Case Note

Czech Constitutional Court

Unconstitutionality of the Czech Implementation of the Data Retention Directive; Decision of 22 March 2011, Pl. ÚS 24/10

Pavel Molek*

Introduction

Ever since the famous article by Brandeis (or maybe even since the older, but almost forgotten article by Thomas Cooley)[1] the Western world has regarded '*... the right to privacy [as] the right to one's personality ... the most comprehensive of rights and the right most valued by civilized men*'.[2] As such, the general right to privacy was included in basic instruments of human rights protection, e.g., Article 12 of Universal Declaration of Human Rights, Article 17 of the International Covenant on Civil and Political Rights, Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter: the European Convention) or, finally, Article 7 and 8 of the Charter of Fundamental Rights of the European Union (hereinafter: the EU Charter). The last document responds to very recent challenges to this right by protecting explicitly not only private and family life, home and 'communications' in Article 7, but it goes further and also protects 'personal data'. This new form of privacy which is rising in importance is protected in Article 8, according to which '*[e]veryone has the right to the protection of personal data concerning him or her*'.

All these universal and regional instruments which provide protection of privacy acknowledge, implicitly or explicitly (as does the European Convention), the necessity of its limitation in accordance with the law and by means necessary in a

* Lecturer at Masaryk University, Faculty of Law, Department of Constitutional Law and Political Science, Brno, Czech Republic; Visiting Lecturer at Faculdade de Direito da Universidade Católica Portuguesa, Lisbon, Portugal. I would like to thank for many inspirational comments to James Cockbill, Kristýna Foukalová, Martin Hostinský, Jan Komárek, and Monika Mareková.

[1] T.M.A. Cooley, Treatise on the Law of Torts, or, the Wrongs Which Arise Independent of Contract (Callaghan & Co. 1880).

[2] L. Brandeis, 'The Right to Privacy', 4 *Harvard Law Review* (1890) p. 207, and US Supreme Court 4 June 1928, 277 US 438 (1928), *Olmstead* v. *United States*, p. 277 US 478.

European Constitutional Law Review, 8: 338–353, 2012

doi:10.1017/S157401961200020X

democratic society, in the interests of national security, public safety as well as the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[3] The tension between the first of these aims, i.e., national security, privacy, and especially the confidentiality of private electronic communication and personal data, has become pressing, especially after 11 September 2001. Already in 1978, the European Court of Human Rights acknowledged in *Klass* v. *Germany*[4] that

> democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. The Court has therefore to accept that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime.

The steadily emerging domestic legislation was harmonized at the EU level by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (hereinafter: the Directive).

This analysis will start with a short description of the Directive and several judicial decisions reviewing it on the EU level as well as in several member states. Next, the description of the Czech implementation of the Directive will be addressed. Finally we will analyze the Czech Constitutional Court decision of 22 March 2011, Pl. ÚS 24/10[5] annulling several provisions of the Czech implementation of the Directive.

[3] Art. 8, para. 2 of the European Convention.

[4] ECtHR 6 Sept. 1978, No. 5029/71, *Klass* v. *Germany*, § 48. In this judgment the ECtHR stated limits for state interference with privacy of individual by the surveillance of mail, post, and telecommunications. The same controversy was dealt with in ECtHR 26 March 1987, No. 9248/81, *Leander* v. *Sweden*; ECtHR 24 April 1990, No. 11801/85, ECtHR *Kruslin* v. *France;* or ECtHR 25 March 1998, No. 23224/94, *Kopp* v. *Switzerland*.

[5] English translation became recently accessible on <www.usoud.cz/clanek/pl-24-10>, visited 27 April 2012.

https://doi.org/10.1017/S157401961200020X Published online by Cambridge University Press

Judicial review of the Data Retention Directive

This Directive was adopted on the basis of Article 95 EC Treaty (which is now Article 114 TFEU) with the aim

> to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.[6]

The Directive was justified and inspired, *inter alia*, by the assumed *'obstacles to the internal market for electronic communications, since service providers are faced with different requirements regarding the types of traffic and location data to be retained and the conditions and periods of retention*;'[7] by *'the prevention, investigation, detection and prosecution of criminal offences, in particular organised crime*[8] and even by the terrorist attacks on London on 7 July 2005.[9]

The scope of the Directive remains rather narrow: it relates only to data generated or processed as a consequence of a communication or a communication service (to the traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user) and not to the content of the information communicated.[10] In Article 5, the Directive enumerates 23 categories of data to be collected by network and service providers and in Article 6 it defines the period of their storage as *'not less than six months and not more than two years from the date of the communication'*.

