Implications of invalidity of Data Retention Directive to telecom operators

LL.M. **Darja LONČAR DUŠANOVIĆ**[1]

Abstract

Obligation for telecom operators to retain traffic and location data for combating crime purposes had been controversial ever since the adoption of the Data Retention Directive in 2006 because of its inherent negative impact on the fundamental right to privacy and personal data protection. However, the awaited judgment of the CJEU in April this year, which declared the Directive invalid, did not so far resolve the ambiguity of the issue. Namely, having in mind that half a year later, some countries did not amend their national data retention legislations (yet) to comply with the aforementioned CJEU judgment, telecom operators as addresses of this obligation are in uncertain legal situation which could be called "lose-lose" situation. Also, the emphasis from the question of proportionality between data privacy and public security is shifted to the question of existence of valid legal basis for data processing (retaining data and providing them to authorities) in the new legal environment in which national and EU law are still not in compliance. In this paper the author examines the implications of the CJEU judgment to national EU legislation, telecom operators and data subjects, providing comparative analysis of national data retention legislation status in EU member states. The existence of valid legal basis for data processing is examined within EU law sources, including within proposed EU General Data Protection Regulation and opinions of the relevant data protection bodies (e.g. Article 29 Working Party).

Keywords: *data retention, Data Retention Directive, data protection, privacy, legal bases.*

JEL Classification: K30, K33

1. Introduction

Without intention to undermine the general positive impact of the Court of Justice of the EU judgment invalidating Data Retention Directive (further in text: CJEU judgment)[2], which is righteously often referred to as historical or landmark judgment, this paper focuses on three legal and factual problematic consequences of this judgment which are inter-related. These are: 1) legal uncertainty, especially for telecom operators[3] as addressees of the data retention obligation with respect to

[1] Darja Lončar Dušanović – Croatian Telecom Inc., darja.loncar@t.ht.hr

[2] Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others, 8.4.2014., Court of Justice of EU, InfoCuria – Case-law of the Court of Justice, the document is available on-line at http://curia.europa.eu/juris/liste.jsf?num=C-293/12# , last day accessed on 13.11. 2014

[3] Telecom operators are joint term for providers of publicly available electronic communications services or of public communications networks; Article (1) of the Directive 2006/24/EC of the

this obligation (4.1.); *inter alia*, due to the unclear answer to the 2) question of existence of legal bases for data retention (4.2.); and additional complexity of the issue having in mind that 3) Data Retention Directive[4] (further in text: DR Directive) was declared invalid, thus with *ex tunc* effect (4.3.). After this introductory part on the issue in question, this paper will provide brief overview about DR Directive, including emergence and reasons for its enactment in 2006, which will be followed by the presentation of the main conclusions and argumentation of the CJEU judgment. This should lead to the central part of this paper- three inter-related consequences of the invalidity of DR Directive as mentioned ad.1)-3) above. Implications of the invalidity of DR Directive are relevant to all EU member states and in particular those in which the national legislation on data retention is still in place and was not (yet) assessed with respect to its compliance with the CJEU judgment. Therefore, the issue in question shall be primarily addressed on EU level, that is, scrutinized from EU law perspective and not from particular national law perspective[5]. However, certain comparative analysis of the status of current data retention regulation in EU member states following CJEU judgment will be provided.

This paper doesn't tend to provide final nor long lasting solution for adequate data retention regulation, as this would be demanding task requiring answers to complex question of supremacy between EU and EU member states law, as well as question about justification of "special status" of national security and combating crime purpose in relation to data privacy, which would go beyond this paper and would require engagement and competences of experts in more fields than in data privacy of electronic communications. However, this paper (although tackling these questions) in its conclusion suggests possible "quick-win" for faster alignment of national data retention legislation with EU law. The novelty of this paper is less in pointing out to the legal uncertainty of telecom operators and data subjects (ad.1) above), as this has been with more or less details mentioned continuously ever since the CJEU judgment, but more in setting the question about legal bases for data retention in general (ad.2) above), which can be useful in particular for telecom operators in assessing their legal position with respect to data retention issue and which can be useful as bases for reaching comprehensive and long(er)lasting solution for data retention regulation on EU and national level.

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, Official Journal of the European Union L 195, 13.4.2006.

[4] 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, Official Journal of the European Union L 105, 13.4.2006., pp. 54-63

[5] This point of addressing the issue is, however, possible only to certain extant as Member States' national laws and EU law are inter-related.

2. Data Retention Directive; emergence and impact

Data retention is the term which is in telecom sector generally understood as obligation of telecom operators to retain certain customer data generated by communication (traffic, location and other related customer data) and to provide access to national authorities for law enforcement purposes[6]. Inherent feature of data retention, as its name clearly suggest, is that it represents restriction to personal data protection and privacy rights.

