DIRECTIVE ON THE RETENTION OF DATA ON ELECTRONIC COMMUNICATION IN THE RULINGS OF THE CONSTITUTIONAL COURTS OF EU MEMBER STATES AND EFFORTS FOR ITS RENEWED IMPLEMENTATION

Jan Durica*

Abstract: *The Directive on the retention of data related to electronic communications has generated doubts with regard to its compliance with the right to protection of privacy. This right is embodied in the constitutions of EU member states, in the European Convention on the Protection of Human Rights and Fundamental Freedoms and in the EU Charter of Fundamental Rights. The national implementation of this Directive was quickly contested in some EU member states before the local constitutional courts. The constitutional courts in Germany, Romania and in the Czech Republic repealed the implementation of the Directive precisely because of this disparity with the right to protection of privacy. In their new legislation on retention of data on telecommunication operations, these states are trying to reconcile the conditions set out in the rulings of the constitutional courts with the obligation to implement this Directive.*

Keywords: *retention of data on telecommunications operations, European Union, implementation, constitutional court, right to privacy.*

1. INTRODUCTION

Human rights and fundamental freedoms have been subject to protection by international conventions since the end of the Second World War. Protection of these rights is based on constitutional traditions common to the democratic states of Europe which are signatories to the European Convention on the Protection of Human Rights and Fundamental Freedoms. The right to protection and respect for one's privacy is one of the rights guaranteed by these constitutions and international conventions. In providing it, both national constitutional courts and the European Court of Human Rights have developed a broad set of case law permitting the protection of this right, without having to change to the original norms in the face of continuing technological progress and the overall development of social relations and communications methods.

However, continuing technological progress currently facilitates committing serious crimes, including acts of international terrorism, for organised crime groups and makes it easier for them to avoid prosecution by the appropriate authorities. For this reason certain limitation of the right to privacy has occurred, in particular following the increase of terrorist attacks in North America and Europe after the turn of the century, in legislation at both national and supra-national level. The aim is to strengthen internal security and provide the security agencies with more effective means and sources of information in the struggle against the most serious forms of organised crime.

Establishing the required equilibrium between the interest of society in stronger security and the individual's right to have his privacy respected is a task precisely for national

* Mgr. Ing. Jan Durica, Office of the Government of the Czech Republic

constitutional courts and the courts of international organisations, which in the case of Europe are the European Court of Human Rights and the Court of Justice of the European Union.

Directive 2006/24/EC on the retention of data on electronic communications is an example of a norm which, in the interest of providing more effective means in the struggle with serious crime, charges EU Member States with an obligation to retain certain data on all users of telecommunications services, and for this reason is the object of criticism for its disproportionate intrusion into fundamental rights of the individual.

1.1 Contents of the Directive and the circumstances surrounding its adoption

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 (the Directive) was adopted in an atmosphere of fear of terrorist attacks following the events of 11. September 2001 in the USA, and also at a time when the terrorist attacks on its own territory - in Madrid (2004) and London (2005) - were still vivid in European minds. The actual negotiation of the directive was accompanied by arguments over its legal basis. The legal basis for adoption of this Directive was Art. 95 of the Treaty on the Establishment of the European Community (TEEC)[1], but of course this legal basis was not accepted by all member states without disagreement. The choice of legal basis was first called into doubt by Ireland during the negotiation of the draft, and subsequently became the subject of a complaint brought by it for invalidity, reasoning that the focus of measures based on Art. 95 of the TEEC must be the harmonisation of internal legal regulations with the aim of improved functioning of the internal market, whereas the only aim of the contested Directive was to facilitate investigation, detection and prosecution of crime. Nevertheless, the Court of Justice of the EU rejected the complaint from Ireland.[2]

In an explanatory memorandum[3] to the draft Directive it is stated that access to operational and localisation data is important for reasons connected with applying the law and assuring security, for example for the prevention, investigation, detection and prosecution of serious crimes such as terrorism and organised crime. According to the explanatory memorandum the fact that, as a result of changes to business models (flat-rate tariffs, pre-paid calls, as well as free services), not all operators need necessarily retain operational data for invoicing purposes to the same extent as before significantly hampers the provision of security, and indeed makes communication between criminals easier. This brought about the urgent need to adopt unified legislation for the whole of the European Union. Moreover internal legislation either already existed or was in preparation in some Member States at this time. According to the explanatory note, differences in member states' legal and technical regulations concerning the retention of

[1] Following the entry into force of the Treaty of Lisbon, harmonisation of internal legal regulations with the aim of improved functioning of the internal market is covered by Art. 114 of the Treaty on the Functioning of the EU.

[2] Verdict in case C-301/06.

[3] The explanatory memorandum is part of the draft Directive published under number Com (2005) 438 in its final wording dated 21. 9. 2005.

operational data represented a barrier in the internal market for electronic communications, since service providers came up against varying requirements as far as what data was to be retained and under what circumstances[4]. Justification for the use of this legal base which has less complicated legislative procedure than a framework decision in the field of police and judicial cooperation can seem to be purpose-built. However this legal base has been used quite widely and a number of directives were adopted using this provision as a legal basis in the area ranging from intellectual property, consumer protection, product safety, technical norms to telecommunication liberalization, but personal data protection as well[5].

