**31st International Scientific Conference on Economic and Social Development –**

**“Legal Challenges of Modern World”** –Split, 7-8 June 2018

**DATA RETENTION IN THE FIELD OF TELECOMMUNICATIONS – PRIVACY AND ELECTRONIC COMMUNICATIONS DIRECTIVE IN THE RECENT CJEU JURISPRUDENCE AND ITS IMPACT ON FIGHTING ECONOMIC CRIME**

**Matko Pajcic**

*University of Split, Faculty of Law*

*mpajcic@pravst.hr*

***ABSTRACT***

*Data retention law is of great significance in fighting crime. Each communication via electronic devices leaves certain traces; most important of them are traffic and location data. These data can be used by law enforcement agencies to identify suspects of the crime, or to check credibility of statements of defendants of witnesses in criminal proceedings, or, generally, gather evidence for court proceedings. Legal regulation of this area of data retention in European Union, where interest of fighting crime and public safety confronts with the right to privacy and the right to protection of personal data, is one of the most debated topics, and therefore it is no wonder that Court of Justice of European Union (CJEU) in its jurisprudence met several very important decisions, among others Digital Rights Ireland & Seitlinger and Ors (joined cases C-293/12 and C-594/12) in 2014. and Tele2/Watson (joined cases C-203/15 and C-698/15) in 2016. These cases deal with application of certain important provisions of Privacy and Electronic Communications Directive1 and some other EU Directives. In the last judgment in Tele2/Watson case, the Grand Chamber of European Court of Justice determined that Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union. Althought the aforementioned judgments of CJEU set some mandatory requirements, the national legislators still have difficult task regulating this sensitive legal area.*

***Keywords:*** *right to respect for private life, protection of personal data, data retention, traffic**data, location data, European Union, Court of Justice of European Union*

**1. INTRODUCTION**

Data retention law is of great significance in fighting crime. Each communication via electronic devices leaves certain traces; most important of them are traffic and location data. These data can be used can be used by law enforcement agencies, or national security bodies to identify suspects of the crime, or to check credibility of statements of defendants of witnesses in criminal proceedings, or, generally, gather evidence for court proceedings. More types of this data, retained in longer period of time, can reveal a lot about private life of individual, his habits, social circle, etc. Legal regulation of this area of data retention in European Union, where interest of fighting crime and public safety confronts with the right to privacy and the right to protection of personal data, is one of the most debated topics, and therefore it is no wonder that

1. 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 L 201 , 31/07/2002 P. 0037 - 0047

277

**31st International Scientific Conference on Economic and Social Development –**

**“Legal Challenges of Modern World”** –Split, 7-8 June 2018

Court of Justice of European Union (CJEU) in its jurisprudence met several very important decisions, among others Digital Rights Ireland & Seitlinger and Ors (joined cases C-293/12 and C-594/12) in 2014. and Tele2/Watson (joined cases C-203/15 and C-698/15) in 2016. These cases deal with application of certain important provisions of Privacy and Electronic Communications Directive2 and some other EU Directives.

**2. EUROPEAN UNION LEGISLATION**

**2.1. Charter of Fundamental Rights of the European Union**

Respect for private and family life is guaranteed in art. 7. of Charter of Fundamental Rights of the European Union (further: Charter) and many other human rights documents. However, neither of these documents provides a definition of privacy, mostly because defining privacy is quite difficult task (Tzanou, M. (2017), p. 8). The provision of art. 7. Contains, beside the right to respect for private and family life, right to respect home and communications. Unlike European Convention on Human rights, one very important aspect of the right to respect for private life is in Charter considered as separate basic human right. It is right to protection of personal data (art. 8).3 The Charter is the first supra-national document recognizing the right to protection of personal data separately from the right to respect for private life (Gonzáles Fuster, G. (2014) p. 199). The Charter in art. 8. contains not only general provisions on the right to the protection of personal data, but also obligation that such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Regarding the right of access to retained data, the Charter states that everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified and that compliance with these rules shall be subject to control by an independent authority. Although art. 7 and art. 8, as described above, at he first glance are the only one that we should consider when discussing Charter provisions in this aspect, one more very important right should also be mentioned. Art. 11. guarantees the right to freedom of expression, that includes freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. Every time when we consider actual scope of some right or principle from Charter, it is inevitable to interpret art. 52. of Charter. According to this provisions of Charter, any limitation on the exercise of the rights and freedoms recognised by the 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 European Union or the need to protect the rights and freedoms of others.