Data retention[7] for law enforcement purposes on the level of EU was first introduced in 1997 by Directive 97/66/EC[8], but only as possibility and not the obligation for Member States, presupposing the necessity of such measure. The purposes for such measure, which were stated in than applicable article 14(1) of the Directive 97/66/EC, were *safeguarding national security, defense, public security, the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the telecommunications systems*. This article 14(1), and for the matter of fact, the whole Directive 97/66/EC was replaced by the new e-Privacy Directive[9] which was part of the entirely new EU regulatory framework of electronic communications sector, which was passed in 2002. e- Privacy Directive remained the facultative approach for EU member States to introduce measures restricting certain rights granted by e-Privacy Directive, provided that such measures are *necessary, appropriate and proportionate within democratic society* (article 15 paragraph 1). The purposes for such measures were the same as those in the Directive 97/66/EC. However, e-Privacy Directive introduced the term data retention by explicitly stating that one of those measures could be retention of data. As a consequence of such facultative approach some EU member states obliged their telecom operators to retain the data and to invest in expansive equipment for retaining data, while other did not, which was seen as distortion of internal EU

---

[6] Although the data retention is the general term which can be used for retaining data for other purposes, e.g. billing purpose, the most common use of the term in telecom sector is the one relating to law enforcement purposes.

[7] However, Directive 97/66/EC did not include the term data retention, but general term of measures restricting the scope of the obligation and rights.

[8] Directive of European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, Official Journal of the European Union L 24, 30.1.1998., pp. 1-8

[9] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal of the European Union L 201, 31.7.2002., pp. 0037-0047 as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, Official Journal of the European Union L 337, 18.12.2009, pp. 11–36

market[10]. Also, further developments of telecom services, as well as terrorist attacks in Madrid and London, had been setting the ground for new regulation on data retention[11] .

DR Directive was enacted in 2006 introducing obligatory data retention and aiming to harmonize Member States' provisions with respect to data retention. According to DR Directive, providers of publicly available electronic communications services or of public communications networks[12] were obliged to retain certain customer data generated by their services and/or networks for purposes of the investigation, detection and prosecution of serious crime, to be determined by each EU member state[13]. DR Directive defined only minimum and maximum period of data retention – 6 months to 2 years following communications, whereas the exact period is left to be determined by national legislation. Categories of data to be retained by telecom operators were explicitly stated in DR Directive[14], however very extensively, including all traffic, location and related customer data generated by usage of fixed network and mobile telephony services, Internet access services, Internet e-mail and Internet telephony services. Nevertheless, retention of data revealing the content of the communication was prohibited by DR Directive[15] . This restriction with respect to content represents adequate safeguards from privacy perspective only on the first site. Namely, retaining and processing of all other data about communication, often referred to as metadata due to its complexity and quality, may reveal even more

---

[10] *Report from the Commission to the Council and the European Parliament; Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)*, Brussels, 18.4.2011., COM (2011) 225 final, the document is available on-line at http://ec.europa.eu/commission_2010-2014/malmstrom/pdf/archives_2011/com2011_225_data_retention_evaluation_en.pdf , last day accessed on 13.11. 2014, p.3-4

[11] *Ibidem*

[12] "*It is useful to present the standpoint of the Article 29 Working Party with respect to this. Namely, it is of the opinion that it is clear that Directive 2006/24/EC will not obligate providers of information society services, such are, for example, web search services and social network services, because these are not electronic communication services. However, in cases when the provider of information society services provides public electronic communication service as additional service, such is publicly available electronic mail service, this provider should comply according to Directive 2006/24/EC with respect to this additional service.*", Nina Gumzej, *Data Protection in Electronic Communications; doctoral work,* Faculty of Law in Zagreb, 5.9.2011., pp. 374-375

[13] Directive 2006/24/EC, *op.cit.*at note 4, article 1

[14] Main categories of data to be retained by telecom operators according to DR Directive were: data necessary to trace and identify the source of a communication (calling number, name and address of customer, users ID ect.), data necessary to identify the destination of a communication (number dialed, name and address of customer, data necessary to identify the data, time and duration of a communication (data and time of the start and end of the communication ect.), data necessary to identity the type of communication (Internet service used ect.), data necessary to identify users' communication equipment or what purports to be their equipment, data necessary to identify the location of mobile communication equipment. Directive 2006/24/EC, *op.cit.*at note 4, article 5

[15] Directive 2006/24/EC, *op.cit.*at note 4, article 5 paragraph 2

information about the person than the content of the communication[16]. DR Directive had derogated the article 15 paragraph 1 of the e-Privacy Directive which is regulating possible restrictions for law enforcement purposes (including data retention), by regulating that this article will not apply to data covered by DR Directive[17]. In other words, article 15.1. of the e-Privacy Directive remained valid for all other situations which were not covered by DR Directive. This had created ambiguity and legal uncertainty with respect to applicability of article 15 paragraph 1 of e-Privacy Directive, as it will be explained later on in this paper (e.g. what could be the other possible measures restricting certain rights granted by e-Privacy Directive which are not data retention measures regulated by DR Directive?).