Even at the time the draft was submitted it was clear that there was a possible clash of the proposed legislation with the constitutionally guaranteed protection of the right to privacy. However, according to the explanatory memorandum the draft was in line with Community law, including the EU Charter of Fundamental Rights, since limitations on protected rights to privacy and the protection of personal data are appropriate and necessary for achieving generally acknowledged goals in the prevention and fight against crime and terrorism. In addition, according to the explanatory memorandum, the draft limits its impact on the private life of citizens mainly by unambiguously stating for which purposes the retained date may be used, by limiting the data categories which may be retained, and finally by establishing a retention period for the data.

The Directive has by and large a short text, with seventeen articles . The aim of the legislation is to secure access to certain, further defined data for the purposes of investigating, detecting and prosecuting serious crimes (Art. 1). But the actual definition of these crimes is left to national legislation which can lead (and has led) to relatively great differences in the possible use of retained data by state authorities in individual Member States. Similarly the circle of state bodies and the conditions for access to retained data are defined very vaguely, whereby "data are supplied only to relevant domestic bodies in specific cases and in accordance with domestic regulations" (Art. 4). The obligation to retain data also applies to unsuccessful dialling attempts, but the Directive, on the contrary, does not require the retention of data related to unconnected calls (Art. 3 (2)). To obtain access to the data the requirement is based on observing the principle of reasonableness and necessity and also observing the relevant provisions of EU law and the European Convention on the Protection of Human Rights and Fundamental Freedoms (Art. 4). It should be, however, emphasised that this limitation focuses only on the use of data already gathered, whereas (as we shall see) the constitutional complaints within Member States object to the illegality of the very gathering of such data.

The Directive (Art. 5) names a total of 23 different data types, which it groups as follows: (1) data needed to search out and identify the source of a communication, (2) data needed to identify the addressee of a communication, (3) to determine the date, time and duration of a communication, (4) to determine the kind of a communication, (5) to identify the communications equipment of the users, and (6) data needed to determine the position

[4] Ibid.

[5] SYLLOVÁ, J. – PÍTROVÁ, L. – PALDUSOVÁ, H. a kol. *Lisabonská smlouva. Komentář.* Praha: C. H. Beck, 2010, pp. 497–498.

of a mobile communications device. There is also an explicit ban on retaining data which reveals the contents of a communication based on this Directive.

The retention period (set out in Art. 6) is a minimum of 6 months and a maximum of 24 months from the date of the communication. This represents a degree of freedom in Member States' implementation of the Directive which does not correspond to the declared efforts in harmonisation. Moreover, the maximum period may be extended by a Member State (on the basis of Art. 12) if the state in question is in a "special situation justifying the extension of the maximum period". According to the Directive, data are not to be retained centrally but always by the individual providers, which prevents state bodies from having instant access to all data Nevertheless, in accordance with Art. 8 data are to be retained in such a way as to be provided immediately to the relevant authorities at their request.

1.2 Rulings of the constitutional courts of EU member states

The implementation of the Directive and its subsequent application has raised doubts in a number of Member States on the compatibility of such data gathering with the constitutionally guaranteed rights to protection of privacy and protection of personal data. These doubts then led to a number of cases before national constitutional courts, aimed in general at the manner of implementation of the Directive, and not at the Directive itself. Examples are cases before the German, Romanian and Czech constitutional courts, to which the following analysis is devoted, but it should also be mentioned that national transpositions of the Directive had already been cancelled by the Supreme Administrative Court in Bulgaria[6] and the Supreme Court in Cyprus[7] and are currently subject to constitutional complaints in Hungary and Poland[8].

Ruling of the Federal Constitutional Court of Germany (Bundesverfassungsgericht - BVerfG)

The constitutional complaint in Germany focused on sections 113a and 113b of the Telecommunications Act (Telekommunikationsgesetz - TKG[9]) and also on section 100g of the Criminal Procedure Code (Strafprozessordnung - StPO[10]), which permits the use of data gathered in accordance with the relevant provisions of the TKG. These provisions were adopted in an Act on the new form of supervision over telecommunications dated 21 December 2007[11] and represented the transposition of Directive 2006/24/EC into German legislation.

Section 113a of the TKG established the obligation of telecommunication service providers to retain the required data on telecommunication operations (telephone, e-mail, internet) for a period of six months. Section 113b of the TKG amended the purp-

[6] Bulgarian Supreme Administrative Court, Decision No. 13627 dated 11. 12. 2008.
[7] Supreme Court of Cyprus, decision in cases 65/2009, 78/2009, 82/2009 and 15/2010–22/2010.
[8] Finding file ref. Pl. ÚS 24/10. Point 52.
[9] Federal Collection of Laws BGB1 I p. 1190.
[10] Federal Collection of Laws BGB1 I pp. 1074, 1319.
[11] Federal Collection of Laws BGB1 I p. 3198.

oses for which retained data may be used. Section 100g of the StPO amended the use of data on telecommunications operations in criminal proceedings. At the same time the Criminal Code did not contain an exhaustive list of serious crimes for the use of preventatively gathered data, nor did it set out the requirement to assess the degree of appropriateness in a specific case of the investigation of a crime. In particular, the complainants saw in the preventative retention of data a breach of the right to telecommunications secrecy and the right to "informational self-determination". They considered the retention of all communications as being opposed to the principle of proportionality. According to the complainants, the retained data could be used to create a personality and movement profile of the individual. The BVerfG developed a broadly conceived right to informational self-determination (Informationelle Selbstbestimmung) in the ruling on the census of the people (Völkszählungsurteil) of 1983[12]. In this ruling the court pointed out that in conditions of modern information technologies specific data on personal and material background of a given person can be stored unlimitedly and loaded at any time from any distance. These data can be used, especially when exploiting multiple databases, for creating a full bodied profile of that person.[13]