**2.2. Privacy and Electronic Communications Directive**

Privacy and Electronic Communications Directive, known as ePrivacy Directive 2002, is the most important source of EU law dealing with protection of privacy of electronic communications of EU citizens. The scope and aim of Directive is to harmonize the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and

1. 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 L 201 , 31/07/2002 P. 0037 - 0047
2. It is understandable regarding the fact that European Convention on Human Rights was drafted in 1950, and Charter of Fundamental Rights of the European Union half of century later, considering the development of international law on human rights in the second half of 20th century. Busser analyzed the judicature of European Court of Human Rights and claims that a clear link between the right to privacy and the right to protection of personal data is finally made in 2000 (Amman v. Switzerland, EctHR, $ 65). Busser, E. D. (2009), p. 48-49.

278

**31st International Scientific Conference on Economic and Social Development –**

**“Legal Challenges of Modern World”** –Split, 7-8 June 2018

of electronic communication equipment and services in the Community (art 1. par. 1.). This Directive was amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009. Directive guarantees several very important rights. Confidentiality of the communications, (art. 5) is one of most important ones for the protection of personal privacy. In this article the Directive creates obligation for member states to ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1) of this Directive. Important provisions of ePrivacy directive can further be found in art. 6. (traffic data), art. 8. (presentation and restriction of calling and connected line identification) and art. 9. (location data). The most important article, regarding the collecting of evidence for the purpose of criminal proceedings , is art. 15. par. 1 which provides that 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.

**2.3. Data Retention Directive4**

In 2006. European Union brought Data Retention Directive, which imposed general obligation to member states to store citizens' telecommunications data to longer periods of time (from 6 to 24 months - articles 3 and 6) It is common assumption that it was at least partially consequence of terroristic attacks in Madrid and London in 2004. and 2005. Approach to stored data for police, criminal prosecution and security agencies was subject to previous judicial approval. This Directive was declared invalid by Court of European Union in the judgment in case Digital Rights Ireland.5 Beside Charter and above mentioned Directives, there are other very important sources of European Union Law regulating conditions of usage of retained data for the purpose of fighting crime, such as „Law Enforcement Directive“ 2016/6806 and Europol Regulation 2016,7 but we will not elaborate it here because it is not focus of the article.

**3. JUDGMENTS OF THE COURT OF THE EUROPEAN UNION**

Court of the European Union dealt with the content of aforementioned directives in several cases, most important of them being Digital Rights Ireland and Seitlinger and others in 2014. and Tele2/Watson in 2016.

1. 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
2. See *infra* 3.1.
3. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent author ities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA .
4. Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for law enforcement cooperation (Europol Regulation) [2016] OJ L 135/53. This Regulation entered into force on the 1 May 2017, and it brings very important changes – most important of them regarding data protection is that, as Coudert emphasizes, the principle of purpose limitation is not implemented anymore through the so-called 'silo-based approach - the focus of the Regulation is not on databases but on data processing operations. Coudert, F. (2017), The Europol Regulation and Purpose Limitation: From the Silo Based Approach to What Exactly, 3 Eur. Data Prot. L. Rev. 313 p. 313.

279

**31st International Scientific Conference on Economic and Social Development –**

**“Legal Challenges of Modern World”** –Split, 7-8 June 2018

**3.1. Digital Rights Ireland and Seitlinger and Others**

In its judgment in the case Digital Rights Ireland and Seitlinger and others8 the Court of Justice of the European Union (henceforth: CJEU or the Court) declared the Data Retention Directive to be invalid. CJEU stated that the obligation imposed by Articles 3 and 6 of Directive 2006/24 on providers of publicly available electronic communications services or of public communications networks to retain, for a certain period, data relating to a person’s private life and to his communications, such as those referred to in Article 5 of the directive, constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter of fundamental human rights of the EU. (par. 34). CJEU pointed that Directive 2006/24 constitutes an interference with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter because it provides for the processing of personal data. It concluded that such interference with the fundamental rights laid down in Articles 7 and 8 of the Charter must be considered to be particularly serious. Furthermore, the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance (par. 36. -37.). CJEU then provided interpretation of above mentioned provisions of art. 52. par. 1. of the Charter. Regarding the subject of this article, and possibility of data retention for the purpose of fighting crime, par. 42. must be cited: „It is apparent from the case-law of the Court that the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest... The same is true of the fight against serious crime in order to ensure public security... Furthermore, it should be noted, in this respect, that Article 6 of the Charter lays down the right of any person not only to liberty, but also to security.“ Regarding the question of whether the retention of data is appropriate for attaining the objective pursued by Directive 2006/24, CJEU wrote that it must be held that, having regard to the growing importance of means of electronic communication, data which must be retained pursuant to that Directive allow the national authorities which are competent for criminal prosecutions to have additional opportunities to shed light on serious crime and, in this respect, they are therefore a valuable tool for criminal investigations. Consequently, the retention of such data may be considered to be appropriate for attaining the objective pursued by that directive (par. 49). As regards the necessity for the retention of data required by Directive 2006/24, CJEU admitted that it must be held that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight. So far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court’s settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (para. 51.-52.). Digital Rights Ireland judgment had great impact, not only in European Union.9

1. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General,intervener: Irish Human Rights Commission (C-293/12), and Kärntner Landesregierung Michael Seitlinger, Christof Tschohl and others (C-594/12), (Judgment in joined cases C - 293/12 and C - 594/12).
2. See. e.g. Vainio, N., Miettinen, S., (2015) Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States, *International Journal of Law and Information Technology, Volume 23, Issue 3,* September 2015, (p. 290), Granger, M. - P., K. Irion. K. (2014) The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection, European Law Review 39, no.
3. (p. 835) and for influence outside Europe: Fabbrini, F. (2015) Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States, 28 Harv. Hum. Rts. J. (p. 65). and Park, H.-Y. (2015) The Invalidation of the EU Data Retention Directive and its Implication for Korea, *Dongguk Law Review, vol. 6.* (p. 55.).

280

**31st International Scientific Conference on Economic and Social Development –**

**“Legal Challenges of Modern World”** –Split, 7-8 June 2018

Although it left some very important question unresolved and unclear (see e.g. Opinion of Advocate General Saugmandsgaard Øe in Joined Cases C-203/15 and C 698/15, pr. 189.), it influenced numerous changes of national legislations, and led to action of one Swedish provider, Tele2, which caused the CJEU judgment in Tele2/Watson case we will discuss now.

**3.2. Tele2/Watson**

In Tele2/Watson case,10 CJEU had to decide if Swedish and UK legislation were compliant to EU law, namely compliant to ePrivacy Directive 2002 as amended by Directive 2009/136/EC, read in the light of Articles 7 and 8 and Article 52(1) of the Charter of Fundamental Rights of the European Union. Swedish and UK law contained provisions that imposed data retention for certain period of time, more precisely imposed obligation for electronic communication providers to retain traffic and location data. Given the seriousness of the interference in the fundamental rights concerned represented by national legislation which, for the purpose of fighting crime, provides for the retention of traffic and location data, CJEU emphasized that only the objective of fighting serious crime is capable of justifying such a measure (par. 102.).11 Further, while the effectiveness of the fight against serious crime, in particular organized crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight (par. 103.). It is further explained why is such general data retention unacceptable; CJEU stated that national legislation such as that at issue in the main proceedings, which covers, in a generalised manner, all subscribers and registered users and all means of electronic communication as well as all traffic data, provides for no differentiation, limitation or exception according to the objective pursued. It is comprehensive in that it affects all persons using electronic communication services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious criminal offences (par. 105).12 The problem with such legislation is that it does not require there to be any relationship between the data which must be retained and a threat to public security. In particular, it is not restricted to retention in relation to (i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to fighting crime. Therefore, such national legislation exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society (para 106.-107). However, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited with respect to four main criteria, or prerequisites, that CJEU built.

1. Tele2 Sverige AB (C 203/15) v Post- och telestyrelsen, and Secretary of State for the Home Department (C 698/15) v Tom Watson, Peter Brice, Geoffrey Lewis, joined case, judgement of 21 December 2016.
2. The Court accepted the opinion of Advocate General *Saugmandsgaard Oe* regarding the difference between ordinary and serious crime when it comes to data retention. Calomme (in article written before court judgement in this case, analysing

Advocate General's opinion, warned that „if the Court decides to follow the Advocate General, it should also specify whether 'serious crime' must be given an autonomous meaning or whether it should follow the meaning given in national law.“

Calomme, C. (2016) Strict Safeguards to Restrict General Data Retention Obligations Imposed by the Member States, 2 Eur. Data Prot. L. Rev. 590 p. 594.

1. Additional problem is professional secrecy – the Court wrote that such general data retention obligation does not provide for any exception, and consequently it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.

