Striking appropriate balance between metadata retention and right to privacy according to the Article 7 of the CFREU

Andrii Konopko
513438
Law and Information Society
University of Turku
Faculty of Law
November 2019

The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin Originality Check service.

UNIVERSITY OF TURKU
Faculty of Law
ANDRII KONOPKO: Striking appropriate balance between metadata retention and right to privacy according to the Article 7 of the CFREU

Master's thesis, 72 p.
Law and Information Society
November 2019

Metadata retention based on the modern technology capabilities is proven to be an effective tool for the investigation and prevention of crimes. However, this governmental tool if not properly limited can lead to mass surveillance and imposes a grave intrusion into privacy. European metadata retention regime established by the Data Retention Directive (2006-2014) fell with the decision of the CJEU in *Digital Rights Ireland* case. The struggle with understanding how metadata retention can be applied on the national level continues even after the following *Tele2&Watson* case.

Presented master thesis is an effort to analyze what was wrong with Data Retention Directive and a springboard to understanding how to build a national metadata retention framework to be in compliance with the European Union law. The research is based on analysis of privacy and metadata retention as two contradicting issues. The researcher pays thorough attention to Article 7 of the Charter of Fundamental Rights and 2 landmark decisions of the CJEU: *Digital Rights Ireland* and *Tele2&Watson*.

Special emphasis in the work is put on analyzing the conditions which allow limiting the right to privacy by means of metadata retention: objective of general interest, provision by law, respect to the essence of the right to privacy and proportionality of the intrusion. The thesis also focuses on 'what is strictly necessary' limitations with regard to amount of people concerned, categories of data, means of communication affected and time period of retention. The outcome of the research confirms that it is highly possible to build up a national metadata retention law even with the imposed by CJEU limitations.

Keywords: *privacy, data protection, metadata retention, proportionality, Data Retention Directive, Digital Rights Ireland, Tele2&Watson, CFREU, right to privacy, surveillance*

CONTENTS

REFERENCES

OFFICIAL DOCUMENTS

European Convention of Human Rights, 1950

Charter of Fundamental Rights of the European Union, 2000

Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, 2012/C 326/01

Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

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 (Data Protection Directive)

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 (Privacy and Electronic Communications Directive)

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 (Data Retention Directive)

Convention on Cybercrime (ETS No. 185) Budapest, 23/11/2001

UK Regulation of Investigatory Powers Act, 2000

UK Data Retention and Investigatory Powers Act, 2014

UK Explanatory Notes to the Investigatory Powers Act, 2016

Swedish Penal Code, 1962

Criminal Code of Ukraine, 2001

European Arrest Warrant

BOOKS

Bygrave, Lee Andrew, *Data protection law: Approaching its rationale, logic and limits*. Alphen aan den Rijn: Kluwer, 2002.

Kirchberger, Christine, *Cyber law in Sweden*. Alphen aan den Rijn: Kluwer Law International, 2011.

Law, Jonathan, – Martin, Elizabeth A, *A Dictionary of Law* (7thed.), Oxford; New York: Oxford University Press, 2009.

Rule, James B.. *Privacy in Peril : How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience*, Oxford University Press USA - OSO, 2007.

Westin, Alan, *Privacy and freedom 7*, 1967.

Handbook on European Data Protection Law, Edited by European Union Agency for Fundamental Rights and Council of Europe, 2018.

Benkler, Yochai, *The wealth of networks: How social production transforms markets and freedom*. New Haven: Yale UP, 2006.

ARTICLES

Bernal, Paul, *Data gathering, surveillance and human rights: recasting the debate*, Journal of Cyber Policy, 1:2, pp.243-264, 2016.

Cameron, Iain, *Balancing data protection and law enforcement needs: Tele2 Sverige and Watson*, Common Market Law Review 54: pp. 1467–1496, 2017.

Fabbrini, Federico, *Human Rights in digital age, the European Court of Justice Ruling in the Data Retention Case and its lessons for Privacy and Surveillance in the U.S.*, pp.65-95, Harvard Human Right Journal, 2015.

Fennelly, David, *Data retention: the life, death and afterlife of a directive*, ERA Forum, pp. 673-692, 2019.

Flaherty, David H., *On the Utility of Constitutional Rights to Privacy and Data Protection*, 41 Case W. Res. L. Rev. 831 (1991), pp.831-855

Gansterer, Wilfried – Ilger, Michael, *Data Retention – The EU Directive 2006/24/EC from a Technological Perspective*, Wien: Verlag Medien und Recht, 2008.

