German Federal Constitutional Court

German Data Retention Provisions Unconstitutional In Their Present Form; Decision of 2 March 2010, *NJW* 2010, p. 833.

Anna-Bettina Kaiser*

Introduction

About one year after the European Court of Justice had handed down its notorious decision[1] on the Data Retention Directive concerning telecommunications traffic data,[2] it was for the German Federal Constitutional Court to take a final decision on the German implementation of the Directive.[3] So far, the latter Court had only issued temporary injunctions restricting data retrieval by the public authorities.[4] Now, the final ruling by the Court has been anxiously awaited since the complainants had not only challenged the German provisions implementing the Directive, but also the Directive itself. Thus, the question was raised whether the Court would finally, for the first time in its history, initiate a preliminary ruling procedure according to Article 267 of the Treaty on the Functioning of the European Union. Or, alternatively, whether the Court itself would declare the Directive to be *ultra vires*, an option that seemed even more probable after the Court's *Lisbon* decision.

At the end of the day, the Court avoided an open conflict with the European Court of Justice. Whereas the Federal Constitutional Court declared the relevant

* Assistant Professor at the Humboldt University, Berlin. I wish to thank Jeremy Bierbach, Lars Hoffmann, Jordan Long and Jan-Herman Reestman for valuable comments on earlier drafts.

[1] ECJ 10 Feb. 2009, Case C-301/06, *Ireland* v. *Parliament/Council*.

[2] Directive 2006/24 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* [2006] L 105/54, 13.4.2006.

[3] An official English version of the ruling does not exist. However, the FCC issued an elaborate Press Release available in English on <www.bundesverfassungsgericht.de/en/press/bvg10-011en.html>, visited 15 Sept. 2010.

[4] BVerfG 11 March 2008, *BVerfGE* 121, 1, repeated for four times: BVerfG 1 Sept. 2008, *BVerfGE* 121, 391; BVerfG 28 Oct. 2008, *BVerfGE* 122, 120; BVerfG 22 April 2009, *BVerfGE* 123, 89; BVerfG 15 Oct. 2009, *BVerfGE* 124, 299.

European Constitutional Law Review, 6: 503–517, 2010

doi:10.1017/S1574019610300083

German implementation to be unconstitutional and void, it held in the meantime that there existed possibilities to implement the Data Retention Directive in a constitutional manner. In this way, the Court left the Directive untouched and also met the data protectionists halfway, quashing the German statutes that virtually nobody wanted to defend anymore. However, there remain certain prices to pay for this intended harmony: the warning issued towards the European Court of Justice by the Federal Constitutional Court in the *Maastricht*[5] and the *Lisbon*[6] rulings to set aside *ultra vires* acts might be increasingly regarded as a toothless tiger.[7] In addition, privacy advocates might have to swallow data retention after all.

The note on this case is organised as follows. The first section examines the legal and political context of the Federal Constitutional Court's judgment. In the second section, the German legal framework relevant to the decision is presented, before the main findings of the ruling itself are examined in a third step. Finally, the most significant effects of the judgment are the focus of the conclusion.

The legal and political context

The setting of the Federal Constitutional Court's ruling is determined by four main factors: the strong tradition of data protection in Germany, the ruling by the European Court of Justice in the data retention case in 2009, the *Lisbon* ruling by the Federal Constitutional Court in 2009 and, finally, the security dimension of the case. Thus, the ruling by the Federal Constitutional Court can be understood best if it is placed in this parallelogram of forces that is to be unfolded in the following section.

The strong tradition of data protection in the Federal Republic

At least since the 1970s, the Germans have developed a close relationship towards data protection. Not only did the *Land* Hessen adopt the first data protection act in the world in 1970, but that act was followed by the Federal Data Protection Act [*Bundesdatenschutzgesetz*] in 1977.[8] Moreover, the German Federal Constitutional Court invented the famous right to informational self-determination (*Recht auf*

[5] BVerfG 12 Oct. 1993, *BVerfGE* 89, 155.

[6] BVerfG 30 June 2009, *BVerfGE* 123, 267.

[7] This is even more true for the recent *Mangold* (or *Honeywell)* decision by the FCC, BVerfG 6 July 2010. The decision is available, as well as all the other decisions of the FCC, on <www.bundesverfassungsgericht.de/entscheidungen.html>. A Press Release in English is also available on <www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-069en.html>, visited on 15 Sept. 2010.