It is important to note that regulation of data retention, as was introduced by DR Directive was not a straight forward process, but a disputable on from its beginning, on the grounds on which it was eventually declared invalid by CJEU[18]. In its first assessment of implementation of the Data Protection Directive[19] in 2004, European Parliament stated that EU member states' laws about retaining data were not in full compliance with privacy right granted by European Convention of Human Rights, nor with the e-Privacy Directive with respect to proportionality and appropriateness in democratic societies[20]. Various EU authorities and human rights experts and activists had been advocating against data retention in general or against data retention as it is regulated by DR Directive; Article 29 Data Protection Working Party[21] has been questioning necessity of general data retention measures continuously[22]. On the other hand, in parallel, some countries (Ireland, Greece,

---

[16] For more information about metadata and relation between "metering" and content surveillance especially see *Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes*, Article 29 Data Protection Working Party, 819/14/EN, WP215, 10.4.2014., the document is available on-line at http://www.cnpd.public.lu/fr/publications/groupe-art29/wp215_en.pdf , last day accessed on 13.11.2014 and Case of Malone v. the United Kingdom, 2.8.1984., European Court of Human Rights, the document is available on-line at http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57533#{"itemid":["001-57533"]}, last day accessed on 13.11.2014.

[17] Directive 2006/24/EC, *op.cit.*at note 4, article 11

[18] For more information about this process see *op.cit*.at note 12, p.370-410

[19] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995 P. 0031 - 0050

[20] *Report on the First report on the implementation of the Data Protection Directive (95/46/EC) (COM(2003) 265 – C5-0375/2003 – 2003/2153(INI)),* final A5-0104/2004, European Parliament, 25.2.2004., p. 9, item 18, the document is available on-line at http://ec.europa.eu/justice/ policies/privacy/docs/lawreport/ep_report_cappato_04_en.pdf, last day accessed on 13.11.2014.

[21] The Article 29 Data Protection Working Party was set up under the Data Protection Directive. It has advisory status in data protection matters and acts independently. Its opinions and recommendations are important source of EU data protection law by authority.

[22] Article 29 Data Protection Working Party opinions: *Opinion 5/2002 on the Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 September 2002) on mandatory systematic retention of telecommunication traffic data*, 11818/02/EN/Final, WP 64, 11.10.2002; *Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with*

Sweden, Austria) did not transpose DR Directive on time, so European Commission initiated procedures against these EU member States and CJEU ruled against them. In its Evaluation Report on the Data Retention Directive[23] from 2011, European Commission, after having assessed the data retention situation in EU, proposed revision of the data retention framework and provided recommendations how this should be done[24], but at the same time stating that data retention is a valuable tool for criminal justice systems and for law enforcement in the EU. Constitutional Courts of several countries (Czech Republic, Germany, Macedonia)[25] annulled national data retention regulation based on DR Directive even before DR Directive was declared invalid by CJEU. In addition to all legal actions and events which had made DR Directive largely disputable, Snowden case in 2013 actualized the general question of proper balance between rights to privacy and data protection on the one side and public security on the other side, as the proportions of US secrete surveillance programs revealed by Snowden were found to be enormous.

3. CJEU judgment invalidating DR Directive

The awaited CJEU judgment was rendered in April 2014, ruling DR Directive invalid on the grounds that DR Directive entails a wide ranging and particularly serious interference with two fundamental rights in the legal order of European Union, without such an interference being precisely restricted to what is strictly necessary[26]; These two fundamental rights are: respect for private and family life from article 7 and protection of personal data from article 8 of the Charter of Fundamental Rights of the European Union[27]. Charter in its article 52 paragraph 1 provides for possibility of limiting the scope of fundamental rights under certain conditions[28]. However, CJEU concluded that "*by adopting Directive*

---

the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005), 1868/05/EN, WP 113, 21.10.20015., *Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive,* 00068/10/EN, WP 172, 13.7.2010.

[23] *Op.cit.* at note 10

[24] One of the recommendations was ensuring proportionality in the end-to –end process of storage, retrieval and use, *ibid*., p.32, item 8.5.

[25] *Annulment of the Data Retention Directive-consequences for national laws*, EU briefing document, Cullen International, 30.7.2014.

[26] *Op.cit.* at note 2, item 65

[27] Charter of Fundamental Rights of the European Union (200/C 364/01), Official Journal of the European Communities, 18.12.2000.

[28] "*Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others"*., *ibid.,* article 52 paragraph 1

200/24/EC, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7,8, and 52(1) of the Charter."[29]

Reasons for this conclusion of CJEU are based in particular on the following: a) DR Directive covers all persons, all means of electronic communications and all traffic data without and differentiation, limitation or exception (e.g. with respect to persons whose communications is subject to the obligation of professional secrecy)[30], b) DR Directive does not envisage objective criterion, substantive and procedural conditions which would ensure that competent national authorities have access to retained data and possibility for their subsequent use only for purposes of prevention, detection or criminal prosecution of criminal offences which are sufficiently serious to justify interference with fundamental rights and on need to know principles[31], c) DR Directive does not require any distinction with respect to time period of data retention between different categories of data[32], d) DR Directive does not ensure adequate safeguards for retained data against their abuse or unlawful processing, nor necessary high level of technical and organizational data protection measures or irreversible destruction at the end of the data retention period[33], e) DR Directive does not require that data should be retained in EU[34]. It should be also mentioned that CJEU in its judgment on DR Directive adopted or confirmed, *inter alia*, two important standpoints; Retaining of data and providing data access to national authorities, each activity by itself, constitutes personal data processing activities, and thus is subject to article 8 of the Charter of Fundamental Rights of the European Union[35] and even though content of communication is not being retained, because of the volume and the type of data being retained, this could influence exercise of the freedom of expression right from article 11 of the Charter of Fundamental Rights of the European Union[36].