The crucial question of defining the right of access to and the use of data by national authorities is not regulated by the Directive, as that falls outside the scope of former EC law and remains to be regulated by domestic legislative measures,[11] which should define *'procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements'*.[12] Thus, the various national supreme and constitutional courts had the liberty to declare the domestic legal measures unconstitutional without contesting the Directive itself.

[6] Art. 1, para. 1 Directive.
[7] Preamble to the Directive, indent 6.
[8] Ibid., indent 7.
[9] Ibid., indent 10.
[10] Ibid., indent 13 and Art. 1, para. 1.
[11] Preamble to the Directive, indent 25.
[12] Art. 4 Directive.

The Directive was challenged directly at the EU level by Ireland under Article 230 EC Treaty in July 2006.[13] Ireland contested the fact that the Union legislator decided to regulate data retention by a directive on the basis of Article 95 of the EC Treaty and not by a framework decision based on the (former) Articles 31(1)(c) and 34(2)(b) of the EU Treaty as proposed originally by Ireland together with France, Sweden, and the United Kingdom in 2004. This approach taken by the Commission appears to be most likely a tactical one, because the unanimity required at that time in the third pillar of EU law would be difficult to gain; instead, the qualified majority required by Article 95 was achieved despite Slovak and Irish voting against the proposal.[14] A disappointed Ireland argued that the choice of Article 95 of the EC Treaty as the legal basis for the Directive was 'a fundamental error'[15] as neither Article 95 of the EC Treaty (enabling the Council to adopt measures for the approximation of the provisions laid down by law, regulation or administrative action in member states which have as their object the establishment and functioning of the internal market) nor any other provision of the EC Treaty was capable of providing an appropriate legal basis for that directive if the main or predominant objective was to facilitate the investigation, detection, and prosecution of crime, including terrorism. For such an aim, the only legal basis on which these measures may be validly based would be Title VI of the EU Treaty. This view was opposed by the EU institutions, Spain, and the Netherlands and finally by the ECJ. And again, the Directive was 'redeemed' by the limitation of its scope, because the ECJ declared that it was directed essentially at the activities of service providers in the relevant sector of the internal market, and therefore related predominantly to the functioning of the internal market.[16] Furthermore, it responded to measures adopted by several member states: these were meant to impose obligations on service providers concerning the retention of such data, but had significant economic implications for service providers insofar as they may involve substantial investments and operating costs.[17]

After this unsuccessful Irish challenge, the Commission 'struck back' by filling successful actions against four member states for failing to implement the Directive in their domestic law. The ECJ declared that Greece,[18] Ireland,[19] Sweden,[20]

[13] ECJ 10 Feb. 2009, C-301/06, *Ireland* v. *European Parliament and Council of the European Union*.

[14] Press Release 2709th Council Meeting – Justice and Home Affairs, 21 Feb. 2006, Brussels.

[15] Ibid., § 28.

[16] Ibid., §§ 84-85.

[17] Ibid., §§ 67-68.

[18] ECJ 26 Nov. 2009, C-211/09, *European Commission* v. *Hellenic Republic*.

[19] ECJ 26 Nov. 2009, C-202/09, *European Commission* v. *Ireland*.

[20] ECJ 4 Feb. 2010, C-185/09, *European Commission* v. *Kingdom of Sweden*.

and Austria[21] had failed to fulfil their obligations under the Directive. Recently, the Commission filed a subsequent action against Sweden for not complying with the first judgment of the Court.[22]

Once it had been upheld by the ECJ, the Directive was contested before the domestic courts. The first was the Bulgarian Supreme Administrative Court, which annulled Article 5 of the Bulgarian Regulation No. 40 by its decision of 11 December 2008.[23] This Regulation, issued by the State Agency on Information Technologies and Communication and the Ministry of Interior and implementing the Directive, provided the Ministry of the Interior (and security services and other law enforcement bodies too) with the competence of passive access (without court's permission) through a computer terminal to all retained data collected and stored by internet and mobile communication providers. Article 5 of this regulation violated Article 32(1) of the Bulgarian Constitution and Article 8 of the European Convention on Human Rights, because that provision did not set any limitations with regard to the data access by computer terminal and did not provide any guarantees for the protection of the right to privacy.