The first Senate of the BverfG ruled on 2 March 2010 that the contested provisions of the StPO and TKG are in contravention of Art. 10 (1) of the Basic Law, leading to the nullity of the contested provisions[14]. However in the court's opinion in spite of this, data retention could be in compliance with the Basic Law[15] if certain limitations were applied (see below). Nevertheless, the BverfG did not declare the Directive itself unconstitutional. According to the BVerfG the contents of the Directive leave Germany considerable room for decisions on the manner of its implementation. Its provisions are limited to the obligation to retain data and a definition of those data. However, the Directive does not deal with access to those data and their use by the authorities of Member States. In view of this content the Directive may be transposed without causing any breach of constitutionally guaranteed rights. The Basic Law does not forbid the retention as such of data in a pre-defined structure[16].

When assessing the implementation regulations, the BVerfG, just like the European Court of Human Rights when assessing the compliance of a given legislation with Art. 8 of the European Convention on the Protection of Human Rights and Fundamental Freedoms, took into consideration the correctness of the legal basis, the legitimacy of the desired goal and the appropriateness of the adopted legislation.[17] According to the BVerfG the first requirement did not represent a problem. As far as the requirement for legitimacy is concerned, the BVerfG stated that the retention of data on telecommunication opera-

[12] BverfGE 65, 1.

[13] EMMENEGGER, S., WIEDMANN, A. *Linien der Rechtsprechung des Bundesverfassungsgerichts - erortert von den wissenschaftlichen Mitarbeitern*. Volume 2. Walter de Gruyter, 2011, p. 303.

[14] Finding of the German Federal Constitutional Court BVerfG 1 BvR 256/08 dated 2. 3. 2010. Press release. Available at: http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011, Para. 37.

[15] BvR 256/08 Press release, para. 10.

[16] Ibid.

[17] Mohini: On the BVG ruling on Data Retention: "Solange" – here it goes again… 5. 3. 2010. Available at: http://afsj.wordpress.com/2010/03/05/so-lange-here-it-goes-again.

tions for a period of six months may be legitimate and in conformity with the Constitution only insofar as the retention and subsequent use of data remains an exception ("dass diese eine Ausnahme bleibt"). The fact that the exercise of citizens' rights and freedoms may not be absolutely mapped and recorded, is part of the constitutional legal identity of Germany. In the opinion of the BVerfG, the Federal Republic should defend these principles both at European and international level.[18] By this, however, the Federal constitutional court in fact cast doubt on one of the main aims of the Directive - that data are to be retained preventatively and for an unlimited number of telecommunications services users.

The retention of data on telecommunication operations without a specific purpose for a period of six months represents particularly strong intrusion into constitutionally guaranteed rights. If such data are monitored for a sufficiently long period of time, they can be used to create a personality and movement profile with a high information content for almost every citizen. However, the greatest problem for the BVerfG was represented by the failure to meet requirements of the principle of proportionality. In view of the degree of intrusion into constitutionally guaranteed rights, caused by preventative collection and retention of data, this activity can be in accordance with Art. 10 (1) of the Basic Law only if its legislative wording satisfies certain constitutional legal requirements. This legislative wording must contain sufficiently precise and definite provisions on 1) data security, 2) data use limitations, 3) transparency and 4) legal protection.[19]

A high degree of security for the retained data must be clearly defined in the legislation. The contested legislation merely requires the maintenance of the general level of prudence assumed in the area of telecommunications. There is no requirement for a minimum level of data security, the adoption of specific measures is left to the discretion of individual telecommunication service providers. The use of such data in criminal proceedings can be considered only for particularly serious crimes, where in the individual case the suspicion that the crime has been committed, is supported by specific facts. The qualifying facts for these particularly serious crimes must be exhaustively enumerated by the legislator in any legislation demanding an obligation to retain data.[20]

The repealed provision of the StPO did not contain any limitation and thus permitted data to be used to prosecute any crime regardless of its seriousness, based only on the discretion of the body requesting it. The use of data for criminal prosecutions then, in view of the scope of the use of telecommunications in everyday life, loses in the opinion of the BVerfG its characteristic exceptionality, as required to meet the condition of legitimate aim.[21]

According to the BVerfG the legislator must, using effective transparency rules, allay any feelings of concern, uncertainty and threat created in citizens by the permanent retention of data. The use of data gathered without the awareness of a particular person must be permitted only in the event when the purpose of an investigation would otherwise be thwarted, such data are essential for the investigation and their use ordered by a judge.

[18] BvR 256/08 Press release, para. 15.
[19] BvR 256/08 Press release, para. 16.
[20] Ibid. para 18.
[21] Ibid. para 30.

If any secret use of such data takes place, the legislator must for these cases set out a obligation to subsequently inform the persons affected.[22]

The gathering and use of data must in the view of the BVerfG be entirely subject to judicial scrutiny. If the affected person does not have the opportunity to avert the use of data gathered about himself, he must be given the possibility of subsequent judicial scrutiny. Legislation respecting the principle of proportionality must also contain effective sanctions for breach of the law.[23]

The German Federal Constitutional Court thus came to the conclusion that the provisions of German acts implementing the Directive were in contravention of the Basic Law. In its opinion the Directive itself can be implemented in a manner consistent with the constitution, but only by meeting strict conditions. Nevertheless, finding an agreement between these conditions arising from the Basic Law and the demands set out in the Directive will not be at all easy for German legislators (see below).