It is important to emphasize that CJEU explicitly recognized that data retention *per se* is compliant with EU law, although it is interfering with fundamental rights. However, the way how this interfering is regulated by DR Directive, is not compliant with EU law and thus DR Directive is declared invalid. This differentiation adds to the legal uncertainty for telecom operators.

---

[29] *Op.cit.* at note 2, item 69
[30] *Op.cit.* at note 2, item 57 -59
[31] *Op.cit.* at note 2, item 60-61
[32] *Op.cit.* at note 2, item 63- 64
[33] *Op.cit.* at note 2, item 65-67
[34] *Op.cit.* at note 2, item 68
[35] *Op.cit.* at note 2, item 29
[36] *Op.cit.* at note 2, item 28

4. Implications of CJEU judgment

4.1. Legal uncertainty

Telecom operators from EU member states which had implemented national data retention legislation following enactment of DR Directive and did not assess and/ or annul and/or amend their national legislation with the CJEU judgment, are in uncertain legal situation. Namely, national data retention legislation was not automatically annulled by CJEU judgment. Therefore, if telecom operators continue with data retention they are in risk of breaching EU data retention law as set by CJEU judgment, thus imposing themselves to lawsuits from data subjects (customers whose data are being retained). On the other hand, if telecom operators cease with data retention, they are at risk of breaching national data retention laws, thus imposing themselves to high administrative penalties prescribed for breach of national data retention obligation[37]. It could be argued that legal uncertainty can be acceptable to some extent in specific situation such is this one. Specific situation refers primarily to the fact the a) DR Directive is declared invalid, thus with *ex tunc* effect (instead of e.g. being repealed by another regulation providing for transposition period), and even more to the fact b) that data retention *per se* was not declared as incompliant with EU law, leaving maneuver space for EU member states to stick to national data retention laws by claiming or relying that these are not incompliant with EU law, as will be further discussed in 4.2.3. of this paper. However, legal uncertainty should not be acceptable for long(er) time (cca 7 months have passed since CJEU judgment) nor with respect to sensitive issues such as this one, where serious interference with fundamental rights is in question.

Having in mind the aforementioned risks to telecom operators' decision on whether to comply with (textual interpretation of) national legislation or not, their situation can be assessed as "loose-losse" situation. Nevertheless, without undermining the problem of legal uncertainty, at the end of any of possible procedures which might be initiated against telecom operators, it is not likely that telecom operators would be found responsible for choosing either of two solutions, but rather EU member states which are obliged to align their national legislation with EU law, including with CJEU decisions[38]. Therefore, and also due to the prevailing legalistic approach, it is not surprising that most of telecom operators chose (in some countries relevant authorities were explicitly demanding from operators to continue with data retention) to comply with particular national data retention legislation (usually regulated by electronic communications acts), instead

[37] For example, according to article 119 of the Croatian Electronic Communications Act (Official Gazette 73/2008, 90/2011, 133/2012, 80/2013,71/2014) failure to retain data is deemed as a serious violation of the Act with fines from 100.000,00 up to 1.000.000,00 HRKN (up to cca 130.000,00 Euros). Also, this violation may result in the imposition of a safeguard measure consisting of the prohibition of performance of activities for a period ranging from three months to one year in case.

[38] Article 4 of the Treaty on European Union (TEU)

of with CJEU judgment. Only Swedish telecom operators (Telia, Tele2, Three and Bahnhof[39]) announced to have stopped with data retention based on CJEU judgment, notwithstanding Swedish national data retention legislation. Adding to the controversy of the issue, Swedish internet service provider Bahnof even reported itself to national postal and telecoms regulator for breaking the national Law on Electronic Communications[40]. In some countries (e.g. Croatia) operators are active players openly and continuously urging national authorities to assess the national data retention legislation and to align it with CJEU judgment, as soon as possible. According to the Cullen International EU briefing document[41], so far only minority of EU member states have annulled national data retention legislation following CJEU and these were Austria, Slovenia, Romania and Slovakia, whereas German national data retention legislation was already found unconstitutional in 2010 on the grounds of breach of proportionality principle. Furthermore, four EU member states have assessed their data retention legislation following CJEU judgment – Denmark and UK have amended their national data retention legislation and in Belgium and Sweden the existing laws have been declared as compatible with the CJEU judgment. Consequences of national data retention legislation annulments are both that new data are not being retained plus destruction of already retained data (with exception of Slovakia where no destruction of already retained data is required).