[8] Bundesdatenschutzgesetz [Federal Data Protection Act], BGBl. I [Federal Law Gazette I] 201 ff.

https://doi.org/10.1017/S1574019610300083 Published online by Cambridge University Press

informationelle Selbstbestimmung), i.e., the right of individuals to decide whether or not to disclose personal information and also to decide about their usage, subject to certain limitations. This right, an extension of the so-called general personality right, was coined in the landmark *Census Act* decision of 1983, a decision that heavily influenced the jurisprudential and legislative climate in the following decades.[9] Accordingly, the right to informational self-determination was invoked in several cases of security legislation and has proved to be a sharp sword even in times of terrorism. Famous examples are the case on the automatic recording of vehicle number plates[10] or on dragnet investigations.[11] In the first case, the Federal Constitutional Court declared security legislation null and void, in the latter the application as unconstitutional, both times basing itself on the right to informational self-determination.

Against this backdrop, it is not astonishing that the European directive on the retention of data, and in particular the German implementation, was received with great suspicion by the German public, as well as in legal academia.[12] In particular, data collection *without occasion* seemed to contravene the very basic German principle of data protection, a doctrine also known on the European level, that was pointed out in the famous Census Act decision and elaborated in later judgments: a precautionary collection of non-anonymised data for undefined or not yet definable tasks would be unconstitutional.[13] The seemingly blatant contravention of this constitutional principle might explain why about 34.000 (!) complainants lodged constitutional complaints against the German provisions implementing the Data Retention Directive (and the Directive itself), the highest number of complainants in one case in the history of the Court. Data protection can rightly be called the Germans' sacred cow.

What is more, the most famous complainant had quite a high profile; she is the current German federal minister of justice, Sabine Leutheusser-Schnarrenberger. She lodged her complaint when she still was a member of the opposition for the Liberal Democratic Party during the time of the grand coalition between the Christian democrats and the social democrats that lasted until October 2009. The change in roles with her party's accession to government demonstrates the complexity of the issue. Would she sit with the complainants or with the German government commenting on and, most of the time, also defending the statutes challenged at

[9] BVerfG 15 Dec. 1983, *BVerfGE* 65, 1.

[10] BVerfG 11 March 2008, *BVerfGE* 120, 378.

[11] BVerfG 4 April 2006, *BVerfGE* 115, 320.

[12] The most active part played the civic movement 'Arbeitskreis Vorratsdatenspeicherung' [working group data retention], *see* <www.vorratsdatenspeicherung.de>, visited 15 Sept. 2010. *See also* K. Graulich, 'Telekommunikationsgesetz und Vorratsdatenspeicherung', *Neue Zeitschrift für Verwaltungsrecht* (2008) p. 485 at p. 489.

[13] BVerfG 15 Dec. 1983, *BVerfGE* 65, 1 at p. 46.

the Federal Constitutional Court? The ambiguity of her role in particular helps to understand why the implementing statutes were defended only half-heartedly.

The ruling by the European Court of Justice on the Data Retention Directive

After what has been said so far on the importance of data protection in Germany, it comes as no surprise that the ruling by the European Court of Justice of February 2009 gave rise to strong disapproval in the Federal Republic, essentially for three reasons. First, rightly or wrongly, few were convinced by the Court's argument that the Data Retention Directive was really about the functioning of the internal market; in the view of most German commentators,[14] the Directive was concerned with combating crime and terrorism,[15] therefore belonging to the third pillar of the European Union in its pre-Lisbon form. Hence, according to the prevailing view of most of the German legal scholars, and following the Irish line of argument in the case, the Directive could not have been based on Article 95 EC (now Article 114 of the Treaty on the Functioning of the European Union, TFEU). Instead, a framework decision of the third pillar would have been the appropriate measure.

Second, and given the fact that the Court of Justice accepted Article 95 EC as a legal basis, there was little understanding that the Court avoided an examination of the compatibility of the Directive with the right to privacy as provided for by Article 8 of the European Convention on Human Rights. While it is true that Ireland as applicant did not invoke this substantive argument, the incompatibility was ultimately put forward after all by the Slovak Republic as supporting intervener.[16] Accordingly, the European Parliament and the Council mentioned the ECHR in their comments.[17]

Third, the ruling by the Court of Justice seemed to fit in a series of decisions where the European Court was all too willing to interpret the competences of the European institutions, including its own competences, in quite a broad manner.[18] Thus, in the data retention case, the Court does not seem to take the problem of the cross-pillar measure serious enough; instead, it argues that the 'competence in