Ruling of the Constitutional Court of Romania

On 8 October 2009 the Romanian Constitutional Court issued Decision No. 1258[24], in which it found Act No. 298/2008, on the retention of data generated or processed by providers of public telecommunication services and communication networks, and amendment to the provisions of Act No. 506/2004, concerning the processing of personal data and protection of privacy in electronic communications, to be unconstitutional. These provisions represented the transposition of the Directive into Romanian legislation.

The contested Act No. 298/2008 charged providers of communication services with the duty of retaining certain data created or processed during their activities for a period of six months, with the aim of making these data available to authorised bodies, to be used for the detection, investigation and prosecution of serious crimes. According to the petitioner the aforementioned provisions were in breach of the following articles of the Romanian constitution: Art. 25 – freedom of movement, Art. 26 – protection of intimate, family and personal privacy, Art. 28 – security of the mails and Art. 30 – freedom of speech.[25]

According to the Romanian Constitutional Court, the right to privacy and to family life is acknowledged and protected by international Conventions, specifically Art. 12 of the Universal Declaration of Human Rights, Art. 17 of the International Covenant on Civic and Political Rights, Art. 8 of the European Convention on Human Rights and finally also Art. 26 of the Romanian Constitution. The right to privacy implies the right to secrecy of the mail (also governed by the same Art. 8 in the European Convention on Human Rights). Correspondence reveals the connection of an individual with other members of the society regardless of the kind of communication chosen, therefore protection also covers tele-

[22] Ibid. para 21.
[23] Ibid. paras. 23, 25.
[24] The decision of the Romanian constitutional court was published in the Romanian Official Journal No. 789 dated 23 November 2009. An unofficial translation into English is available at: http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf. (the "unofficial translation").
[25] Page 1 of the unofficial translation.

phone conversations and electronic communications.[26] These rights are not however absolute and unconditional. By setting out the obligation to retain named data, Act No. 298/2008 expressed the desire of the legislator to set certain limits on the exercise of the right to privacy, freedom of speech and in particular on secrecy of the mail.[27]

Neither the ECHR nor the Romanian Constitution forbid the law from amending the possibility of interfering with the exercise of the aforementioned basic rights and freedoms, but any interference by the state must respect strict rules which are specified in Art. 8 of the ECHR or in Art. 53 of the Romanian Constitution.[28] The Romanian Constitutional Court referred in its ruling to case law of the European Court of Human Rights (ECHR) from which it infers that normative acts introducing measures which may impinge on the exercise of named rights must contain appropriate and adequate means of protection against any abuse on the part of state authorities.

The Romanian Constitutional Court admittedly acknowledged the option for the legislator to limit the exercise of guaranteed rights and freedoms and at the same time also recognised the need to give bodies participating on criminal proceedings effective means to prevent and detect terrorism and other serious crime. It found nevertheless that Act No. 298/2008 can affect the exercise of these fundamental rights and freedoms in a manner which does not satisfy the requirements set out in Art. 53 of the Romanian Constitution.[29] This act establishes, inter alia, the obligation of a provider to retain "related data needed for the identification of a user". However, it did not define this obligation in any more detail. According to the Romanian Constitutional Court this opens the way to abuse in the processing and use of the retained data. In the opinion of the Romanian Constitutional Court, any limitation on the exercise of the aforementioned rights guaranteed by the constitution must be conducted in a clear, predictable and unambiguous manner, so as to prevent any arbitrary use or abuse on the part of the authorities to the greatest possible extent. The targets of any data gathering must have a clear idea of the standards being applied, so that they can adapt their behaviour and anticipate any consequences which might arise in the event that they breach these rules. ECHR case law expresses itself in the same manner. Similarly, the actual concept of "threat to national security" is not specified in more detail in the contested Act, so that, according to the Romanian Constitutional Court it can happen that certain proper activities of legal entities and private persons will be assessed as a threat to national security through an arbitrary action of state authorities.[30]

In the opinion of the Romanian Constitutional Court the obligation to retain data, as set out in Act No. 298/2008, as an exception to, or departure from, the principle of the protec-

[26] Ibid. p. 18.
[27] Ibid. p. 4.
[28] Art. 53 of the Romanian Constitution:
(1) The exercise of guaranteed rights and freedoms may be limited by law only when it is essential for: defence of national security, public order, health and morality, civic rights and freedoms; the conduct of criminal investigations; avoiding the consequences of natural disasters, catastrophes and emergencies.
(2) Such limitations may be ordered only if it is essential in a democratic society. Measures must be commensurate with the situation which generated them and applied without discrimination and without disruption to the existence of such a right or freedom.
[29] Page 5 of the unofficial translation.
[30] Ibid. p. 6.

tion and confidentiality of personal data, voids the content of this principle by its very nature, length and areas of application. The Court meanwhile pointed to ECHR case law[31] from which it follows that provisions guaranteeing the protection of human rights and fundamental freedoms must be specific and effective, and not theoretical and illusory. The obligation laid down by the law to permanently retain personal data transforms an exception from the principle of effective protection of fundamental rights into an absolute rule. In this connection the Romanian Constitutional Court pointed out the fact that in this case a right is defined in a negative manner, and its positive role thus loses its predominance.[32]

In addition, the Romanian Constitutional Court emphasised that it is not the authorised use of gathered data itself that breaches the exercise of constitutionally guaranteed rights and freedoms in an unacceptable manner. The breach is caused by the legal duty to gather data, applied permanently and to an indefinite group of persons - regardless of whether these persons have committed illegal acts or not, whether they are the object of investigation or not, which contravenes the principle of the presumption of innocence - thereby placing all users of communications services in the position of being suspected of committing serious crime.