Similarly, the Romanian act implementing the Directive was declared unconstitutional by the Romanian Constitutional Court in Judgment No. 1258 of 8 October 2009, because of its vagueness and the absence of judicial safeguards against potential abuse.[24]

The Directive was contested and discussed at length by the German Federal Constitutional Court in its judgment of 2 March 2010.[25] The German Court had to solve around 35 000 individual constitutional complaints[26] based on alleged violation of, *inter alia*, Article 10 (*Fernmeldegeheimnis* – secrecy of telecommunications) and of Article 12 (free choice and performance of occupation – *Berufsfreiheit*) of the German Basic Law (*Grundgesetz*).[27] These violations were alleged

[21] ECJ 29 July 2010, C-189/09, *European Commission* v. *Republic of Austria*.

[22] Case C-270/11, *European Commission* v. *Kingdom of Sweden.*

[23] 'Bulgarian Court annuls a vague article of the data retention law', <www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention>, visited 9 July 2011.

[24] Quoted by the Czech Constitutional Court in § 52 of commented decision. English translation available at <www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf>, visited 9 July 2011.

[25] 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, English shortened version accessible on <www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011en.html>, visited 9 July 2011. *See* the case note by Kaiser, 'German Data Retention Provisions Unconstitutional in Their Present Form'; Decision of 2 March 2010, *NJW* 2010, p. 833, *EuConst* (2010), p. 503-517.

[26] J. Herczeg, 'Ústavněprávní limity monitoringu telekomunikačního provozu: konflikt mezi bezpečností a svobodou' [Constitutional limits of monitoring telecommunication: conflict between security and freedom], 5 *Bulletin advokacie* (2010), p. 22 at p. 31.

[27] German version accessible on <www.gesetze-im-internet.de/gg/index.html>, English translation accessible on <www.gesetze-im-internet.de/englisch_gg/index.html>, last visited 20 Dec. 2011.

to have been made by Article 113a (imposing a duty to store traffic data on providers of publicly accessible telecommunications services) and Article 113b (governing the possible purposes for which these data may be used) of the Telecommunications Act (*Telekommunikationsgesetz*) and by Article 100g (specifying the terms of the direct use of stored data for criminal prosecution) of the Code of Criminal Procedure (*Strafprozessordnung*).

The German Federal Constitutional Court (hereinafter the German Court) considered these norms from the perspective of the right to secrecy of telecommunications and, just as the aforementioned domestic jurisdictions, did not address the question of validity of the Directive and criticized only those measures that are left by the Directive for the member states. The Directive provisions are essentially limited to the duty of storage and its extent, and do not govern the access to the data or the use of the data by the member states' authorities. Therefore, the Directive could be implemented into German law without violating fundamental rights laid down in the *Grundgesetz*. The argument of violation of occupational freedom, based on the assertion that the costs of the data storage disproportionately disadvantaged the freedom of occupation of telecommunications service providers, was rejected by the German Court, because the duty of storage is not typically excessively burdensome for the service providers. Conversely, regarding the secrecy of telecommunications, the German Court stated that

> such storage constitutes a particularly serious encroachment with an effect broader than anything in the legal system to date. Even though the storage does not extend to the contents of the communications, these data may be used to draw content-related conclusions that extend into the users' private sphere. In combination, the recipients, dates, time and place of telephone conversations, if they are observed over a long period of time, permit detailed information to be obtained on social or political affiliations and on personal preferences, inclinations and weaknesses. Depending on the use of the telecommunication, such storage can make it possible to create meaningful personality profiles of virtually all citizens and track their movements. It also increases the risk of citizens to be exposed to further investigations without themselves having given occasion for this.[28]

Dissenting judge Schluckebier contested this attitude, emphasising the fact that the storage did not extend to the contents of the telecommunications.

Subsequently, the German Court made a distinction between direct and indirect use and subjected each of them to the proportionality test. As regards the direct use, i.e. use for prosecution of crimes, it should be permitted only if there

[28] Quoted from shortened English translation at <www.btg-bestellservice.de/pdf/80201000.pdf>, visited 9 July 2011. The complete German version accessible at <www.bundesverfassungsgericht.de/entscheidungen.html>, visited 20 Dec. 2011.

is a sufficiently proved concrete danger to the life, limb or freedom of a person or to the existence or the security of the state; besides, persons to whom a request for data retrieval directly applies have to be informed, in principle, at least subsequently. None of these requirements was met, because the *Strafprozessordnung* accepted every criminal offence committed by means of telecommunications, regardless of its seriousness, as a possible trigger for data retrieval, even without the knowledge of the person affected. As regards indirect use, i.e., the use of data stored by way of precaution, even here it must be ensured that the information is not obtained at random, but only on the basis of a sufficient initial suspicion or a concrete danger and the persons affected must be informed – at least *ex post* – when such information is obtained. However, no such limitation of purpose and no duty of notification were assured by the *Telekommunikationsgesetz*. Last but not least, the German Court was highly critical of the security of this 'data pool open to manifold and unlimited uses' and of the absence of judicial protection of individuals affected by storage of these data. Therefore, those three contested provisions were held to be unconstitutional. Furthermore, the Court required the destruction of the data detained by the telecommunications providers.