[14] *See* S. Simitis, 'Der EuGH und die Vorratsdatenspeicherung oder die verfehlte Kehrtwende bei der Kompetenzregelung', *Neue Juristische Wochenschrift* (2009) p. 1782; J.P. Terhechte, 'Rechtsangleichung zwischen Gemeinschafts- und Unionsrecht – die Richtlinie über die Vorratsdatenspeicherung vor dem EuGH', *Europäische Zeitschrift für Wirtschaftsrecht* (2009) p. 199. But *see* S. Poli, 'The Legal Basis of Internal Market Measures With a Security Dimension', 6 *European Constitutional Law Review* (2010) p. 137 at p. 140 and p. 151.

[15] These objectives were also mentioned in the Directive.

[16] ECJ 10 Feb. 2009, Case C-301/06, *Ireland* v. *Parliament/Council*, para. 34.

[17] Ibid., para. 39 and para. 46.

[18] The probably most well-known example from a German perspective is the so-called *Mangold* ruling, ECJ 22 Nov. 2005, Case C-144/04, *Mangold* v. *Helm*.

issue has already been accorded to the European Union in the broad sense.'[19] As a matter of fact, the unanimity required for a framework decision could have never been achieved. So it was a bad omen for the Constitutional Court's *Lisbon* decision that the European Court of Justice delivered its judgment on the Data Retention Directive during the oral proceedings of the *Lisbon* case. This leads us to the third relevant aspect.

The Lisbon ruling by the Federal Constitutional Court

This paper is not the proper place to give a comprehensive account of the *Lisbon* ruling by the Federal Constitutional Court.[20] Instead, this short comment will be limited to the passages of the judgment that are relevant to the present case as well as to the reception of the decision in Germany and abroad. As is well-known, the Court declared the German Act approving the Treaty of Lisbon to be constitutional. However, concerning its own future scope of review, the Federal Constitutional Court added two important caveats: first, the Court repeated that it would always reserve its right to declare acts by Community or Union institutions to be *ultra vires* where those institutions had transgressed the boundaries of their competences. Second, using novel reasoning, the Court introduced a review as to whether the inviolable core content of the constitutional identity of the Basic Law was respected.[21] Both reviews could lead to a declaration of inapplicability of Community or Union law in Germany.[22]

After what has been said on the reception of the ruling by the Court of Justice on the Data Retention Directive in Germany so far, it becomes clear that the outcome of whether or not the Federal Constitutional Court would back up its words from the Lisbon decision in the data retention case was awaited with interest. However, since the Federal Constitutional Court was heavily criticised for its *Lisbon* ruling,[23] the use of the *ultra vires* doctrine by the German Court would have been a difficult step to take. As will become apparent later, it was not the *ultra vires* clause, but, quite unexpectedly, the identity review that the Federal Constitutional Court referred to.

[19] ECJ 10 Feb. 2009, Case C-301/06, *Ireland* v. *Parliament/Council*, para. 56.

[20] BVerfG 30 June 2009, *BVerfGE* 123, 267. This decision is available in English on <www.bundesverfassungsgericht.de/en/decisions/es20090630_2bve000208en.html>, visited 15 Sept. 2010.

[21] Ibid., para. 240.

[22] Ibid., para. 241.

[23] *See*, e.g., D. Halberstam/C. Möllers, 'The German Constitutional Court says "Ja zu Deutschland!"', 10 *German Law Journal* (2009) p. 1241 <www.germanlawjournal.com/index.php?pageID=11&artID=1157>, visited 15 Sept. 2010. *But see* A. Voßkuhle, 'Multilevel cooperation of the European Constitutional Courts: Der Europäische Verfassungsgerichtsverbund', 6 *EuConst* (2010) p. 175.

Data retention as part of the security legislation

Last but not least, it is important to keep in mind that the data retention case is above all a case on security law. As such, the case has to be placed in the context of other judgments by the Federal Constitutional Court on security legislation. In fact, in recent years, numerous constitutional complaints were lodged against all important acts concerning security legislation, e.g., against the online search of computers, the above-mentioned dragnet investigation, the automatic recording of vehicle number plates, the major acoustic surveillance of private premises (*Großer Lauschangriff*) and the new legal basis in the air security law (*Luftsicherheitsgesetz*) enabling the state to shoot down a hijacked passenger aircraft. In all of the mentioned cases, the Federal Constitutional Court set aside the new provisions or had constitutional concerns with the application. However, as a general pattern of the security cases, it might be said that the Federal Constitutional Court has always tried to reach a compromise. Thus, none of the new measures – with the exception of the air security law – were declared to be *a priori* unconstitutional. Yet, often the existing legal prerequisites for the application of the new measure were held to be insufficient or the application was lacking in view of the standard of proportionality. As will be shown, this argumentative pattern also applies to the data retention case.