The Romanian Constitutional Court did not deny the intentions of the legislator as such, in the sense that there exists an urgent need to secure appropriate and effective means to pursue crime and which will take into account progress in communication technologies. But when implementing this legislative intention a balance must be maintained between the interests and guaranteed rights of the individual on the one hand and the interests of society in national security on the other. In the opinion of the Romanian Constitutional Court, the introduction of state surveillance measures without proper guarantees can lead to the destruction of democracy while trying to defend it.[33]

In comparison with the ruling of the German Federal Constitutional Court (BVerfG), which concedes the possibility of a constitutionally admissible implementation of the Directive, provided the conditions of a legitimate goal and proportionality are met, the Romanian Constitutional Court has declared the very requirements set out in the Directive as being incompatible with the Romanian Constitution and the ECHR.

Ruling of the Constitutional Court of the Czech Republic

On 26 March 2010 the Constitutional Court (CC) received a proposal from 51 members of the Czech Parliament, represented by deputy Marek Benda, to repeal Section 97 (3) and (4) of Act No. 127/2005, on Electronic Communications, as amended (the Act) and a proposal for the repeal of Decree No. 485/2005 on the Scope of Operational and Localisation Data, Retention Period and Form and Manner of their Transfer to Authorities Authorised to use them.[34]

The petitioners claimed that the contested provisions breach Art. 7 (1), Art. 10 (2) and (3) and Art. 13 of the Charter of Basic Rights and Freedoms (the Charter) and Art. 8 of the

[31] e.g. Prince Hans-Adam II of Liechtenstein vs. Germany (2001).
[32] Page 7 of the unofficial translation.
[33] Ibid. p. 10.
[34] Proposal of a group of parliamentary deputies to the CC of the Czech Republic, file ref. Pl. ÚS 24/10.

ECHR, that is the basic rights to personal and family privacy, to protection against unjustified gathering of data about oneself and to protection of secrecy of the mails and security of means of communication to the widest possible range.[35]

In their reasoning, the petitioners focused primarily on the lack of compliance of the contested provisions of the implementing legislation with Art. 8 of the ECHR, having regard to existing case law of the European Court of Human Rights, which is recognised and relied upon by the CC in its decisions, particularly on the principle of proportionality. It was the assessment of compliance of the contested provisions with this principle that this proposal for the repeal of the Czech transposition of the Directive was based on.

The Constitutional Court, in its judgement dated 22. March 2011, ruled in favour of the petitioners and repealed the contested provisions[36]. The CC based its assessment of the proposal on the justifiability of encroaching the autonomy of the individual, defined by fundamental rights and freedoms, for the reason of a collision with the public interest, which must be constitutionally based and unambiguously defined in the law. The prerequisite for compliance with the principle of a democratic state respecting the rule of law is that any encroachment on the autonomy of the individual and anticipated by the law is proportionate both with regard to the aim which is to be achieved and with regard to the extent of the curtailment of a fundamental right or freedom (Point 26 of Ruling Pl. ÚS 24/10). In the ruling concerning telephone communication[37] the CC insisted on the maintenance of strict proportionality of interference with the right to privacy, especially in respect of the purpose for which the intrusion into the private communication was conducted, i. e. the existence of a specific suspicion of committing a crime, respectively the seriousness of a specific threat.[38]

The CC acknowledges the individual's right to informational self-determination which the BVerfG had developed and had also applied when assessing the German transposition of the Directive. The right to informational self-determination as an aspect of the wider right to privacy was derived in the rulings of the Constitutional Court from Art. 10 (3) in conjunction with Art. 13 of the Charter. It follows from CC case law that protection of the right to informational self-determination relates not only to the actual content of messages, but to data on telecommunications operations[39] (Point 32 of Ruling Pl. ÚS 24/10) as well.

These rights which are embodied in Chapter two of the Charter have a specific significance among others rights and freedoms because they are directly applicable and can be sought by virtue of the Charter itself and differ from some other fundamental rights and freedoms embodied in the Charter which can be sought only within ordinary laws implementing the respective provision of the Charter.[40] But this does not alter the fact that exercise of these rights can be limited by the law if certain conditions are fulfilled – which is set out explicitly in Art. 13 of the Charter. In addition to the conditions for permissibility

[35] Ibid.
[36] Finding file ref. Pl. ÚS 24/10.
[37] Finding file ref. I. ÚS 3038/2007.
[38] WAGNEROVÁ, E. a kol. *Listina základních práv a svobod. Komentář.* Praha: Wolters Kluver ČR, 2012, p. 342.
[39] Finding file ref. II. ÚS 502/2000.
[40] SLÁDEČEK, V. – MIKULE, V. – SYLLOVÁ, J. *Ústava České republiky. Komentář.* Praha: C. H. Beck, 2007. p. 39.

of interference with the right of informational self-determination by public authorities, set out explicitly in Art. 8 of the ECHR (such interference may take place only exceptionally, where it is essential in a democratic society, if the aim being pursued in the public interest cannot be attained in any other manner), the CC held that the interference must be subject to certain specific safeguards against arbitrary conduct. These safeguards then consist in the corresponding legislation and its effective enforcement (Point 36 of Ruling Pl. ÚS 24/10).