Lastly, the Supreme Court of Cyprus decided on 1 February 2011[29] that some of the provisions of Law 183 (I)/2007 (Retention of Telecommunication Data for Purposes of Investigation of Serious Criminal Offences Law of 2007) violated Article 15 (right to privacy) and Article 17 (confidentiality of communications) of the Cypriot Constitution. By this decision, the Court annulled three court orders for the disclosure of telecommunications data issued by several Cypriot district courts at the request of police investigating serious crimes. The Court was well aware of the fact that the contested Law 183 (I)/2007 implemented the Directive; nonetheless, the Court did not allow this to stand in the way of its own judicial review, because the articles in question went beyond the provisions of the Directive, which does not address the issue of access to the retained data.

Czech implementation of the Directive

The Czech Republic recently joined the aforementioned group of states. It may not be a coincidence that these states, with the exception of Cyprus, have had recent experience with totalitarian regimes that used different forms of electronic surveillance. This experience remains still deep in the minds of the peoples of these countries (as witnessed by its artistic reflection in famous movies, like the

[29] Information available on <www.edri.org/edrigram/number9.3/data-retention-un-lawful-cyprus>, visited 9 July 2011.

Czechoslovakian *Ucho* [The Ear] 1969, or the German *Das Leben der Anderen* 2006).[30]

In the Czech Republic, the Directive was implemented by an amendment no. 247/2008 Coll. to Electronic Communications Act No. 127/2005 Coll. (*zákon č. 127/2005 Sb., o elektronických komunikacích*, hereinafter: the Act) in 2008. In 2005, the Act was supplemented by Regulation No. 485/2005 Coll., on the scope of traffic and location data, period of its storage, and form and method of its communication to national authorities competent for its usage (*vyhláška č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání,* hereinafter: the Regulation). This Regulation, based on Article 97(4) of the Act, contained the concrete technical description of traffic and location data and technical details of its storage and of its communication to national authorities.

The most problematic provision was contained in Article 97(3) and (4) of the Act, obliging the telecommunication service providers to store traffic and location data, including missed calls, for a period of at least 6 months and not longer than 12 months and to provide this data without delay to competent national authorities. Although several details were modified by the amendment No. 247/2008 Coll., 90% of the Directive[31] was already implemented by the Czech legislature in the original version of the Act as early as in March 2005, i.e. even before the final version of the Directive was adopted in March 2006. The resulting implementation after 2008 went beyond the Directive requirements, particularly in requesting the storage of information about amount of data transferred via the internet, about the use of encryption, about sending SMS from internet portals, and much more.

The Act was highly criticized from the very beginning of its application,[32] especially because of its abuse by Czech police. According to the 2009 Report on Data Retention,[33] Czech police made the most requests for telecommunication data in the whole EU in 2008, including 98 000 requests regarding mobile phones. The Act was not the only target of criticism; criticism was also directed at Article 88a of the Code of Criminal Procedure No. 141/1961 Coll. (*zákon č. 141/1961 Sb., o trestním řízení soudním*), according to which the conditions for a request for traffic and location data were less demanding than the conditions for a request for

[30] *See* the academic reflection from legal perspective in K. Hutchens et al., 'The Laws of Others: A Jurisprudential Reflection on The Lives of Others', 7 *German Law Journal* (2009) p. 951.

[31] According to the Report of the Data Retention Conference, 'Towards the Evaluation of the Data Retention Directive', Brussels, 14 May 2009, p. 18, <ec.europa.eu/home-affairs/doc_centre/police/docs/meeting_report_09_07_14_en.pdf>, visited 9 July 2011.

[32] For a complex critique *see* Herczeg, *supra* n. 27, p. 31.

[33] Report from Conference, 'Towards the Evaluation of the Data Retention Directive', *supra* n. 31.

traditional monitoring of telecommunication set out in Article 88 of the Code of Criminal Procedure. To be more precise, both articles demand authorization by a president of a court chamber or by a judge, but Article 88 contains further conditions (concrete reasoning for the authorization, limited period for monitoring that shall not exceed four months) that are not contained in Article 88a.