Kang, Jerry, *Information Privacy in Cyberspace Transactions*, 50 Stanford law review, pp. 1193-1260, 1998.

Kokott, Juliane, – Sobotta, Christoph, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, International Data Privacy Law, 2013, Vol.3, No.4, pp.222-228.

Mbioh, Will R., *Post-och Telestyrelsen and Watson and the Investigatory Powers Act 2016*, European Data Protection Law review, 2/2017, pp. 273-282.

Rauhofer, Judith, *Privacy and surveillance: legal and socioeconomic aspects of state intrusion into electronic communications,* pp.545-575 in Edwards, L. & Waelde, C. *Law and the Internet* (3rd ed.). Oxford : Portland, Or.: Hart. 2009. Rauhofer B

Rauhofer, Judith, *The retention of communications data in Europe and the UK*, pp.575-600 in Edwards, L. &
Waelde, C. *Law and the Internet* (3rd ed.). Oxford : Portland, Or.: Hart. 2009. Rauhofer A

Rivers, Julian, *Proportionality and variable intensity of review*, Cambridge Law Journal, 65(1), 03/2006, pp. 174–207.

Rubenfeld, Jed, *Privacy's end*, pp.207-229 in White, James Boyd, – Powell, H. Jefferson (ed.): *Law and Democracy in the Empire of Force*, University of Michigan Press, 2009.

Simitis, Spiros, *Reviewing Privacy In an Information Society*, 135 U. PA. L. REV. 707 (1987), pp. 707-746.

Solove, Daniel J., *A taxonomy of privacy*, University of Pennsylvania Law Review, Vol. 154, No. 3 (Jan., 2006), pp.477-564.

Swire, Peter P., *Financial Privacy and the Theory of High-Tech Government Surveillance*, 77Wash. U. L.Q. pp.461-512, 1999.

Vainio, Niklas – Miettinen, Samuli, *Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States,* International Journal of Law and Information Technology, Vol. 23, Issue 3, 1 September 2015, pp. 290–309.

Walden, Ian, *Privacy and Data Protection*, pp.573-626 in Reed, C. (ed.): *Computer law* (7th ed.): Oxford University Press, 2011.

Warren, Samuel D. – Brandeis, Louis D, *The Right to Privacy*, pp.193-220, 4 HARV. L. REV. No 5, 1890.

ONLINE ARTICLES

Agrawal, Nina, *There's more than the CIA and FBI: The 17 agencies that make up the U.S. intelligence community*, Los Angeles Times, January 17th 2017, (http://www.latimes.com/nation/la-na-17-intelligence-agencies-20170112-story.html, Accessed: 10th Mar 2019).

Beck, Gunnar, *Case Comment: C-203/15 Tele2 Sverige AB v Post-och telestyrelsen and C-698/15 SSHD v Tom Watson & Others*, Opinion, 13th Jan 2017, (https://eutopialaw.com/2017/01/13/case-comment-cases-c-20315-tele2-sverige-ab-v-post-och-

telestyrelsen-and-c-69815-secretary-of-state-for-the-home-department-v-tom-watson-and-others/, Accessed 1st May 2019).

Benkler, Yochai, *Fact: the NSA gets negligible intel from Americans' metadata. So end collection*, Opinion 8th October 2013, The Guardian, (https://www.theguardian.com/commentisfree/2013/oct/08/nsa-bulk-metadata-surveillance-intelligence, Accessed 27th Mar 2019).

Biermann, Kai, *Betrayed by your own data*, Zeit Online, section Digital, 03/2011, (https://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz, accessed on 27th Mar 2019).

Blaze, Matt. *'Phew, NSA is just collecting metadata (You should still worry)',* Wired Magasine, Opinion, 06/2013, (https://www.wired.com/2013/06/phew-it-was-just-metadata-not-think-again/, Accessed 26th Mar 2019).

Bowden, Caspar, *Closed circuit television for inside your head: blanket traffic data retention and the emergency anti-terrorism legislation*, Duke Law & Technology Review 05/2002, (https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1046&context=dltr, Accessed 26th Mar 2019).