The German legal framework

After tough debates, the German law implementing the Directive 2006/24/EC was enacted on 21 December 2007,[24] modifying above all the Federal Telecommunications Act (*Telekommunikationsgesetz*) and the Federal Code of Criminal Procedure (*Strafprozessordnung*). As to the Telecommunications Act, two new provisions were introduced (§§ 113a and b). § 113a of the Telecommunications Act required, according to Article 3 of the Directive, the retention of data generated or processed by providers of publicly available electronic communications services or of public communications networks. Furthermore, the article ensured a six-month period of retention, the minimum period required by Article 6 of the Directive, plus an extra month for the destruction of the data. Concerning data security, § 113a of the Telecommunications Act remained rather laconic, asking the providers for no more than for the 'requisite care' in the area of telecommunications (*erforderliche Sorgfalt*), in particular by adopting technical and organisational measures to ensure that the data can be accessed only by specially authorised personnel.

[24] Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG [Act for the Amendment of Telecommunications Surveillance], BGBl. I [Federal Law Gazette I] 3198.

In contrast, the meaning of § 113b of the Telecommunications Act remained obscure even though its wording seemed to be clear cut. At first sight, this provision seemed to regulate the use of the retained data by the competent authorities, but in a very general manner. Whereas Article 1 of the Directive 2006/24/EC envisages the 'investigation, detection and prosecution of *serious* crime'[25] as the purpose for data sharing, § 113b of the Telecommunications Act stated that the transmission of data upon request to the competent authority was possible for the prosecution of criminal offences, the warding off of substantial dangers to public security and the performance of intelligence tasks. However, the scope of the rule becomes less comprehensible as soon as it becomes clear that a transmission of data to the competent authorities could not be based on § 113b of the Telecommunications Act alone. Instead, the fulfilment of certain conditions posed in other legal acts referring to § 113b and expressly allowing for a transmission, was necessary. Such conditions could be found in several security acts such as the challenged § 100g of the Code of Criminal Procedure. This complicated legal technique, namely the interplay between § 113b of the Telecommunications Act and other acts, can (partly) be explained by the federal structure of Germany. It is mainly the *Länder* that have the competence for preventive security law, so it is up to them to create statutes allowing for data transmission.

The main findings of the ruling

The Federal Constitutional Court declared the German data retention rules (§§ 113a and b of the Telecommunications Act) to be null and void as they contravened the right to privacy of telecommunications guaranteed in Article 10 of the German Constitution. Furthermore, § 100g of the Code of Criminal Procedure was also declared to be partly null and void, namely insofar as it allowed the consultation of data retained according to § 113a of the Telecommunications Act. Finally, the Federal Constitutional Court required the destruction of the data detained by the telecommunications providers. In order to reach this decision, the Federal Constitutional Court made several statements that go far beyond this case and are of general interest.

Change of stance towards the admissibility of cases with a European law dimension

To begin with, the Federal Constitutional Court broke new ground concerning the scope of constitutional review of cases which have a European Union law dimension and in which German fundamental rights are allegedly violated. The Court's jurisprudence up to now was determined by the well-known so-called

[25] Emphasis added.

https://doi.org/10.1017/S1574019610300083 Published online by Cambridge University Press

Solange II ruling delivered in 1986. It addressed the question of a possible conflict between EC law and the basic rights laid down in the German Constitution. The Court held in that decision that it would no longer review secondary Community legislation by the standard of the fundamental rights enshrined in the German constitution as long as the European Communities, and in particular the European Court of Justice, generally ensured an effective protection of fundamental rights that is regarded as substantially similar to the protection of fundamental rights required by the German Constitution.[26] Thus, the *Solange II* ruling had repercussions on the admissibility of cases. Constitutional complaints putting forward either the incompatibility of European secondary law or the incompatibility of German law prescribed by European secondary law with basic rights were no longer admissible[27] as long as the plaintiff does not convincingly argue the general level of protection at the Union level has deteriorated.[28] However, it remained possible to bring a constitutional complaint in cases where a directive left discretion to member states in implementing the directive. In such cases, the Federal Constitutional Court was at least able to review whether the implementing law had made use of the remaining discretion in a constitutional manner.[29]