This criticism resulted in the commented decision of the Czech Constitutional Court. The Czech Constitutional Court was not a *tabula rasa* when it was called to review the Act. It was bound by a considerable number of its previous judgments regarding the right to privacy (see i.e. the judgment of 27 August 2001, IV. ÚS 78/01, according to which the right to secrecy of telecommunications covers not only the content of the transferred messages, but the data regarding dialled numbers, and time and duration of the call as well).

The decision

The Czech implementation of the Directive, more concretely Article 97(3) and (4) of the Act and the Regulation were contested in March 2010 in an abstract constitutional review procedure, although the 'German way' of individual constitutional complaints of individuals affected by storage of data was also available.[34] A group of 51 MPs submitted a proposal for annulment, contesting the Act *in abstracto*, not its application by state organs. This fact was criticized by the Czech Constitutional Court at the very outset of the decision of 22 March 2011. Several of these MPs were members of political parties forming the government coalition that adopted the Act and had even voted in favour of the Act in the Parliament. The Czech Constitutional Court labelled this as '(ab)use' of the right of a group of (at least 41)[35] MPs to file a proposal for annulling an act by the Czech Constitutional Court, because this procedure should be a means of protection of a parliamentary minority, not of a parliamentary majority which should instead amend the law in the Parliament if the same majority finds it to be unconstitutional.[36]

The applicants asserted that the Act violated the right to physical and moral integrity (Article 7 para. 1 of the Charter of Fundamental Rights and Freedoms – *Listina základních práv a svobod*, hereinafter: the Charter), the right to privacy (Article 10 para. 2 and 3 of the Charter) and secrecy of telecommunications (Ar-

[34] Herczeg, *supra* n. 26, p. 31.

[35] According to § 64 para. 1 lit. b of Constitutional Court Act No. 182/1993 Col. (*zákon č. 182/1993 Sb., o Ústavním soudu*). For description of these procedures, *see* J. Filip et al., 'Governance in the Czech Republic', in N. Chronowski et al. (eds.), *Governmental Systems of Central and Eastern European States* (Oficyna a Wolters Kluwer Business 2011) p. 166 at p. 224.

[36] Pl. ÚS 24/10, § 2.

ticle 13 of the Charter). They argued that the infringement of these rights was disproportionate because the police had not proven how the monitoring of virtually the whole population, including the vast majority of innocent individuals (the argument of *presumptio boni viri*), contributed to fighting criminality.[37] They also criticized the absence of safeguards against the abuse of these data by national authorities, employees of service providers or hackers,[38] and against their storage by private providers of telecommunication services, not by the state.[39] Finally, the applicants stressed that the stored data reflected communication and patterns of movement of individuals.[40]

The applicants, being aware that the contested Act and Regulation were implemented by the Directive, proposed to file a preliminary ruling concerning the validity of the Directive to the Court of Justice of the European Union.[41] This was rejected by the Czech Constitutional Court. The Directive supposedly left enough space for a constitutionally conforming implementation, because it only imposed the duty to store the data, but did not detail the scope of this duty. The legislator had to implement the Directive while respecting both the aim of the Directive and the constitutional standard, as defined in the Czech Constitution and the Charter and interpreted by the Czech Constitutional Court.[42]

The Czech Constitutional Court began the substantive part of its decision by setting the right to privacy in the context of the general principles of the Czech Constitution, political liberalism (quoting Brandeis) and Western culture, pointing out that this right was not mentioned expressly in many national human rights bills as late as the middle of the 20th century (noting its absence in the *Grundgesetz*, in the French and the Austrian Constitutions and many others).[43] It included the specific aspect of informational self-determination within the right to privacy, referring to previous Czech[44] and German[45] as well as ECtHR case-law,[46] and to

[37] Ibid., §§ 8-9.

[38] Ibid., § 10.

[39] Ibid., § 5.

[40] Ibid., § 7.

[41] Despite the fact that the applicants filed their proposal in March 2010, they referred to 'Article 234 of EC Treaty' and generally used former pre-Lisbon terminology.

[42] Ibid., § 25.

[43] Ibid., § 26-28.

[44] Czech Constitutional Court judgments 17 July 2007, IV. ÚS 23/05; 1 Dec. 2008, I. ÚS 705/06 and others.

[45] German Federal Constitutional Court judgments 15 Dec. 1983, BVerfGE 65, 1 (*Volkszählungsurteil*); 4 April 2006, BVerfGE 115, 320 (*Rasterfahndungurteil II*); 27 July 2005, BVerfGE 113, 348 (*Vorbeugende Telekommunikationsüberwachung*); or 27 Feb. 2008, BVerfGE 120, 274 (*Grundrecht auf Computerschutz*).