Craig, Paul P., *Proportionality, Rationality and Review*, Oxford Legal Studies Research Paper No. 5/2011, Oxford, UK: University of Oxford, February 2011, (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1756271, Accessed 9th June 2019).

Elliott, Kennedy – Rupar, Terri, *Six months of revelations on NSA*, (https://www.washingtonpost.com/wp-srv/special/national/nsa-timeline/, Accessed 19th Mar 2019).

Feiler, Lukas, The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection, European Journal of Law and Technology, Vol. 1, Issue 3, 2010, (http://ejlt.org/article/view/29/75, Date Accessed: 01st Sep 2019).

Formici, Giulia, *ECJ, the floor is yours! The never ending story between Data Retention and Right to Privacy*, 23 Mar 2019, Opinion in KU leuven, Centre for IT&IP law,

(https://www.law.kuleuven.be/citip/blog/ecj-the-floor-is-yours-the-never-ending-story-between-data-retention-and-right-to-privacy/, Accessed 06th Nov 2019).

Gluhovskiy, Mykhailo, *Intelligence agencies on a way to total control upon Ukrainians*, (Spetssuzbi na shljahu do povnogo kontrolju za ukrajintsjami), Glavcom UA, (https://glavcom.ua/columns/gluhovskiy/123592-spetssluzhbi-na-shljahu-do-povnogo-kontrolju-za-ukrajintsjami.html, Accessed 27th Mar 2019).

Grech, Michael, *Data protection vs. The Right to Privacy*, GVZN Advocates website opinion, (https://www.gvzh.com.mt/malta-law/data-protection/vs-the-right-to-privacy/, Accessed 20th Mar 2019)

Hundt, Reed, *A New Principle of International Law: The Internet Is a Common Medium*, The Aspen Institute blog, World economy, 22 March 2012, (https://www.aspeninstitute.org/blog-posts/new-principle-internatio/, Accessed: 21st Feb 2018).

Lane, Svetlana, *The (potential) Use of Metadata in a Surveillance Operation Conducted by an Intelligence or Law Enforcement Entity within Australia*, 05/2016, (https://www.academia.edu/29043016/The_potential_Use_of_Metadata_in_a_Surveillance_Operation_Conducted_by_an_Intelligence_or_Law_Enforcement_Entity_within_Australia, Accessed on 26th Mar 2019)

Lynskey, Orla, *Joined cases C-293/12 and 594/12 Digital Rights Ireland and Seitlinger and others: the good, the bad and the ugly*, April 8, 2014, (http://europeanlawblog.eu/2014/04/08/joined-cases-c-29312-and-59412-digital-rights-ireland-and-seitlinger-and-others-the-good-the-bad-and-the-ugly/, Accessed: 21st Jan 2019). Lynskey (A)

Lynskey, Orla, *Tele2 Sverige AB and Watson Et al: continuity and radical change*, Opinion, 12th Jan 2017, (https://europeanlawblog.eu/2017/01/12/tele2-sverige-ab-and-watson-et-al-continuity-and-radical-change/, Accessed 1st May 2019). Lynskey (B)

Lynskey, Orla, *Plenty to retain? Opinion of the Advocate General in Joined cases C-293/12 and 594/12, Digital Rights Ireland Ltd and Seitlinger and others*, Opinion 17th Dec 2013, (http://europeanlawblog.eu/2013/12/17/plenty-to-retain-opinion-of-the-advocate-general-in-

joined-cases-c-29312-and-59412-digital-rights-ireland-ltd-and-seitlinger-and-others/, Accessed: 28th Mar 2019). Lynskey (C)

McIntyre, T. J., *Data Retention in Ireland: Privacy, Policy and Proportionality*, Computer Law & Security Review, Volume 24, Issue 4, 2008, pp. 326–334. (https://ssrn.com/abstract=2426208, Accessed: 11th Dec 2018).

Morgan, Lydia, *The DRIP(A) of Watson*, Opinion in SCRIPTed, A Journal of Law, Technology and Society, 02/2018, (https://script-ed.org/blog/the-dripa-of-watson/, Accessed 29th Apr 2019).

Opsahl, Kurt, *Why metadata matters*, Opinion on Electronic Frontier Foundation website, 07 June 2013, (https://www.eff.org/deeplinks/2013/06/why-metadata-matters, accessed 07 Nov 2019).