In the case at hand, the Federal Constitutional Court purports to confirm this line of jurisprudence. Yet, it held constitutional complaints to be admissible, even insofar the challenged German provisions were prescribed by binding European law leaving no discretion to the member states. By this step, the German Court accepted the claimants' submission which was based on a three-stage argumentation and aiming at a preliminary ruling. First, the claimants had argued that the Directive was void, because it lacked a legal basis and also infringed European fundamental rights. Second, in order to have the Directive nullified at the European level for those reasons, the complainants had petitioned the Federal Constitutional Court to request a preliminary ruling from the Court of Justice according to Article 267 of the Treaty on the Functioning of the European Union. Third, once the Court of Justice had cleared the road by nullifying the Directive, the Federal Constitutional Court would finally be able to review the German provisions against the standard of the Basic Law. Even though the Federal Constitutional Court did not request a preliminary ruling from the Court of Justice in the end, this line of argumentation sufficed for the Federal Constitutional Court to declare the complaint admissible.

[26] BVerfG 22 Oct. 1986, *BVerfGE* 73, 339 at p. 387; (1987) 3 *CMLR* p. 225 at p. 265.

[27] Last mentioned by BVerfG 13 March 2007, *BVerfGE* 118, 79 at p. 95; BVerfG 11 March 2008, *BVerfGE* 121, 1 at p. 15.

[28] BVerfG 7 June 2000, *BVerfGE* 102, 147 (Bananas).

[29] BVerfG 13 March 2007, *BVerfGE* 118, 79 at p. 96.

On the one hand, this new turn in the Constitutional Court's jurisdiction is to be welcomed, since it will not give rise to further conflict with the Court of Justice and might even give the famous dialogue between constitutional courts further impetus. On the other hand, many future claimants will make use of this new argumentation. For the Federal Constitutional Court, this may result in an enormous workload, because it will now have to deal with the question whether it is at least plausible that secondary legislation contravenes the Treaties.

Extended scope of constitutional review

In the meantime, after the complainants had lodged their constitutional complaints, the Court of Justice handed down its ruling on data retention. For the Federal Constitutional Court, it now became crystal-clear that it could not base a request on a purported lack of legal basis anymore. Yet it could have argued that the Directive infringed European fundamental rights. Instead, the German Court went for a more sophisticated solution, thereby avoiding a request for a preliminary ruling once more and, at the same time, extending its scope of review.

Contrary to the complainants, the Court held, more or less implicitly, that a referral to the Court of Justice was not relevant, because the answer of the Court of Justice could in no way affect the outcome of the case.[30] This result can be understood best by going back to the complainants' arguments, namely their third assumption. They had thought that once the Court of Justice had nullified the Directive, the Federal Constitutional Court would not only be able to review the German implementation against the standard of the German Basic Law, but would also surely quash the German implementation acts for infringing Article 10 of the Basic Law. The Federal Constitutional Court, however, argued that in order to find out whether a preliminary ruling was relevant, the question was whether there really was an infringement of Article 10 of the Basic Law. As mentioned above, the Federal Constitutional Court answered the question in the affirmative. Therefore, at first sight, a referral to the Court of Justice *did* seem necessary. Yet the Federal Constitutional Court introduced a last differentiation: while it was true that the German implementation acts infringed Article 10 of the Basic Law, the infringing part of the implementation acts was not prescribed by the Directive, but originated from the German legislature using its discretion in an unconstitutional manner. Thus, a referral to the Court of Justice was irrelevant.

The surprising element of this ruling is the effect of the above-mentioned construction: actually, the Federal Constitutional Court had only to solve a preliminary question, namely the relevance of a referral to the Court of Justice. But

[30] This corresponds to the CILFIT judgment of the ECJ, 6 Oct. 1982, 283/81, *CILFIT* v. *Ministry of Health*, para. 10.

in order to answer that preliminary question, the Federal Constitutional Court reviewed the whole German implementation by the standard of the German Basic Law, irrespective of the fact that those provisions were partly prescribed by EU law. In sum, via the indirect route of the possible referral, the court succeeded in doing what it had refrained from doing since the *Solange II* ruling:[31] reviewing implementing provisions as a whole by the standard of the Basic Law. It is more than doubtful whether this comprehensive review was the right way to take for the Federal Constitutional Court.

