Act to transpose the data retention directive.[60] Furthermore, the Bundesverfassungsgericht recognised that the changes in the Federal Telecommunications Act go beyond the changes required to effectively transpose Directive 2006/24/EC, because the act allowed for data transfers not only for criminal prosecution means, but also for preventive measures and other acts of law enforcement.[61] Moreover, the obligations to store data were more extensive than the provisions of Directive 2006/24/EC demanded.[62] Thus, the lawsuits were admissible.

The decision is remarkable in itself, because successful interim injunctions by the Bundesverfassungsgericht are very rare. The basis for a decision on an interim injunction is an appreciation of values. The Bundesverfassungsgericht had to weigh the negative effects of dismissing the interim injunction if the main proceedings were successful against the negative effects of granting an interim injunction if the main proceedings were not successful. Less surprising than the fact that the court granted an interim injunction at all was the court's highly critical position against data retention. The Bundesverfassungsgericht had already argued in the population census case that the collection of data for unspecified purposes was a violation of the concerned citizen's right to informational self-determination.[63]

Following this appreciation of values, the Bundesverfassungsgericht ruled out the possibility of completely forbidding the storing of traffic data. However, it restricted the use of this data to the sole purpose of investigating serious crimes (like murder, rape, violations of the narcotics law or similarly severe crimes), while the transposing act had also allowed for the use in cases in which a crime had been committed via telecommunications, without any reference to the weight of the crime.

The Bundesverfassungsgericht decided that the complete retention of traffic data without any reason given by the monitored citizen, as planned in the transposition act, would have an extremely intimidating effect on citizens.[64] Yet, the negative effect on the liberty and privacy of citizens would only be brought about if the transfer of traffic data to security authorities

---

[59] The reporting judge for all three decisions, W. Hoffmann-Riem, left the Bundesverfassungsgericht after the data retention decision as he had reached the age limit, and afterwards, gave an interview in which he stated that it had been fairly difficult to get any information from the government on the expected impact of data retention on basic rights and the success probability, see Süddeutsche Zeitung 12th / 13th of April, 2008, p. 7, via http://www.sueddeutsche.de/deutschland/artikel/992/168505/.

[60] Bundesverfassungsgericht, 11.3.2008 - 1 BvR 256/08, para. 137.

[61] Bundesverfassungsgericht, 11.3.2008 - 1 BvR 256/08, para. 136.

[62] Although this was obvious for anybody who had read both the Directive 2006/24/EC and the act of transposition, the Minister of Justice had repeatedly insisted that only the very minimum of Directive 2006/24/EC would be implemented into German law.

[63] See G. Hornung / C. Schnabel (above n. 3), p. 87.

[64] Bundesverfassungsgericht, 11.3.2008 - 1 BvR 256/08, para. 148; see also Bundesverfassungsgericht, decisions volume 113, pp. 29, 46.

were possible. This is why the Bundesverfassungsgericht considered it to be sufficient to stop the data transfer.

The data transfer could, in the opinion of the Bundesverfassungsgericht, severely impact the personality rights of affected citizens.[65] Moreover, data retention would affect nearly every citizen when using any form of telecommunication. A vast amount of sensitive data about practically every citizen would be made available for administrative access. This could have a heavy impact not only on individuals, but on society itself.[66] It could even unnecessarily stop exchange of communication amongst citizens, thus hindering them from making use of telecommunication devices. Such intimidating effects would be incompatible with the secrecy of telecommunications as guaranteed in Article 10, para. 1 of the

[Page 122]

Grundgesetz. The analysis of traffic data allows for the extensive analysis of the concerned individual's communication behaviour and his/her social contacts. After data has been transferred, such effects could not be undone.

The possible negative effects of granting an interim injunction if the main proceedings were not successful were outweighed by the considerations above. The Bundesverfassungsgericht also had problems evaluating the importance of access to traffic data for criminal investigations. Only one survey, from 2005, exists on this matter. It concluded that in only 2-4% of criminal investigations, traffic data that was needed was no longer available.[67] Although the Ministry of Justice found this survey to be insignificant, because it was outdated and too few cases were subject to the survey,[68] it did not offer any other material that could have convinced the Bundesverfassungsgericht.[69]