Besides legal uncertainty for telecom operators, it goes without saying that there is legal uncertainty for customer, so called data subjects, whose data are being retained by telecom operators based on national data retention legislations.

4.2. Existence of valid legal basis for data retention following CJEU judgment

DR Directive was declared invalid by CJEU judgment, thus with *ex tunc* effect[42]. Furthermore, annulment of DR Directive does not automatically annul national data retention legislations which were enacted based on DR Directive. Furthermore, the fact that "only" DR Directive was declared invalid, but data retention *per se,* although interfering with fundamental rights, was found to be in compliance with EU legislation, added to the complexity of the issue[43]. This fact

---

[39] Liam Tung, *For of Sweden's telcos stop storing customer data after EU retention Directive overthrown*, 11.4.2014., the article is available on-line at http://www.zdnet.com/four-of-swedens-telcos-stop-storing-customer-data-after-eu-retention-directive-overthrown-7000028341/ , last day accessed on 7.11.2014

[40] Telecompaper, *Bahnhof reports itself for breaking law on data retention*, 8.7.2014., the article is available on-line at http://www.telecompaper.com/news/bahnhof-reports-itself-for-breaking-law-on-data-retention--1024203, last day accessed on 7.11.2014.

[41] *Op.cit.* at note 25

[42] Consolidated version of the Treaty on the Functioning of the European Union, Official Journal C 326, 26.10.2012, pp. 47–390 Article 264 paragraph 1

[43] It should not be concluded that this finding about acceptability of data retention *per se* is surprising at all, as data retention is mostly seen as necessary tool for combating crime purposes, even more today in increasingly digital world.

provides maneuver space for EU member states to stick to national data retention laws by claiming or relying that their national data retention laws are not contrary to CJEU judgment. Most EU member states still have national data retention obligation in place and most telecom operators are still retaining data. The question therefore arises what are the legal bases for data retention today when DR Directive does not exist anymore?

The answer to this question is not clear due to at least three reasons: 1) purposes for data retention which are essential for any interpretation of data processing legal bases are not clear (4.2.1.), b) EU legislation generally lacks crucial definitions of terms of data retention purposes (e.g. definition of "serious crime") (4.2.2.) and c) it is not entirely clear in which situation and/or to what extant is data retention excluded or exempted from the scope of EU data protection law (or even EU law in general)(4.2.3.). Without intention to provide final answer to these questions which would go beyond this paper and would require in-depth analysis, these questions are posed to refer to unclear situation with respect to legal basis for data retention, but also the problems of legal bases in data protection and relation between data protection and specific data processing purposes in general.

4.2.1. Purposes for data retention, which are essential for any interpretation of data processing legal bases, are not clear

In determining legality of any data processing activity one of the main elements is determining the purpose for which particular data are being processed[44]. For example it is allowed and necessary for mobile telecom operator to process communication data (e.g. calling number and receiving number, duration of call, time of call, location - so called traffic data) in order to enable communication between two persons via mobile phone (purpose: performance of contract for mobile services). On the other hand, the same communication data/traffic data are not allowed to be used for marketing and sales purposes without customer consent[45]. This is entirely different purpose and therefore the new legal bases, in this case consent, must be applicable.

The purposes of data retention in the annulled DR Directive were the *investigation, detection and prosecution of serious crime*, as defined by each EU member state in the national law (article 1 paragraph 1). On the other hand article 15 paragraph 1 of the e-Privacy Directive extends the scope of purposes for which data retention can be imposed; *to safeguard national security (i.e. State security), defense, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic*

---

[44] One of the main data protection principles is therefore purpose limitation; "*Member States shall provide that personal data must be collected for specified, explicit and legitimate purposes and not further processes in a way incompatible with those purposes*." *Op.cit.* at note 19, article 6 paragraph 1 item b

[45] *Op.cit.* at note 37, article 102 paragraph 3

communication[46]. As mentioned before in this paper, this provision of e-Privacy Directive was amended by DR Directive (article 11) by excluding its applicability to data specifically required by DR Directive[47]. Anyhow, this exclusion does not exist anymore after DR Directive, including its article 11, was declared invalid. Furthermore, although data retention is not explicitly mention as a measure, Data Protection Directive provides for possibility for Member States to adopt measures restricting certain provision of this directive for *inter alia* purposes of *national security, defense, public security and prevention, investigation, prosecution of criminal offences* (article 14 para1 item a)-d). Also proposal of the new EU data protection framework, called General Data Protection Regulation[48], provides for possibility for EU or EU member states' laws to restrict certain rights and obligations of this regulation for purposes of *public security, the prevention, investigation, detection and prosecution of criminal offences* (article 21 paragraph 1 item a-b).

Following the above it can be concluded that purposes for imposing data retention measure are differently defined in applicable and proposed EU legislation. Therefore, assessing validity of particular data retention will very much depend on the particular purpose for which the data are being retained in each particular case and on the interpretation of different EU legislation.