Six month data retention by private telecommunications services, prescribed by European law, as such not incompatible with the privacy of telecommunications

Now that the Federal Constitutional Court had cleared the road for a comprehensive review of the German data retention provisions, it began its review by some remarks on the standard: Article 10 of the Basic Law, the right to privacy of telecommunications.[32] Even though Article 10 is a *lex specialis* to the unwritten and more general right to informational self-determination, the court applied the developed standards and tests of the latter on Article 10 of the Basic Law.[33] As to the area of protection of Article 10, according to the Court, the Article does not only protect the content of the communication, but also the confidentiality of the particular circumstances and the corresponding data, notably the question of whether someone used telecommunications services at all and, if so, when and how often.

To the Court, each of the following steps – namely the collection of data, their retention, matching, evaluation, selection and transmission – as provided for by the challenged provision, are encroachments to Article 10, therefore each demands justification. The Court explained that it made no difference in this context that it was *private* communications services that were collecting and retaining the data instead of the state, since they were in its view mere helpers to carry out the state's duties.

As customary, the Federal Constitutional Court placed the emphasis on the question of the justification of the encroachment. The main test applied is the standard of proportionality. Thus, the encroachments are justified if they serve a legitimate end, if they are appropriate and necessary to achieve this end and if the means used are proportionate to the end.[34] While in the case at hand, the Federal

[31] *See* for a self-assessment of the previous jurisprudence BVerfG 13 March 2007, *BVerfGE* 118, 79 at p. 96.

[32] BVerfG 2 March 2010, *NJW* 2010 p. 833, paras. 188 et seq.

[33] Ibid., para. 191.

[34] Ibid., para. 204.

Constitutional Court easily acknowledged that prosecution, warding off of danger, and intelligence service duties were legitimate ends which justified an encroachment on Article 10 and that data retention was also an appropriate and necessary measure, the issue of proportionality *stricto sensu* remained the crucial question. This is even more so as the Federal Constitutional Court judged the encroachments on Article 10 to be particularly serious ones: virtually all of the telecommunications data were retained without the affected citizens having given occasion for any suspicion. And while it was true that the retention did not cover the content of the communications, the combination of data relating to recipients, dates, time and place of electronic conversations allowed drawing at least content-related conclusions, e.g., about social and political affiliations. Finally, the possibility of the creation of meaningful personality profiles could have an intimidating effect on the citizens.

Nevertheless, there were, according to the Court, several factors that could constitutionally justify the data retention. First, the data were retained by several private providers and not by the state interested in the data.[35] What is more, due to the manifold telecommunications enterprises, the data were dispersed and not available as agglomerate. Also, the data retrieval by the *state* was not possible without occasion, but rather only insofar as legally determined criteria were met. Second, the data retention was limited in time and the citizens could be sure that the data were destroyed after six months, the upper limit of a justifiable retention. Third, the new means of telecommunications facilitated the actions of criminal offenders so that data retention was particularly important for the prosecution and warding-off of dangers.

Remarkably, the Court then adds a *second test of proportionality*. Whereas the court had adopted an isolated perspective before, asking only for the proportionality of the telecommunications traffic data retention, it now took an overall view. Thus, the Court looked at the citizen's overall burden being composed of the telecommunications traffic data retention and possible other (future) data collections. Thus, the Federal Constitutional Court held:

> The data retention relating to electronic communications must not be understood as a step towards a regulation that aims at as comprehensive a storage as possible of all data useful for the prosecution of criminal offences or warding off dangers. Such a regulation would be incompatible with the Constitution from the outset, irrespective of the drafting of the transmission provisions. *For storage of telecommunications traffic data without occasion* [*anlasslos*] *by way of precaution to be constitutionally unobjectionable, this procedure must remain an exception to the rule.* […] The introduction of

[35] The weakness of the argumentation lies in the assumption that private providers are less dangerous than the state as far as the handling of data is concerned.

https://doi.org/10.1017/S1574019610300083 Published online by Cambridge University Press

> the data retention relating to electronic communications must not serve as a model for the creation of more data collections without cause [*anlasslos*] by way of precaution, but forces the regulator, when considering new collection obligations or permissions, to exercise restraint in view of all of the different existing data collections.[36]

This summary approach, as it may be called, fits to recent developments which are discussed under the keyword of 'cumulative encroachment' (*additiver Grundrechtseingriff*):[37] Even if a single encroachment on a right might be constitutional in an isolated perspective, it still may be considered to be unconstitutional in an overall view taking account of the citizen's total burden composed of comparable encroachments. Or, vice versa, an encroachment is constitutional only as long as no more similar restrictions to a basic right are added. Surprisingly, the Court went even further:

> It is part of the constitutional identity of the Federal Republic of Germany that the citizens' enjoyment of freedom may not be totally recorded and registered, and the Federal Republic must endeavour to preserve this in European and international connections. Precautionary storage of telecommunications traffic data also considerably reduces the latitude for further data collections without occasion, including collections by way of European Union law.[38]

So the Court made two extraordinary points of considerable importance in this paragraph. Firstly, it links the absence of overall data registration to Germany's constitutional identity (*Verfassungskern*) and thereby to its own recent *Lisbon* ruling. In that decision, the Court had emphasised exactly this constitutional identity and declared it resistant to any change, even in the connection with the European Union.[39] Thus, secondly, European Union (or national) legislation creating further data collections would most probably be declared to be unconstitutional by the Federal Constitutional Court. This can only be interpreted as a warning by the Court with respect to Germany's voting behaviour on the European Union level. It goes without saying that this is quite a far-reaching step for a court to take.

So far, the Court focused on the parts of the provisions that were prescribed by the Directive 2006/24. Yet, in a last step, still within the test of proportionality, it linked the prescribed parts to the ones leaving discretion to the member states. So the Court predicated the constitutionality of the data storage, belonging to the

[36] Ibid., para. 218; the parts in italics are drawn from the ruling's translation in the Press Release, p. 4, otherwise they are my own translation.

[37] *See* J. Lücke, 'Der additive Grundrechtseingriff sowie das Verbot der übermäßigen Gesamtbelastung des Bürgers', *Deutsches Verwaltungsblatt* (2001) p. 1469 et seq.

[38] BVerfG 2 March 2010, *NJW* 2010 p. 833, para. 218; the translation is drawn from the ruling's translation in the Press Release, p. 4.

[39] BVerfG 30 June 2009, *BVerfGE* 123, 267 at p. 354.

prescribed part, on a legal framework which is appropriate to the encroachment.[40] This last requisite is to be examined in the following.

Requirements for the legislative framework by the standard of proportionality

As was mentioned above,[41] the Federal Constitutional Court had to deal with its own precedent from the *Census Act* case, according to which precautionary data retention without occasion is prohibited if the citizen does not know from the outset for what purpose the data is collected. So, in the ruling which is commented on here, the Federal Constitutional Court had to make clear why the data retention concerning telecommunications did not fall under this prohibition.[42] According to the Court, this could only be the case insofar as a sufficiently sophisticated legal framework with well-defined provisions met the requirements of (1) data security, of (2) special purposes for the use of data, of (3) transparency of data transmission and of (4) legal protection and sanctions.

As for data security, the Federal Constitutional Court explained that the private telecommunications services had little interest in guaranteeing data security themselves. This is why the legislation had not only to prescribe a high degree of data security by means of clear-cut and binding provisions, e.g., stipulating sophisticated encryption, but also to make sure that data security did not lie unsupervised in the hands of the telecommunications providers. Instead, the legislator had to involve a data protection officer, possibly also a regulatory agency.

Of particular importance to the Federal Constitutional Court were the requirements for the use of data:

> The use of such data is proportionate only if it serves particularly high-ranking common interests. This is why a use of data comes into consideration only for paramount tasks of the protection of legal interests, i.e., for the prosecution of crimes that threaten paramount legal interests or for warding off dangers to such an interest.[43]

The Federal Constitutional Court elaborated this point, stating, e.g., that the legislature must not make use of a general clause referring to 'serious crimes'; instead, an exhaustive list of the criminal offences has to be provided that made clear in which cases a data transmission was possible. Similar considerations apply for warding off danger. Here, data retrieval may only be permitted if there is a sufficiently evidenced concrete danger to the life, limb or freedom of a person, to the

[40] BVerfG 2 March 2010, *NJW* 2010 p. 833, paras. 219 et seq.
[41] *See* text to n. 13 *supra*.
[42] BVerfG 2 March 2010, *NJW* 2010 p. 833, paras. 205, 206 and 213.
[43] Ibid., para. 227.

existence or the security of the Federal Government or of a *Land* or to ward off a common danger.

Since provisions on the information of the citizens, concerned by data usage, belong to the basic principles of data protection under the Basic Law, here too, the legislature has to provide for transparency provisions.[44] The use of data has to take place openly as far as possible, e.g., in criminal prosecution, in order to enable the person concerned to seek legal protection. If the open use of data is not feasible, for instance in cases of the intelligence service, the concerned person has to be informed subsequently. Exceptions to the duty of subsequent information require judicial supervision in order to counteract the secrecy.