Owen, Phil, *'Jack Ryan': Do Terrorists Actually Use Video Games to Communicate and Plan Attacks?* Opinion in The Wrap posted on 1st September 2018, (https://www.thewrap.com/jack-ryan-terrorists-actually-use-video-games-communicate-plan-attacks/, Accessed 17th Apr 2019).

Reilly, Claire, *The metadata debate: What you need to know about data retention*, CNET Article, 08/13, 2014, (https://www.cnet.com/news/what-you-need-to-know-about-data-retention/, Accessed 27th Mar 2019)

Thimm, Johannes, *From Exception to Normalcy, The United States and the War on Terrorism*, 10/2018, Stiftung Wissenschaft und Politik, (https://www.swp-berlin.org/fileadmin/contents/products/research_papers/2018RP07_tmm.pdf, Accessed 29th Apr 2019)

Woods, Lorna, *Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber)*, Opinion, 21st Dec 2016, (https://eulawanalysis.blogspot.com/2016/12/data-retention-and-national-law-ecj.html, Accessed 9th Apr 2019).

LEGAL CASES

Europe (CJEU)

Judgment of 8 April 2014, *Digital Rights Ireland*, Joined cases C-293/12, C-594/12, EU:C:2014:238, paragraph

Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others,* Joined Cases C-203/15 and C-698/15, EU:C:2016:970, paragraph

Judgment of 6th October 2015, *Maximillian Schrems v Data Protection Commissioner,* C-362/14, EU:C:2015:650

Judgment of 10th February 2009, *Ireland v Parliament and Council*, C-301/6, EU:C:2009:68

Judgment of 7th May 2009, *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer*, C-553/07, EU:C:2009:293

Judgment of 7th November 2013, *Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert and Others*, C-473/12 EU:C:2013:715

Judgment of 3rd September 2008, *Kadi and Al Barakaat International v Council and Commission,* C-415/05 P, EU: C: 2008:461

Judgment of 23rd November 2010, *Land Baden-Württemberg v Panagiotis Tsakouridis*, C-145/09 EU:C:2010:708

Judgment of 29th January 2008, *Productores de Música de España (Promusicae) v Telefónica de España SAU*, C-275/06, EU:C:2008:54

Judgment of 15th November 2012, *Al-Aqsa v. Council,* Joined cases C 539/10 P and 550/10 P, EU:C:2012:711

Judgment of 29th June 2010, *Commission v Bavarian Lager,* Case C-28/08 P, EU:C:2010:378

Judgment of 20th May 2003, *Rechnungshof v. Österreichischer Rundfunk*, Joined Cases C-465/00, C-138/01 and C-139/01, EU:C:2003:294

Judgment of 9th November 2010, *Volker and Markus Schecke GbR v. Land Hessen*, C-92/09, EU:C:2010:662

References for preliminary ruling of CJEU:

Belgian Constitutional Court (Case C-520/18)

Supreme Court of Estonia (Case C-746/18)

Conseil d'Etat in France (Case C-511/18)

Europe (ECtHR)

X. v. the United Kingdom, no. 8160/78, ECHR 1981 -III

Malone v. The United Kingdom, no. 8691/79, ECHR 1984 – VIII

Margareta and Roger Andersson v. Sweden, no. 12963/87, ECHR 1992 – II

Ludi v. Switzerland, no 12433/86, ECHR 1992 -VI

Niemietz v. Germany, no. 13710/88, ECHR 1992 - XII

Halford v. the United Kingdom, no. 20605/92, ECHR 1997-VI

Amman v. Switzerland [GC], no. 27798/95, ECHR 2000-II

P.G. and J.H. v. The United Kingdom, no. 44787/98, ECHR 2001-IX

Petri Sallinen and Others v. Finland, no. 50882/99, ECHR 2005 - IX

Copland v.The United Kingdom, no. 62617/00, ECHR 2007-IV

Weiser and Bicos Beteiligungen GmbH v. Austria, no. 74336/01, ECHR 2008 – I

Petrov v. Bulgaria, no. 15197/02, ECHR 2008 - V

S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, § 102, ECHR 2008-V

Iliya Stefanov v. Bulgaria, no. 65755/01, ECHR 2008 – VIII

Zakharov v. Russian Federation, no. 47143/06, ECHR 2009-X

M. K. v. France, no. 19522/09, § 35, 2013-IV

Barbulescu v. Romania, no. 61496/08, ECHR 2017 – IX

Privacy International v FCO, Home Office & GCHQ & Others, (communicated case), no. 46259/16, ECHR 2018-XI

OTHER CASES

Germany

Bundesverfassungsgericht, 1 BvR 256/08 of 2 March 2010.