4.2.2. EU legislation generally lacks crucial definitions of data retention purposes

In addition to differentiation with respect to purposes for data retention between different EU legislation as described under 4.2.1. above, the definitions of

---

46 "*Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union*."

47 Interestingly enough, this exclusion relates only to data defined by DR Directive and not to particular purpose. Therefore, at least theoretically, this can be interpreted that other customer data, besides those define by DR Directive, could be processed for the same purposes as stated in DR Directive or for other purposes as stated in article 15 paragraph 1 of the e-Privacy Directive.

48 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 2012/0011 (COD), 25.1.2012, the document is available on-line at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf , last day accessed on 13.11.2014.

certain terms of purposes are not clear or precise enough. For example, the definition of serious crime (which was left explicitly by DR Directive to EU member states to determine) varies between countries. Even more, according to the Evaluation Report on the Data Retention Directive, some countries have broadened the applicability of data retention to all criminal offences[49]. Thus, there is a need for more harmonization and clarity with respect to defining terms of each data retention purpose (what is meant by each purpose, its scope and limitations).

4.2.3. It is not clear in which situation and/or to what extant is data retention excluded or exempted from the scope of EU data protection law (or even EU law in general)

Question of determining legal bases for data retention today when DR Directive does not exist, presupposes first answering a question whether data retention is a) entirely excluded from the scope of EU data protection regulation or even EU law (4.2.3.1.) or b) only application of certain provisions form EU data protection regulation is restricted with respect to data retention (4.2.3.2.). Final answers to these questions would require in-depth analysis and clarification of each particular purpose of data retention, as mentioned ad. 4.2.1. and 4.2.2. above, as well as analysis of each national legislation on the issue and in particular its more or less complex relations to EU law, which again goes beyond this papers. Therefore, I would provide only part of argumentation with respect to a) and b) approach, based on existing and newly proposed EU data protection legislation in order to demonstrate the lack of clarity.

In favor of a) approach both article 1 paragraph 3 of e-Privacy Directive and article 3 paragraph 2 of Data Protection Directives have to mentioned, because these provisions are explicitly excluding activities which fall outside the scope of Community law, including public security, defense, State security and the activities of the State in areas of criminal law. Furthermore, article 2 paragraph 2 of the proposed General Data Protection Regulation excludes from the scope of this regulation processing of data which falls outside the scope of Union law, in particular national security, and for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties[50]. Nevertheless, it is important to emphasize, that even if all or certain aspects of data retention (access to retained data, that is surveillance) are not subject to EU law, following in particular national security exemptions, according to opinion of the Article 29 Data Protection Working Party *" (...) data protection*

---

[49] For information about various national regulation on purposes of data retention please the *Evaluation Report on the Data Retention Directive*, *Op.cit* at note 10, pp. 6-9.

[50] Interestingly, e.g. Croatian Data Protection Law (Official Gazette No. 103/2003, 118/2006, 41/2008, 130/2011) does not recognize exclusion of the provision of this law with respect to data processing for purpose the same or similar to those in Data Protection Directive, although Data Protection Directive was transposed into this law. Nevertheless, application of data protection regulation (in particular Data Protection Law) is excluded by the Croatian Electronic Communications Act, article 108 paragraph 4

principles following the European Convention on Human Rights and Council of Europe Convention 108 on the protection of personal data will for the most part still need to be respected by intelligence services in order to lawfully perform these duties. These principles are oftentimes also included in the national constitutions of the Member States."[51].

Grounds in favor for b) approach, according to which EU data protection law would be applicable to data retention in general and only application of certain provision of EU data protection law would be restricted, can be found already in the same legislation, but in different provisions. Namely, according to article 15 paragraph 1 of the e-Privacy Directive Member States are allowed to adopt measures to restrict the scope of the rights and obligations provided in (only) certain provision of this directive for mostly the same purposes which are in article 1 paragraph 3 entirely excluded from the scope of this Directive. The same approach is present in article 13 paragraph 1 of the Data Retention Directive, allowing EU member states to restrict (only) the scope of the obligation and rights provided for in articles 6(1), 10, 11 (1), 12 and 21 (provided the necessity principle is fulfilled). Thus, provision about criteria for making data processing legitimate, that is provision about legal grounds for data processing according to Data Protection Directive (article 7), can not be restricted by these measures. In other words, article 7 of Data Protection Directive applies to data retention and thus opens another complex question which legal base(s) would allow for data retention (consent, public interest or, much more likely, legal obligation imposed on telecom operator)[52]. Similar approach is reconfirmed in the proposal of the General Data Protection Directive (article 21 paragraph 1). Also, European Commission[53] explicitly stated that legal bases for data retention after invalidity of DR Directive can be found in article 15 paragraph 1 of the e-Privacy directive.