According to the CC, the legal formulation of an interference in informational self-determination must then satisfy the requirements arising from the proportionality test developed by the ECHR and also used by the BVerfG in assessing the transposition of the Directive. The test comprises three steps: assessment of eligibility of the purpose to be fulfilled; assessment of the necessity (whether the means chosen is the most respectful of fundamental rights); assessment of proportionality in the narrower sense of the word (whether the intrusion in fundamental rights is not inappropriate in relation to the intended aim). Just like both earlier Constitutional Court decisions, the CC emphasised the condition developed by the ECHR, that is that the legislation *"must be precise and visible in its formulations and sufficiently predictable as to provide potentially affected individuals with sufficient information, so that the latter may as required adjust their behaviour in such a manner as not to come into conflict with a limiting regulation"* (Point 37 of Ruling Pl. ÚS 24/10).

According to the CC the contested legislation does not satisfy the aforementioned requirements for a number of reasons. In particular, the group of authorities entitled to request operational and localisation data is not unambiguously defined. Similarly, the period for data retention is not precisely defined. The duties of organisations which retain data on telecommunication operations are set out in the Act only vaguely (a duty to *"provide data to bodies authorised to request them in line with a special legal regulation"*) which does not satisfy the aforementioned requirements for precision and clarity in respect of a state respecting the rule of law. In contrast to the Directive, the purpose for which the operational and localisation data are being provided is not precisely and clearly defined *("elucidation of facts important for criminal proceedings")*. Similarly, there is no regulation of the obligation of criminal proceedings bodies to inform an affected person that he is being monitored, not even retrospectively, which in the opinion of the CC fails to satisfy the demands arising from the second step of the proportionality test (Point 47 of Ruling Pl. ÚS 24/10).

According to the CC, the absence of legislation meeting these requirements then leads to the option for criminal proceedings bodies to request data on telecommunications operations being overused for the investigation of not just serious, but also routine crime. The contested legislation also *"fails to establish adequately, if indeed at all, clear and detailed rules containing minimum requirements to secure retained data against the risk of data abuse and arbitrary misuse"* (Point 51 of Ruling Pl. ÚS 24/10). Nor are there definitions of the responsibilities of, and sanctions for failing to meet the duties assigned to, telecommunication service providers. Interference with the right of individuals to informational self-determination in the form of retention of data about their telecommunication activities thus *"through the impact of inadequate legislation which does not correspond to the abovementioned constitutional legal requirements, finds itself outside any immediate, or*

even retrospective scrutiny, and in particular outside judicial scrutiny" (Point 51 of Ruling Pl. ÚS 24/10).

In its conclusion, the CC summarised that the contested provisions *"cannot be considered as conforming to the constitution, since they clearly breach these previously explained constitutional limits, since they do not satisfy the requirements arising from the principle of a legal state and are in conflict with the requirements for limiting fundamental rights to privacy in the form of the right to informational self-determination in the sense of Art. 10 (3) and Art. 13 of the Charter, which follow from the principle of proportionality"* (Point 54 of Ruling Pl. ÚS 24/10).

The CC also considers unconstitutional the provision of Section 88a of the Criminal Procedure Code governing the conditions for using retained data for the purposes of criminal proceedings. However, because this provision was not contested by the petitioners, the CC did not repeal it. It was eventually repealed by the CC ruling dated 20. 2. 2012 (Pl. ÚS 42/11), which repealed this provision as of 30 September 2012.

Nevertheless according to the CC the actual retention of data on telecommunication operations, as required by the Directive, is not unconstitutional providing the abovementioned requirements are satisfied, since the *"content of the Directive itself leaves the Czech Republic sufficient room for its transposition into national legislation in a manner conforming to the constitution, when its individual provisions in essence only define the obligation to retain data"* (Point 25 of Ruling Pl. ÚS 24/10)

The CC therefore repealed the national transposition of the Directive because of defects similar to the ones found by the German BVerfG in their legislation. Just like the German Constitutional Court, the CC is also of the view that the Directive itself is not in contravention of the constitution and that it can also be transposed into national law in a manner which conforms to the constitution. Thus the Romanian Constitutional Court leaves for the moment the only constitutional court of an EU member state which has declared the actual retention of data, the very substance of the Directive unconstitutional. Nevertheless, as previously stated, national transpositions of the Directive had also already been cancelled by the Supreme Administrative Court in Bulgaria and the Supreme Court in Cyprus and are currently the subject of constitutional complaints in Hungary and Poland.

1.3 Government reactions to the rulings of the constitutional courts of EU Member States

The reaction to the aforementioned case law of the constitutional courts on the part of the legislator is indeed different across the countries being compared.

Germany

In Germany the CDU/CSU and FDP coalition is unable to agree on new legislation to implement the Directive, following the repeal by the Federal Constitutional Court. The Justice Minister for the FDP, Sabine Leutheusser-Schnarrenberger, considers data retention in the manner called for by the Directive to be a breach of fundamental rights. She is therefore proposing limited retention of data on telecommunication operations only on the basis of specific suspicions. In contrast, its coalition partner CDU/CSU, represented by Minister of the

Interior Hans-Peter Friedrich (CSU) is calling for the full transposition of the Directive and in this context is he even calling the coalition Justice Minister "a security risk".[41]

On 31 May 2012, the Commission submitted a complaint against Germany at the EU Court of Justice for infringement of the Treaty, in an attempt to force it to speed up new implementation of the Directive. It proposes that a fine be imposed on Germany until it adopts implementation legislation.