Administrative Court Wiesbaden, Decision of 27th February 2009, Az 6 K 1045/08. WI.

USA

Griswold v. Connecticut, 381 U.S. (1965)

Eisenstadt v. Baird, 405 U.S. (1972)

Roe v. Wade, 410 U.S. (1973)

Hiibel v. Sixth Judicial District Court, 542 U.S., (2004).

Murray v. Express Newspapers [2008] ENWA Civ 446

Carolyn Jewel v. National Security Agency, (complaint), no. 4373 CRB, U.S. (2008)

OFFICIAL OPINIONS

Opinion of AG Villalon delivered on 12 December 2013, *Digital Rights Ireland*, Joined cases C-293/12 and 594/12, EU:C:2013:845

Opinion of AG Saugmandsgaard delivered on 19th July 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others,* Joined Cases C-203/15 and C-698/15, EU:C:2016:572

Opinion of AG Bot delivered on 25th September 2015, *Maximillian Schrems v Data Protection Commissioner*, Case C-362/14, EU:C:2015:627

Opinion of AG Kokott delivered on 8th May 2008, *Satakunnan Markkinapörssi et Satamedia*, Case C-73/07, EU:C:2008:266

Opinion of AG Bot delivered on 14 October 2008, *Ireland v Parliament and Council*, C-301/6, EU:C:2008:558

Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism. [Proposal presented by France, Ireland, Sweden and Great Britain (Document of the Council 8958/04 of 28 April 2004)], adopted 9th November 2004, (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp99_en.pdf, Accessed: 4th Apr 2019).

Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), European Data Protection Supervisor, 31 May 2011.

INTERNET SOURCES

BBC News online, *Spy law 'used in dog fouling war'*, (http://news.bbc.co.uk/2/hi/uk/7369543.stm, Accessed 4th Jun 2019).

Case analysis, Global Freedom of Expression, Columbia University, *Joined Cases Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v. Watson*, (https://globalfreedomofexpression.columbia.edu/cases/joined-cases-tele2-sverige-ab-v-post-och-telestyrelsen-c-20315-secretary-state-home-department-v-watson/, Accessed 9th Apr. 2019).

Data of Eurostat, (https://ec.europa.eu/eurostat/en/web/products-eurostat-news/-/DDN-20190104-1, Accessed 10th May 2019).

Deutsche Welle World, *Germans file mass lawsuit against sweeping data retention law*, 31 December 2007, (http://www.dw.com/en/germans-file-mass-lawsuit-against-sweeping-data-retention-law/a-3025009, Accessed: 12th Dec 2018).

Edward's Snowden interview to the program Vice on HBO, time 21:45 (out of 26:55), Interview available at: https://www.youtube.com/watch?v=ucRWyGKBVzom, Accessed: 18th Oct 2019

Electronic Frontier Foundation, *How Digital Rights Ireland Litigated Against the EU Data Retention Directive and Won*, (https://www.eff.org/node/81899, Accessed: 8th Dec 2018).

Electronic Frontier Foundation, *NSA Spying on Americans, Jewel v. NSA*, (https://www.eff.org/cases/jewel, Accessed: 16th Dec 2018).

Electronic Frontier Foundation, *Russia asks for the impossible with its new surveillance laws*, 19th July 2016, (https://www.eff.org/deeplinks/2016/07/russia-asks-impossible-its-new-surveillance-laws, Accessed 6th Jun 2019).

Electronic Frontier Foundation, *Why metadata matters*? 21 March 2019, (https://ssd.eff.org/en/module/why-metadata-matters, Accessed 27th Mar 2019).

European Union agency for fundamental Rights, *Data Retention Across the EU*, (https://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention, Accessed 10th Apr 2019).

Guide on Article 8 of the Convention – Right to respect for private and family life, 31st August 2018, (https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf, Accessed 18th Mar 2019).

Library of Congress, *European Union: ECJ Invalidates Data Retention Directive*, (http://loc.gov/law/help/eu-data-retention-directive/eu.php, Accessed: 14th Dec 2018).

Official Statistics of ECtHR 1959 – 2018, (https://www.echr.coe.int/Documents/Stats_violation_1959_2018_ENG.pdf, Accessed 22nd Mar 2019).