In any case, without prejudice what would be the final conclusion for legal bases for data retention (which would again also very much depend on the particular purpose and relation between national legislation and EU law), even if, from data protection perspective less favorable, a) approach would apply, any national legislation which had properly transposed DR Directive into its national legislation can not be in compliance with CJEU judgment and thus should be amended or annulled. This relates at least[54] with respect to data which were

---

[51] *Op.cit*. at note 16, p. 6

[52] According to article 7 of the Data Protection Directive there are six grounds under which personal data may be processed: data subject's consent, performance of a contract, compliance with a legal obligation, protection of the vital interests of the data subject, performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed, legitimate interests.

[53] *Frequently Asked Questions: The Data Retention Directive,* European Commission-MEMO/14/269,8.4.2014. the document is available on-line at http://europa.eu/rapid/press-release_MEMO-14-269_en.htm , last day accessed on 14.11.2014.

[54] With respect to other findings of CJEU judgment about DR Directive to be seriously interfering with EU fundamental rights, without such interference being precisely defined to what is strictly necessary (ad.3 b-e above), assessment of compliance with EU law would very much depend on

regulated to be obligatory retained by telecom operator according to DR Directive. Namely, DR Directive covers all persons, all means of electronic communications and all traffic data without and differentiation, limitation or exception and thus should have been transposed into national legislation in the same way. As stated ad.3. above, such broad regulation according to CJEU judgment is contrary to proportionality principle in the light of article 7, 8 and 52(1) of the Charter of Fundamental Rights of the European Union. Furthermore, in case were national law explicitly states that DR Directive is transposed in that laws, *an argumentum ab absurdo* it can not be concluded that this law is entirely in compliance with CJEU judgment. Furthermore, all national legislation which have imposed essentially the same data retention obligations for at least purposes of prevention, investigation, detection and prosecution of criminal offences (based on article 15 paragraph 1 of e-Privacy Directive or article 13 of Data Protection Directive), as were imposed by DR Directive for purposes of prevention, investigation, detection and prosecution serious crimes, should be, based on *argumentum a maiore ad minus*, amended or annulled to comply with EU law.

4.3. *Ex tunc* and certain other effects of CJEU judgment

DR Directive was declared invalid based on the article 264 paragraph 1 of the Treaty on the Functioning of European Union and thus with *ex tunc* and *erga omnes* effect. *Ex tunc* effect in particular broadens the problematic of the consequences following CJEU judgment because it opens up the question of possible liability towards not only data subject, but also towards telecom operators, in particular those who were obliged to provide data retention entirely on their own expanse, for years of data retention preceding CJEU judgment (in addition to problems relating to the time period after annulment).

Also, CJEU judgment and its interpretation of proportionality principle will influence some other data protection issues in telecom sector such is data retention for billing purposes. Although these purposes are different and thus data processing should be assessed separately, CJEU judgment will nevertheless via interpretation of proportionality principle influence on justification for keeping the billing data for any time longer than is necessary (e.g. in particular with respect to data about communication which was already paid and not disputed).

5. *De lege ferenda*; but only as a *quick- win*

Following the above, adequate regulation of data retention on EU and national level, is demanding task. Therefore, it is not surprising that it has been disputable for many years and that even today, months after CJEU judgment

how these possibilities provide by DR Directive to EU member states were transposed to national legislation. For example, with respect to access rights, if national legislation provides for objective criterion, substantive and procedural conditions which would ensure that competent national authorities have access to retained data and for clearly defined purpose (ad.3 b above), than no alignment with CJEU judgment would be necessary.

(which provided new valuable conclusions about the issue) had been rendered, most of EU member states are still assessing compliance of their national data retention legislation with EU law. This prolongs legal uncertainty which was created after CJEU judgment. As it has been pointed out previously in this paper, legal uncertainty should not be acceptable for long(er) time nor with respect to sensitive issues such as this one, where serious interference with fundamental rights is in question. To that respect, before conducting overall assessment of national data retention legislation and deciding on comprehensive national data retention solutions which would be in compliance with EU law, national legislator should think of possible *quick-win* solution in the meantime. Namely, the legislator could, based on its assessment so far, amend its data retention legislation in an express procedure and with limited time period. This was essentially done by UK legislator, which had, following CJEU judgment, annulled its 2009 data retention regulation transposing DR Directive, and passed Data Retention Investigatory Powers Act 2014 with so called sunset-clause, meaning that parliament will need to pass a new law before the act it automatically repealed on December 31th 2016. The other, at least theoretical solution, which is not likely in practice though, would be to refrain from data retention in the meantime, and therefore to annul data retention legislation which had properly transposed DR Directive and with that respect can not be in compliance with EU law at least with respect to amount of data subject to data retention (as explained ad.4.2.3.above).