281

**31st International Scientific Conference on Economic and Social Development –**

**“Legal Challenges of Modern World”** –Split, 7-8 June 2018

Eventual data retention hence must be limited to what is strictly necessary with respect to 1) with respect to the categories of data to be retained, 2) the means of communication affected,

1. the persons concerned and 4) the retention period adopted. CJEU imposed obligation to member states - in order to satisfy the requirements, the national legislators must, first, lay down clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse (par. 109). It is also very important to emphasize that CJEU confirmed (phrase: „it is essential“ was used) the principle that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime. Additional very important parts of Tele2/Watson judgment that, in my opinion, should be emphasized are 1) the obligation of the competent national authorities to whom access to the retained data has been granted to notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities, 2) the right of persons affected to a legal remedy, expressly provided for in Article 15(2) of Directive 2002/58, read together with Article 22 of Directive 95/46, where their rights have been infringed, and 3) the data concerned should be retained within the European Union (ruling that is very important regarding international police and judicial cooperation in criminal matters).To summarize, CJEU ruled that Article 15(1) of ePrivacy Directive 2002, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication. Therefore, that provisions must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union (par. 134.)

**4. CONCLUSION**

Approach to retained traffic and location data can certainly be very useful tool for finding perpetrators and collecting evidences in fighting crime. Organized economic crime, in some cases, regarding the amount of money that is dealt with, or the size of the company involved, can have devastating effect not only for individuals, but also for large companies and in some cases even for whole economy of some smaller countries.13 Therefore in such cases it should without doubt be considered as „serious crime“ in terms of CJEU judgments.14

1. There are situations where some large companies or concerns represent significant part of nation's economy (quantified in % of BDP), and therefore criminal activity in connection with such large entities can have negative effect on whole country.
2. CJEU judgement in Taricco case of 5. December 2017. is perfect illustration of the significance of serious organized economic crime, in this case VAT fraud. CJEU ruled that „Article 325(1) and (2) TFEU must be interpreted as requiring the national court, in criminal proceedings for infringements relating to value added tax, to disapply national provisions on limitation, forming part of national substantive law, which prevent the application of effective and deterrent criminal penalties in a significant number of cases of serious fraud affecting the financial interests of the European Union, or which lay down shorter limitation periods for cases of serious fraud affecting those interests than for those affecting the financial interests of the Member State concerned, unless that disapplication entails a breach of the principle that offences and penalties must be

282

**31st International Scientific Conference on Economic and Social Development –**

**“Legal Challenges of Modern World”** –Split, 7-8 June 2018

After CJEU 2014. judgment Digital Rights Ireland declared Data Retention Directive invalid, situation in Europe could be described as heterogeneous.15 Tele2/Watson judgment has clarified some confusion around the proper interpretation of the Digital Rights case - specifically, it has clarified confusion concerning whether EU law allows for the generalised retention of personal data and determined extended mandatory requirements or measures that allow for the retention of personal data and its accessing by public bodies (Mbioh, R., W. (2017) p. 281-282). Yet, some European countries still have „old“ rules which impose general and indiscriminative retention of traffic and location data, what must be considered as breach of basic human rights guaranteed in the Charter. While Constitutional and other courts in some countries declared such provisions contrary to constitutions, some other countries still wait for common European frame and legislation to be adopted into national legislation systems.16 But, it seems that European Union is not willing to take the lead in regulating tasks this time (Munir, A., B., Yasin, S., H., M., Bakar, S., S., A. (2017), p. 83). As stated in Tele2/Watson case judgment, national legislators must, first, lay down clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. Therefore, it is slippery ground for national regulators, which have to be very careful and have to take into account many different elements, from the interests of national security and fight against terrorism and other serious crime to the right to private life and right to protection of personal data.

***ACKNOWLEDGMENT:*** *This article is result of research in the frame of scientific project*

*„Croatian Judicial Cooperation in Criminal Matters in the EU and the Region: Heritage of the Past and Challenges of the Future (CoCoCrim)" funded by Croatian Science Foundation.*

**LITERATURE:**

1. Blasi Casagran C. (2017) Global Data Protection in the Field of Law Enforcement: An EU Perspective, Routledge.
2. Busser, E. D. (2009) Data Protection in EU and US Criminal Cooperation: A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters between Judicial and Law Enforcement Authorities, Maklu Publishers.
3. Calomme, C. (2016) Strict Safeguards to Restrict General Data Retention Obligations Imposed by the Member States, *2 Eur. Data Prot. L. Rev.* (p. 590).

defined by law because of the lack of precision of the applicable law or because of the retroactive application of legislation imposing conditions of criminal liability stricter than those in force at the time the infringement was committed.