[46] ECtHR 2 Aug. 1984, No. 8691/79, *Malone* v. *United Kingdom*; ECtHR 16 Dec. 1992, No. 13710/88, *Niemitz* v. *Germany*; ECtHR 25 Sept. 2001, No. 44787/98, *P. G. and J. H.* v. *United Kingdom*; ECtHR [GC] 16 Feb. 2000, No. 27798/95, *Amman* v. *Switzerland*; ECtHR 4 Dec.

the previous decisions of European domestic courts concerning the Directive implementations. The limitation of the right to informational self-determination is generally possible for the prosecution of crimes, but only in accordance with the law and in a proportional manner, as regards foreseeability for individuals and safeguards – especially judicial safeguards – for affected individuals.[47] The Court stated that it could not classify the safeguards provided by the Act as *'sufficient, unambiguous, detailed and appropriated.'*[48]

Why did the contested Act and Regulation not fulfil these requirements? As said before, the Regulation and the main part of the Act were adopted before the Directive and went far beyond the requirements of the Directive[49] by stipulating that the service providers monitor and store information about the amount of data transferred via Internet connections and e-mail communication, information about usage of encryption, information about the method and status of other requests for telecommunication services, about SMS sent from the Internet, about identification of pre-paid SIM cards, public phone booths, numbers of top-up coupons and about connections between mobile phones and inserted SIM cards.[50] As the German Federal Constitutional Court had, the Czech Constitutional Court emphasized that not only from the content of communication, but also from the stored data, one can induce many details about the social contacts of an individual. The intensity of the infringement of right to privacy is even more serious if a legal regulation orders the storage of data of a vast number of individuals for preventive purposes. The Czech Constitutional Court criticized the vagueness of the duty of providers of telecommunication services to provide 'competent bodies' with the data they store. The Court could only 'presume' that these competent bodies should be criminal prosecution and secret services agencies, because this was not stated explicitly in the Act; such a vague legal regulation did not comply with certainty and clarity requirements.[51]

Furthermore, the aim of providing 'competent bodies' with these data was vague, too. In other words, not only the answer to 'how' the data should be provided, but even the answer to 'why' it was not concrete enough. Whereas Article

2008, No. 30562/04 and 30566/04, *S. and* Marper v. *United Kingdom*; ECtHR 4 May 2000, No. 28341/95, *Rotaru* v. *Romania*; ECtHR 6 Sept. 1978, No. 5029/71, *Klass* v. *Germany*; ECtHR 26 March 1987, No. 9248/81, *Leander* v. *Sweden*; ECtHR 24 April 1990, No. 11801/85, *Kruslin* v. *France*; ECtHR 25 March 1998, No. 23224/94, *Kopp* v. *Switzerland*; ECtHR 29 June 2006, No. 54934/00, *Weber and Saravia* v. *Germany*; or ECtHR 1 July 2008, No. 58243/00, *Liberty and others* v. *United Kingdom*.

[47] Pl. ÚS 24/10, §§ 36-40.

[48] Ibid., § 51.

[49] Ibid., § 41.

[50] Ibid., § 43.

[51] Ibid., § 46.

https://doi.org/10.1017/S157401961200020X Published online by Cambridge University Press

1(1) of the Directive mentions 'that the data are available for the purpose of the investigation, detection and prosecution of serious crime', the Czech Code of Criminal Procedure contained no such limitation of crimes. Furthermore, there was no obligation to inform the affected individuals – not even *ex post* – about the fact that they were monitored. Since there are less intrusive means available to achieve the legitimate aim of prosecuting crime, the Czech Constitutional Court ruled the Czech measures to be not proportional.[52] The legislator should draw inspiration from Article 88 of the Code of Criminal Procedure and define more precisely for which crimes and under what conditions the monitoring of data stored is justifiable. The Court remarked that judicial control of this monitoring through the approval of a judge in this respect is not a sufficient safeguard and referred to the enormous amount of decisions approving the monitoring[53] (in addition, two months after the Court's decision, an investigative newspaper found out that even the Court's Chief Justice Pavel Rychetský had been monitored in this way, unbeknownst to the judge who had approved the monitoring).[54]

Finally, the Czech Constitutional Court expressed doubts whether data services providers, i.e., private subjects, are the proper subjects to be competent to collect all these valuable data.[55] By this critique, it departed from the argumentation of the German Federal Court, which acclaimed the engagement of private data service providers in data retention to be a positive development. In this point, the Czech Constitutional Court implicitly shared the opinion of Anna-Bettina Kaiser, who criticized 'the assumption that private providers are less dangerous than the state as far as the handling of data is concerned.'[56] Both positions have their advantages and disadvantages. The collection of data by private providers is problematic in view of their responsibility and accountability. Collection by a state agency may solve these problems, but that would imply a problem of the availability of the data as an agglomerate. It is easier to abuse such an agglomerate of data than disperse collections of data collected by manifold telecommunications enterprises. Therefore, neither of these solutions is entirely satisfactory.