6. Concluding remarks

Respect for private and family life and protection of personal data is in most cases entirely contrary to purposes or objectives of data retention, notwithstanding the exact purpose in question. Data retention is mostly, with more or less arguments, recognized as a necessary tool for, generally speaking, crime combating purposes, even more so in todays' increasingly digital world. This was again reconfirmed in CJEU judgment invalidating DR Directive and providing new valuable conclusions on this issue. Therefore, it is crucial how the balance between these contrary requirements will be struck, both on EU and national level, after this so called historical CJEU judgment. It seems that current attitude of EU member states with respect to this new situation varies from active involvement, over *wait to see* approach, till denying CJEU judgment and applying clearly legalistic approach. Actually, overall impression about data retention EU at the moment could be described as hectic. However, it is clear that comprehensive assessment and solution for reaching this balance and adequately regulating data retention is complex and interdisciplinary. It will very much depend on interpretation of purposes and legal bases for data retention, which are not clear nor harmonized enough, as well as on interpretation of EU law supremacy doctrine. Hopefully, "new" European Commission which had just started its five years mandate this November, will finalize new EU data protection regulation in 2015 as announced, and thus help in regulating data retention issue. In the meantime, national legislators should think of quick-win solutions, based on UK model.

Bibliography

1. Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others, 8.4.2014.,Court of Justice of EU, InfoCuria - Case-law of the Court of Justice, the document is available on-line at http://curia.europa.eu/juris/liste.jsf? num=C-293/12#, last day accessed on 13.11. 2014.
2. 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, Official Journal of the European Union L 195, 13.4.2006.
3. Directive of European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, Official Journal of the European Union L 24, 30.1.1998.
4. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal of the European Union L 201, 31.7.2002., pp. 0037-0047 as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, Official Journal of the European Union L 337, 18.12.2009.
5. European Commission, *Report from the Commission to the Council and the European Parliament; Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)*, Brussels, 18.4.2011., COM (2011) 225 final, the document is available on-line at http://ec.europa.eu/commission_2010-2014/malmstrom/pdf/archives_2011/ com2011_225_data_retention_evaluation_en.pdf , last day accessed on 13.11. 2014.
6. Gumzej Nina, *Zaštita podataka u elektroničkim komunikacijama; doktorska disertacija,* Sveučilište u Zagreb, Pravni fakultet u Zagrebu, 5.9.2011.
7. Article 29 Data Protection Working Party, *Opinion 04/214 on surveillance of electronic communications for intelligence and national security purposes*, 819/14/EN, WP215, 10.4.2014., the document is available on-line at http://www.cnpd.public.lu/fr/ publications/groupe-art29/wp215_en.pdf, last day accessed on 13.11.2014.
8. Case of Malone v. the United Kingdom, 2.8.1984., European Court of Human Rights, the document is available on-line at http://hudoc.echr.coe.int/sites/eng/pages/ search.aspx?i=0 01-57533#{"itemid":["001-57533"]}, last day accessed on 13.11.2014.
9. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 pp. 0031 – 0050

10. European Parliament, *Report on the First report on the implementation of the Data Protection Directive (95/46/EC) (COM(2003) 265 – C5-0375/2003 – 2003/2153(INI)),* final A5-0104/2004, 25.2.2004., p. 9, item 18, the document is available on-line at http://ec.europa.eu/justice/policies/privacy/docs/lawreport/ep_report_cappato_04_en. pdf, last day accessed on 13.11.2014.
Article 29 Data Protection Working Party*, Opinion 5/2002 on the Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 September 2002) on mandatory systematic retention of telecommunication traffic data*, 11818/02/EN/Final, WP 64, 11.10.2002.
11. Article 29 Data Protection Working Party*, Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with* the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005, 1868/05/EN, WP 113, 21.10.20015.
12. Article 29 Data Protection Working Party*, Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive,* 00068/10/EN, WP 172, 13.7.2010
13. Cullen International, *Annulment of the Data Retention Directive-consequences for national laws*, EU briefing document, 30.7.2014
14. Charter of Fundamental Rights of the European Union (200/C 364/01), Official Journal of the European Communities, 18.12.2000
15. Zakon o elektroničkim komunikacijama (Narodne novine 73/2008, 90/2011, 133/2012, 80/2013,71/2014)
16. Zakon o zaštiti osobnih podataka (Narodne novine 103/2003, 118/2006, 41/2008, 130/2011)
17. Consolidated version of the Treaty on the Functioning of the European Union, Official Journal C 326, 26.10.2012, pp. 47–390
18. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 2012/0011 (COD), 25.1.2012., the document is available on-line at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_ en.pdf, last day accessed on 13.11.2014.
19. European Commission, *Frequently Asked Questions: The Data Retention Directive,* MEMO/14/269,8.4.2014. the document is available on-line at http://europa.eu /rapid/press-release_MEMO-14-269_en.htm, last day accessed on 14.11.2014.
20. Liam Tung, *For of Sweden's telcos stop storing customer data after EU retention Directive overthrown*, 11.4.2014, the article is available on-line at http://www.zdnet.com/four-of-swedens-telcos-stop-storing-customer-data-after-eu-retention-directive-overthrown-700002 8341/, last day accessed on 7.11.2014.
21. Telecompaper, *Bahnhof reports itself for breaking law on data retention*, 8.7.2014., the article is available on-line at http://www.telecompaper.com/news/bahnhof-reports-itself-for-breaking-law-on-data-retention--1024 203, last day accessed on 7.11.2014.