Romania

In Romania a new draft of national implementation of the Directive on Data Retention was submitted for public comments on 23 June 2011, which is roughly a year and a half after the repeal of the previous legislation by the Constitutional Court. This may have been an immediate reaction to infringement proceedings started by the Commission for not implementing the Directive, dated 16 June 2011.

Although the sponsor of the new legislation, the Ministry for the Information Society and Communications, states that the draft is in line with the Constitutional Court's decision and ECHR case law, according to critics it is no more than a copy of the repealed Act No. 298/2008[42]. According to the latter the only change is a very general provision in the new Art. 13 of the draft, according to which the retention of data on telecommunication operations must meet the same security requirements as other data used by providers of telecommunication services and requirements for suitable technical and organisational measure to prevent the loss or misuse of retained data.

According to the critics, the proposed text is even more general than the repealed legislation, where for example access to the data is to be provided under conditions set out in the criminal procedure code or other special regulations. According to the draft the right to use retained data may be invoked by judicial bodies and state authorities whose activities are related to national security - a similarly vaguely formulated enabling provision was one of the reasons for repealing the previous legislation.

The proposer himself admits to being trapped in a blind alley: "According to the Constitutional Court one may not retain data for a period of six months for a person who is not under investigation for committing a crime. On the other hand, this is in contravention of the Directive, which calls for the retention of data on all users for a minimum period".[43]

The proposer thus prioritised meeting Romania's obligations arising from its membership of the EU ahead of a binding decision of its constitutional court - it will be interesting to follow what position the latter takes on the proposed legislation, should it come into force.

Czech Republic

In the Czech Republic, the government reacted to the Constitutional Court's ruling on 27 February 2012 by presenting a draft amendment to the Act on Electronic Communica-

[41] Spiegel: CSU nennt Justizministerin "Sicherheitsrisiko", 31. 5. 2012, available at: http://www.spiegel.de/politik/deutschland/vorratsdatenspeicherung-eu-kommission-verklagt-deutschland-a-836221.html.

[42] New Draft Law For Data Retention In Romania, 29. 6. 2011, available at: http://www.edri.org/edrigram/number9.13/new-draft-data-retention-romania.

[43] Ibid.

tions[44]. The amendment aims to introduce the obligation on the part of telecommunications service providers to retain operational and localisation data while meeting the conditions set out in the repeal ruling of the Constitutional Court.

In contrast to the repealed legislation, the draft precisely defines the period of retention, which is limited to 6 months from the start of the communication. This is the shortest period called for by the Directive.

The petitioner has taken account of the condition set out in the CC decision and defined an exhaustive list of authorised organisations which may request provision of the record of a telecommunication transaction. These are the bodies active in criminal proceedings as defined in the Criminal Procedure Code, the Police outside criminal proceedings (wanted or missing persons search, etc.), the intelligence services (the Security Information Service, Military Intelligence) and the Czech National Bank in exercising supervision of the capital markets.

As far as the obligation given in the repeal ruling to set out clear and detailed rules for securing retained data, according to its explanatory note the draft envisages an obligation on the part of organisations retaining data to maintain the conditions set out in the Act on the Protection of Personal Data and also the conditions defined in the relevant (and not repealed) provisions of the Act on Electronic Communications. This obligation was, however, also contained in the repealed legislation, and the draft thus does not introduce a new, higher level of protection.

In addition, the draft, with reference to the repeal ruling of the CC, introduces the obligation to inform a person whose data have been requested of this use, following the valid termination of the criminal case. There are a number of exceptions to this obligation, for example in case of proceedings on a crime for which the law sets a punishment of imprisonment with an upper limit of at least 8 years.

The draft adds the requirement of the principle of subsidiarity to the Criminal Procedure Code and the Act on Supervision of Capital Markets. That means a judge may order the issue of data on telecommunication operations only if the pursued aim cannot be achieved in any other manner, or if other means would substantially hamper its achievement. This requirement thus does not affect the authorisation of the intelligence services. This definition of the principle of subsidiarity corresponds to the amendment of phone tapping in the Criminal Procedure Code. The implementation of tapping, just like the provision of data on telecommunication operations for the purposes of supervision of the capital markets, must, however, also satisfy the condition that one can reasonably assume that this will provide significant information for criminal proceedings. The principle of subsidiarity would thus be interpreted somewhat more freely when requesting telecommunication data for criminal proceedings purposes.

In its ruling the CC repealed the act on the ground that it failed to unambiguously set out the purpose, prerequisites and conditions for the use of data on telecommunication operations, ensuring that the intrusion into basic human rights will be proportionate to the aim pursued. In other words, the option to use these data is to be limited only to the most serious cases. Whereas neither the Directive, nor any other Union legal regulations defines in more detail the category of especially serious crimes, and the individual Member States have selected various criteria in definition of this category, the petitioner in the explanatory note

[44] Government Bill to change Act No. 127/2005, on Electronic Communications and a change to certain related Acts (the Act on Electronic Communications) as amended, and certain other laws. Parliamentary Press 615/0, Czech Chamber of Deputies, delivered 27. 2. 2012.

also maintains that the Directive does not forbid the gathered data from being used for other cases than just the investigation of serious crimes, nor does it give any kind of rules for the group of state bodies which might obtain them (p. 15). The draft amendment to the criminal code comes with limitation on the possibility of requesting these data for the purposes of criminal proceedings only for certain groups of crimes. These categories are (i) wilful crimes for which the law sets a punishment of imprisonment with an upper limit of at least three years (the limit is defined by the possibility of being taken into custody for unpremeditated crimes), (ii) wilful crimes to the prosecution of which the Czech Republic is committed by international treaty and (iii) listed crimes in which the offender's behaviour is based on the use of electronic communications. When compared with the amendment for the use of phone tapping for criminal proceedings purposes, which sets an upper limit for punishment of at least 8 years, the proposed limit for the use of a telecommunications operations record seems fairly soft, as these data can be requested by criminal proceedings bodies when verifying their suspicions of the commitment in an absolute majority of crimes.