The Czech Constitutional Court also criticized the absence of precise procedures for the destruction of stored data; even the period of its storage was set only vaguely by the maximum period of 12 months and the minimum period of 6 months.[57] Furthermore, there were no effective safeguards regarding the secu-

[52] Ibid., § 47.

[53] Ibid., § 48-49.

[54] ČTK, 'President says phone calls statements case is scandalous', Prague Daily Monitor, 21 June 2011, <praguemonitor.com/2011/06/21/president-says-phone-calls-statements-case-scandalous>, visited 12 July 2011.

[55] Pl. ÚS 24/10, § 57.

[56] Kaiser, *supra* n. 25, p. 513.

[57] Pl. ÚS 24/10, § 51.

rity of stored data against access by unauthorized third parties and other dangers. Such safeguards, including a clearly defined responsibility regime or sanctions, are even more necessary in an era when the public and private spheres are increasingly intertwined.[58] The Court considered the supervision of the Office for Personal Data Protection (*Úřad na ochranu osobních údajů*) to be inadequate and insufficient, because this office cannot be engaged by affected individuals, thereby leaving them with no reasonable remedies.

For these reasons, the Czech Constitutional Court annulled Article 97(3) and (4) of the Act and the Regulation. Thereby, it implicitly ordered not only a halt to the collection and storing of traffic and location data, but also the destruction of the data stored up till now.

The Czech Constitutional Court also criticized Article 88a of the Code of Criminal Procedure.[59] But as this provision was not contested in the application and the Czech Constitutional Court does not rule *ultra petitum,* this critique was technically *obiter*, although the Court did invite 'the legislature to consider amending' Article 88a of the Code of Criminal Procedure to bring it into conformity with the constitutional order.

This invitation had only recently been accepted by one of the Czech district courts, which proposed annulment of Article 88a of the Code of Criminal Procedure in a concrete review of constitutionality. The Czech Constitutional Court therefore annulled this provision in its decision of 20 December 2011, Pl. ÚS 24/11, because such a limitation of the right to informational self-determination did not pass the second step of the proportionality test (i.e. necessity).

In a final consideration, the Czech Constitutional Court expressed its understanding for the necessity of modernising the means of fighting against modern forms of criminality. Nevertheless, it added that the statistics show that the storage of traffic and location data is not very effective in this regard.

***

Obviously, the decision of 22 March 2011 is inspired by the aforementioned decision of the German Constitutional Court. The Czech Constitutional Court was precluded from following the steps of the German Court even more precisely, mainly by the fact that the applicants had not been inspired by the latter's decision and had not contested Article 88a of the Code of Criminal Procedure. Another reason was the different regulation of storage limits in German and Czech law.

The decision of 22 March 2011 is interesting not only for the relationship between data retention and right to privacy, but also for the relationship between

[58] Ibid., § 50.
[59] Ibid., § 54.

the Court of Justice and the Czech Constitutional Court (and other national constitutional courts). It is difficult to overlook that the Act and Regulation were only 'red herring' targets and that the majority of the Court's critical comments were meant indirectly for the Directive. A good example is the Court's manifest doubts as to whether general and preventive retention of traffic and location data is an effective tool for fighting serious crimes.[60] Another example can be found in its critique of the fact that the data is collected by private service providers,[61] which is prescribed directly by Article 3 of the Directive and acclaimed by the German Court. In contrast, the German Court warned that overall collection of data would lead to a potential threat to the constitutional identity of Germany.[62] Although this notion is not unfamiliar with the Czech Constitutional Court, it is not mentioned in this case.

The fact that the German, Bulgarian, Romanian and Cypriot implementation of the Directive was criticized by their supreme or constitutional courts[63] can be explained in two ways: either all these national legislators had a legislative 'epidemic' of bad national implementation, or the real problem lies in the Directive. Also, in the light of the many critical voices against the Directive,[64] the second explanation is much more probable. In such a situation, it is hypocritical to annul only the implementation of the Directive and not to contest directly the Directive by submitting a reference for preliminary ruling to the Court of Justice. However, one understands that the Czech Constitutional Court, as well as the other abovementioned courts, did not want to engage in an already lost battle, taking into account the European Court's decision in case C-301/06, *Ireland* v. *European Parliament and Council of the European Union*. Furthermore, the constitutional courts are generally not enthusiastic about requesting preliminary rulings.[65] Nevertheless, the Czech Constitutional Court's 'self-restraint in asking' seems pharisaic, especially given the same Court's critique on Czech ordinary courts' refusal to submit a reference for a preliminary ruling if none of the parties asks for it.[66] In this case, however, the applicants explicitly asked the Constitutional Court to file a preliminary ruling. Did the Court really have no doubts regarding the interpretation of the Directive?