Since significant part of economic crime of larger scale has some international element within, exchange of information between European countries is crucial and unevitable element of investigation in such cases. While cooperation between EU members is mostly regulated and therefore faces less problems, cooperation with other significant partners must also be considered and developed while simultaneously maintaining data protection principles of different legal systems. Especially significant in this aspect is cooperation between EU and United States of America, because of number of big companies and concerns that do business in both continents. See: Busser, E. D. (2009) Data Protection in EU and US Criminal Cooperation: A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters between Judicial and Law Enforcement Authorities, Maklu Publishers.

1. Very important and useful are also judgments of European Court of Human Rights regarding the question if retention of certain data or DNA samples is disproportionate interference with the right to private life from art. 8. of European Convention of Human Rights. See. Kouvakas, I., The Watson Case: Another Missed Opportunity for Stricto Sensu Proportionality, 2

Cambridge L. Rev. 173 (2017), p. 178., where author claims the reasoning of the Strasbourg Court in the case „Adarper v UK' was extensively followed by the Grand Chamber in Digital Rights Ireland.

1. See e.g. for Germany: Etteldorf, C., Higher Administrative Court of Northrhine Westphalia Declares German Data Retention Law Violates EU Law, 3 Eur. Data Prot. L. Rev. 394 (2017), and her comment on problems in period between 2010, when German Constitutional Court had declared unconstitutional German law transposing the Data Retention Directive and 2014. Digital Ireland CJEU judgement.

283

**31st International Scientific Conference on Economic and Social Development –**

**“Legal Challenges of Modern World”** –Split, 7-8 June 2018

1. Charter of Fundamental Rights of the European Union, (2000/C 364/01) 18.12.2000 *Official Journal of the European Communities C 364/1EN*
2. Coudert, F. (2017), The Europol Regulation and Purpose Limitation: From the Silo Based Approach to What Exactly, 3 Eur. Data Prot. L. Rev. (p. 313)
3. 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 L 201 , 31/07/2002 P. 0037 – 0047.
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
5. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA .
6. Digital Rights Ireland, CJEU judgment (2016) Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General,intervener: Irish Human Rights Commission, and Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl and others, (Judgment of CJEU of 8 April 2014).
7. Etteldorf, C. (2017) Higher Administrative Court of Northrhine Westphalia Declares German Data Retention Law Violates EU Law, *3 Eur. Data Prot. L. Rev.* (p. 394).
8. Fabbrini, F. (2015) Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States, 28 Harv. Hum. Rts. J. (p. 65).
9. Gonzáles Fuster, G. (2014) The Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer.
10. Granger, M. - P., K. Irion. K. (2014) The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection, European Law Review 39, no. 4 (p. 835).
11. Kouvakas, I. (2017) The Watson Case: Another Missed Opportunity for Stricto Sensu Proportionality, *2 Cambridge L. Rev.* (p. 173).
12. Mbioh, R., W. (2017) Post-Och Telestyrelsen and Watson and the Investigatory Powers Act 2016, 3 Eur. Data Prot. L. Rev. (p. 273).
13. Munir, A., B., Yasin, S., H., M., Bakar, S., S., A. (2017) Data Retention Rules: A Dead End, 3 European Data Protection Law Review , p 71.
14. Opinion of Advocate General Saugmandsgaard Øe in Joined Cases C-203/15 and C 698/15), delivered on 19 July 2016.
15. Park, H.-Y. (2015) The Invalidation of the EU Data Retention Directive and its Implication for Korea, *Dongguk Law Review, vol. 6.* (p. 55.)
16. Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for law enforcement cooperation (Europol Regulation) [2016] OJ L 135/53.
17. Taricco and Others (2015) CJEU - C-105/14 / Judgment of CJEU (Grand Chamber) of 8 September 2015.

284

**31st International Scientific Conference on Economic and Social Development –**

**“Legal Challenges of Modern World”** –Split, 7-8 June 2018

1. Tele2/Watson (2016) Tele2 Sverige AB (C 203/15) v Post-och telestyrelsen, and Secretary of State for the Home Department (C 698/15) v Tom Watson, Peter Brice, Geoffrey Lewis, joined cases, judgement of CJEU of 21 December 2016.
2. Tzanou, M. (2017) The Fundamental Right to Data Protection: Normative Value in the

Context of Counter-Terrorism Surveillance, Oxford: Hart Publishing.

1. Vainio, N., Miettinen, S., (2015) Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States, *International Journal of* *Law and Information Technology, Volume 23, Issue 3,* September 2015, (p. 290).

285