Thus, the Bundesverfassungsgericht ordered a preliminary stop to the transfer of traffic data under the new Federal Telecommunications Act until a decision on the merits has been made. A decision by the European Court of Justice on Ireland's action of nullity against Directive 2006/24/EC was delivered on the 10 February, 2009. Since the European Court of Justice decided to dismiss Ireland's action, the situation in Germany is unforeseeable. The Bundesverfassungsgericht could stick to its as-long-as II jurisdiction and allow for data retention, which it has so far always considered being unconstitutional, or it could decide that the European Court of Justice does not provide an effective protection of basic rights anymore and thus exercise its own jurisdiction again. The first way would be a blow for the Bundesverfassungsgericht, because it would mean that German security politicians could in the future introduce privacy by taking the European indirection, thereby *de facto* overpowering objecting rulings of the Bundesverfassungsgericht. Giving up the as-long-as II jurisdiction and exercising its own jurisdiction again would however mean a judicial earthquake the likes the European Community has never seen before and could endanger the process of the European integration altogether.

---

[65] Bundesverfassungsgericht, 11.3.2008 - 1 BvR 256/08, para. 155 f.

[66] For the parallel argumentation in the census case see G. Hornung / C. Schnabel, (above n. 3), p. 85 f.

[67] Max-Planck-Institute for foreign and international criminal law, *Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO*, via http://www.ak-vds.de/images/mpi-gutachten.pdf.

[68] Bundesverfassungsgericht, 11.3.2008 - 1 BvR 256/08, para. 4; ironically, the Ministry of Justice was the client for the survey.

[69] A survey by the German federal police in 2005, which was explicitly done to "stress the importance of data retention", concluded that in recent years, there had been 381 cases in which it was impossible to identify a suspect due to the lack of traffic data. Even if these cases could have been solved with such data, the percentage of crimes solved could only go up by 0.006% from 55% to 55.006%.

4 Conclusion

The recent developments show an ambivalent situation of data protection in Germany: On the one hand, the Bundesverfassungsgericht is self-confident and willing to stop the excesses of security politics and laws we have witnessed in the last couple of years. While the point of view the Bundesverfassungsgericht has taken may be called radical, and is not representative for the situation in Europe, it is not the Bundesverfassungsgericht that has changed. Rather, its decisions are all dominated by legal principles that are as old as data protection itself. Also, in none of the decisions did the Bundesverfassungsgericht rule that the plans of the government were by all means unconstitutional, but, on the contrary, it criticised the legislative-technical deficiencies, such as the lack of privacy safeguards or a violation of the principles of clarity and certainty regarding the enabling act.

On the other hand, there is an obvious "division of tasks": The protection of fundamental rights is a job that is being exclusively left to the Bundesverfassungsgericht, while the federal government and parliament are only taking responsibility for security and the intervention into privacy and other fundamental rights that are thus deemed necessary.[70] The first enabling acts for new security measures are often produced hastily and with little care. When the court scraps an enabling act, it is no longer considered either a defeat or a disgrace for parliament and government, but rather seen as something that regularly occurs in the course of legislative procedures. Although, in the constitutional framework, the executive and the legislative branch should be responsible for protecting fundamental rights as well, as stated in Article 1, para. 3 of the Grundgesetz. Instead, enabling acts are enacted without privacy safeguards and the scrapping rulings of the Bundesverfassungsgericht are then used like expert opinions to see which safeguards are absolutely necessary to avoid the enabling act from being annulled again. The new version of the enabling act is then to be drafted in a way that fulfils the absolute minimum of what the Bundesverfassungsgericht considers necessary for an enabling act to be constitutional.

This "assignment of tasks" not only violates the spirit of the constitution, but is also dangerous. The decisions of the Bundesverfassungsgericht are nearly always political decisions[71] and the pressure from security politicians is increasing. If the Bundesverfassungsgericht gave up its position, there would be no defence left against the unconstitutional invasion of the privacy of citizens.

Dr Gerrit Hornung *LLM (European Law) (gerrit.hornung@uni-kassel.de) and* **Christoph Schnabel** *LLM (Legal Informatics) (c.schnabel@uni-kassel.de) University of Kassel, Germany.*

---

[70] 26 MPs from the social democratic party claimed they had severe political and constitutional doubts about data retention, but still voted for a transposition of the data retention act and justified this with the opinion that basic rights will be preserved because the Bundesverfassungsgericht will stop the transposition nonetheless, or at least reduce it to something constitutional, cf. stenographic report of the 124th session, annex 4, p. 90, via http://dip.bundestag.de/btp/16/16124.pdf.

[71] Cf. W. Hassemer, "Politik aus Karlsruhe?", *Juristenzeitung* 2008, pp. 1 ff.