[60] Ibid., § 56.
[61] Ibid., § 57.
[62] Kaiser, *supra* n. 25, p. 514.
[63] Pl. ÚS 24/10, § 52.
[64] Ibid., § 55.
[65] One of the recent exemptions is the reference for a preliminary ruling from the Spanish *Tribunal Constitucional*, lodged on 28 July 2011 and pending before the Court of Justice as Case C-399/11 (notice published in *OJ* C 290, 1 Oct. 2011).
[66] Czech Constitutional Court judgment 8 Jan. 2009, II. ÚS 1009/08, accessible online at: <www.usoud.cz/view/2-1009-08>, visited 30 Dec. 2011.

This attitude of the Czech and the other constitutional courts leaves the most important question unanswered: does the Directive leave any real space for an implementation compatible with the protection of the right to privacy? Is the space wide enough for any 'margin of appreciation' of the legislator, or is it so narrow, that the Czech Constitutional Court (as well as German Federal Constitutional Court) actually acted as a 'pseudo-legislator'[67] defining the only possible legislative solution itself? By annulling the provisions of the Act and the Regulation instead of sending a preliminary reference to the Court of Justice, the Czech Constitutional Court closed one 'gate' for answering these questions.

Perhaps the Court of Justice will be able to answer these questions in an infringement procedure. Now that the Czech Constitutional Court has annulled the Czech implementation measures by the commented decision, the Czech Republic has in fact joined Greece, Ireland, Sweden, and Austria in not implementing the Directive in time. In other words, by closing the gate of Article 267 TFEU, the Czech Constitutional Court opened the much less comfortable gate of Article 258 TFEU. If the Commission starts such a procedure, a possible defence is the argument that it is impossible to implement the Directive in a way compatible with the right to privacy. Hopefully, the Czech government will not feel precluded from taking this stance by the Czech Constitutional Court's hypocritical statement that the problem lies in the domestic implementation, and not in the Directive itself.

Conclusion

If one looks only at the operative parts of the commented decision and those of other member state courts, one senses some sort of 'civil disobedience' toward the Union amongst member state supreme and constitutional courts. After Ireland had not succeeded in a direct action to the Court of Justice, the Bulgarian, Romanian, Cypriot, German and Czech supreme and constitutional courts, perhaps followed by the courts in Poland and Hungary (where the implementation of the Directive has been contested recently[68]) have started to break it up from below.[69]

This is in a sense not true. All of these courts, with the exception of the Romanian Constitutional Court, which was directly critical of the Directive, were very

[67] The same suspicion relates to the German Federal Constitutional Court too, *see* Kaiser, *supra* n. 25, p. 517.

[68] J. Durica, 'Právo na soukromí versus posílení bezpečnosti: směrnice o uchovávání údajů o telekomunikačním provozu v nálezech ústavních soudů členských států EU' [Right to privacy versus protection of safety: Data Retention Directive in decisions of constitutional courts of EU member states], 6 *Bulletin advokacie* (2011), p. 19, at p. 20.

[69] As regards the German Federal Constitutional Court decision, the same seems surprising for Kaiser, *supra* n. 25, p. 511.

careful not to contest the Directive itself. They focused their explicit criticism only on those aspects of the domestic implementing legislation that went beyond the Directive requirements. They put the blame on the domestic legislators who had allegedly abused their power given by the Directive and had added unnecessary provisions – which violated the right to privacy in the name of domestic security – to the necessary implementing provisions. By giving the domestic legislators a second chance to regulate issues outside the scope of the Directive, these courts remained loyal to the EU legal system, at least formally.

At the same time, the question remains whether the problems really lay beyond the scope of the Directive and whether domestic legislators still have some 'margin of appreciation' between the Scylla of the Directive and the Charybdis of domestic constitutions. This was the criticism of the dissenting German judge Schluckebier. He pointed out, among other things, that the German Court found that the storage duration of six months was the upper limit, while that was precisely the minimum period called for by the Directive.

Where, then, is the room for a margin of appreciation of domestic legislators? We will see.

https://doi.org/10.1017/S157401961200020X Published online by Cambridge University Press