As to effective legal protection, the Federal Constitutional Court required a judge to order the data retrieval by public authorities as a procedural safeguard[45] in addition to the subsequent judicial review.[46] Finally, proportionality required effective sanctions for the violations of the right to privacy of telecommunications, although the current law might already provide corresponding sanctions.

Voidness of the challenged provisions

It comes as no great surprise that the challenged provisions fell short of all four of the proportionality requirements – data security, qualified purposes, transparency and legal protection. Interestingly, at this point, the Court came back to the link between electronic data retention as such, prescribed by European law, and the rest of the legal framework:[47] because the whole of that framework did not meet the standard of proportionality, the provisions allowing for electronic data retention were also 'contaminated'.[48] Accordingly, providers are no longer allowed to retain data concerning telecommunications, nor the state to retrieve them.

Conclusion

The requirements set up by the Federal Constitutional Court are demanding to such an extent that it takes a great effort to set up a legal framework allowing for data retention and transmission. This is why, as the German Federal Minister of Justice has explained recently, a new bill cannot be expected in the near future.[49]

[44] Ibid., paras. 239 et seq.

[45] Ibid., para. 247.

[46] Ibid., para. 251.

[47] *See* text to n. 40 *supra*.

[48] BVerfG 2 March 2010, *NJW* 2010 p. 833, para. 269.

[49] S. Leutheusser-Schnarrenberger, 'Kein Schnellschuss bei der Vorratsdatenspeicherung', <www.bmj.bund.de/enid/dc9531fe6f0b6934f5f39da9b4a65216,af46eb636f6e5f6964092d0937323434093a095f7472636964092d0937323531/Mediathek/Interviews_1mz.html>, visited 15 Sept. 2010.

https://doi.org/10.1017/S1574019610300083 Published online by Cambridge University Press

From the data protection perspective, the strict prescriptions by the Federal Constitutional Court are to be welcomed. The Court has managed to uphold the data retention required by the European Union without giving up the standards of German data protection. However, this decision is anything but beyond doubt.

One aspect of concern relates to the precision of the Court's prescriptions. Even the complainants were surprised by the rather detailed guidelines given to the legislator.[50] This raises the question of how far prescriptions of a Constitutional Court can possibly go without being accused of acting as a 'pseudo-legislator',[51] particularly as all of the Court's considerations are based on proportionality *stricto sensu*. And this is precisely what the two dissenting judges in this case stress.[52] The same concern can be expressed when it comes to the restraints on the European level. Again the principle of the separation of powers raises the question to what extent a constitutional court is allowed to influence member states' voting behaviour within the European decision-making processes.

The European Commission has already shown understanding for the German situation. On the one hand, this might be due to the fact that the Federal Constitutional Court upheld the constitutionality of the data retention, prescribed by European law, as such. On the other hand, the Commission is in a process of evaluating the Data Retention Directive anyway.[53] Finally, it is an irony of history that the Court of Justice of the European Union, even without the referral by the Federal Constitutional Court, will still have to decide on the Directive once more, because the Irish High Court is going to lodge a request for a preliminary ruling.[54] This time, however, the Court of Justice will have to say something about fundamental rights.

[50] G. Hornung/C. Schnabel, 'Verfassungsrechtlich nicht schlechthin verboten – Das Urteil des Bundesverfassungsgerichts in Sachen Vorratsdatenspeicherung', *Deutsches Verwaltungsblatt* (2010) p. 824 at p. 828.

[51] H.A. Wolff, 'Vorratsdatenspeicherung – Der Gesetzgeber gefangen zwischen Europarecht und Verfassung?, *Neue Zeitschrift für Verwaltungsrecht* (2010) p. 751.

[52] *See* in particular the dissenting vote of Judge Schluckebier, BVerfG 2 March 2010, *NJW* 2010 p. 833 at p. 852, paras. 317, 326 and 327.

[53] *See* the MEMO/10/139 by the European Commission of 20 April 2010, available on <europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/139&format=HTML&aged=0&language=EN&guiLanguage=en>, visited 15 Sept. 2010.

[54] High Court of Ireland, 5 May 2010, *Digital Rights Ireland Ltd* v. *Minister for Communication & Ors*, para. 113. The decision is available on <www.bailii.org/ie/cases/IEHC/2010/H221.html>, visited 15 Sept. 2010.