As far as the intelligence services are concerned, the Act on the Security Information Service and the Act on Military Intelligence would, according to the draft, allow both of these organisations to request operational and localisation data "to the extent needed to fulfil a specific task", that is, to the same extent as in the case of phone tapping.

Whereas in the case of the intelligence services one might consider such generously defined access to the data to be appropriate in view of their specific tasks, in the case of access by criminal proceedings bodies it is not so clear. What may be more problematic is the proposed option for a much broader use of operational and localisation data than is allowed for phone tapping, whereas the information value of operational and localisation data may be minimally comparable with the information value of the content of a communication, as was maintained at least, by reference to international studies, by Benda and others in their successful proposal to have the previous legislation repealed.

The proposer of the new amendment admittedly formally meets the requirement of the CC to set out the purpose for the use of data on telecommunication operations by defining a group of crimes. Nevertheless, by including almost all crimes, this limitation in reality almost fails to be visible and therefore the condition formulated in Ruling Pl. ÚS 24/10 is not met, that "the intrusion into basic human rights must be appropriate to the aim being pursued, that is, must comply with the principle of appropriateness" (Point 37 of Ruling Pl. ÚS 24/10). According to the doctrine, the purpose of proportionality principle is to ensure that legal reservation will not be used to higher limitation of fundamental rights than it is really necessary. Legislation in the field of fundamental rights is limited by maintaining the appropriate proportionality of purpose which should be achieved and proportionality of selected means.[45] One can reasonably doubt that in case of less serious crimes the intended purpose is really proportionate to the degree of fundamental right limitation.

Under the conditions set up in this way, one cannot rule out that there will be excessive use of the option to request data on telecommunication operations, which was one of the reasons why the CC ruled against the repealed legislation in its judgement.

The Chamber of Deputies passed the government proposal on 20 June 2012, the Senate passed it on 18 July 2012, and the President signed the bill on 1 August 2012. The Act was

[45] WAGNEROVÁ, E. a kol. *Listina základních práv a svobod. Komentář.* Praha: Wolters Kluver ČR, 2012, p. 26.

declared in the Collection of Laws under 273/2012 Coll. and came into force on 1 October 2012. The bill was voted for by representatives and senators from all political parties represented in both chambers of the Czech Parliament.

2. CONCLUSION

One may take the view that if the new legislation is once more contested at the Constitutional Court, there will once more be a repeal of the national implementation of the Directive in the Czech Republic, since in my view the draft did not meet all the conditions set by the Constitutional Court in its repeal decision. In Romania a new Act implementing the Directive has been passed, but nor in this case were the conditions met as raised by the ruling of their constitutional court. Judging by the intense debates generated in Germany by the intention to implement once more the retention of data on telecommunication operations, one may infer that they have not been successful in finding a compromise between the obligation to implement the Directive in national legislation and the binding decision of the Federal Constitutional Court.

The European Commission has so far obstinately demanded the renewed implementation of the Directive in those Member States where the constitutional courts had repealed it. It has not hesitated to make use of the institution of proceedings for breach of the Treaty by these Member States as a means of pressure. The fact that a ruling of constitutional court of a Member State can be subject of an infringement procedure before the Court of Justice of the EU can be assessed as problematic. However, according to the doctrine the opinion prevails that conduct of a national court represents conduct of its Member States.[46]

It is, however, possible that the situation where legislators in several member states have a problem in finding an implementation of the Directive which conforms to their constitution, and where it is the subject of constitutional complaints in others, such as Hungary and Poland, has forced the European Commission to re-evaluate this uncompromising position.[47] The Commission is planning to propose a new amendment for the retention of data on electronic communications. The new proposal was due to have been presented in July 2012.[48] According to unofficial sources this plan has however been deferred by at least a year[49]. Nevertheless, it is still a question as to how large a change would be represented by the new amendment compared to the current Directive. And whether it will be a change for the better, when seen from the viewpoint of fundamental rights and freedoms.

[46] TICHÝ a kol. *Evropské právo.* 4 vydání. Praha: C. H. Beck, 2011, p. 368.

[47] The Directive is once more the subject of proceedings on a preliminary question in case C-293/12, with which the High Court of Ireland addressed the CJEU (and not for the first time) on 10 August 2012. The Irish court submitted the question of whether the Directive is compatible with the right of citizens to move freely and reside on the territory of member states, as set out in Art. 21 of the TFEU, with the right to privacy set out in Art. 7 of the EU Charter of Fundamental Rights and in Art. 8 of the ECHR, with the right to the protection of personal data set out in Art. 8 of the EU Charter of Fundamental Rights, with the right to freedom of speech as set out in Art. 11 of the EU Charter of Fundamental Rights and in Art. 10 of the ECHR and with the right to proper administration set out in Art. 41 of the EU Charter of Fundamental Rights.

[48] Consultation on reform of Data Retention Directive: emerging themes and next steps. Council document No. 18620/11 dated 15. 12. 2012.

[49] Data Retention Directive reform delayed by a year, available at https://publicaffairs.linx.net/news/?p=8453.