Spitz, Malte, *How metadata retention works*, published to Zeit Online, (https://www.zeit.de/datenschutz/malte-spitz-data-retention, Accessed 27th Mar 2019).

Statement by Joe Meade, Data Protection Commissioner at the Forum on the Retention of Communications Traffic Data on 24 February 2003, (https://www.dataprotection.ie/docs/Press-Release-Retention-of-Communications-Traffic-Data/i/224.htm, Accessed: 12th Dec 2018).

Statista: Global digital population as of January 2019, (https://www.statista.com/statistics/617136/digital-population-worldwide/, Accessed 6th Mar 2019).

The Guardian, *NSA Prism program taps in to user data of Apple, Google and others*, (https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, Accessed 19th Mar 2019).

The Verge, *Trump signs bill banning government use of Huawei and ZTE tech*, (https://www.theverge.com/2018/8/13/17686310/huawei-zte-us-government-contractor-ban-trump , Accessed 17th Mar 2019).

Top secret documents of NSA regarding games and virtual worlds leaked by E.Snowden, (https://www.documentcloud.org/documents/889134-games, Accessed 17th Apr 2019).

Transcript of Mark Zuckerberg's hearing in Congress of the USA (Committee on energy and commerce), (https://docs.house.gov/meetings/IF/IF00/20180411/108090/HHRG-115-IF00-Transcript-20180411.pdf, Accessed on 19th Mar 2019).

UK Presidency of the European Union, *Liberty and Security – Striking the Right balance*, Paper, (http://www.statewatch.org/news/2005/sep/ukpres-paper.pdf, Accessed 4th Jun 2019).

REPORTS, EXPLANATIONS, SURVEYS

Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), 18.04.2011 COM (2011) 225 Final

Report of the Committee on Data Protection, (Sir Norman Lindop, Chairman) (Cmnd 7341, 1978)

Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, National Security Agency, pub.12th September 2013, Available at: https://fas.org/irp/offdocs/ict-review.pdf, Accessed: 28th Mar 2019, P. 260

Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Privacy and Civil Liberties Oversight Board, pub. 2nd July 2017, Available at: https://www.pclob.gov/library/702-Report.pdf, Accessed: 28th Mar 2019, P.149

The Report of US Department of Health, Education and Welfare, Records, Computers and Rights of Citizens U.S. Dep't of Health, Educ, & Welfare, Records, Computers, and the Rights of Citizens xxxii (1973)

Explanations of the Praesidium of the Convention which drafted the Charter of Fundamental Rights of the European Union, in Official Journal of the European Union C 303/17 - 14.12.2007

Commission's Fundamental Rights Check-List for all legislative proposals in Commission Communication COM (2010) 573/4, 'Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union'.

Privacy and Human Rights 2004: An International Survey of Privacy Laws and Developments. Washington, D.C.: Electronic Privacy Information Center.

OTHER REFERENCES

Council of the European Union, *Data retention – State of play*, document #14319/18, (http://data.consilium.europa.eu/doc/document/ST-14319-2018-INIT/en/pdf, Accessed 08 Aug 2019).

Presentation of Jan Ellerman, slide 17, WK 5900/2018 INIT (Outcome 2.Workshop)

Statement on European Data Protection Supervisor's website, (https://edps.europa.eu/data-protection/data-protection_en, Accessed 20th Mar 2019).

ABBREVIATIONS

AG	Advocate General
CFREU	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
DAPIX	Working Party on Information Exchange and Data Protection
DRD	Data Retention Directive
DRI	Digital Rights Ireland
DRIPA	Data Retention and Investigatory Powers Act 2014
ECHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EU	European Union
Europol	European Union Agency for Law Enforcement Cooperation
Eurostat	European Statistical Office
GDPR	General Data Protection Regulation
GVE	Game Virtual Environment
IP	Internet Protocol
JHA	Justice and Home Affairs
MS	Member State
NSA	National Security Agency
PRISM	National surveillance program in the USA
RF	Russian Federation
RIPA	Regulation of Investigatory Powers Act 2000
SIM	Subscriber Identification Module
SORM	System of Operative and Investigatory Actions (abbreviations from Russian ‘система оперативно-розыскных мероприятий’)
TELE2	Tele 2 & Watson
TFEU	Treaty on Functioning of the European Union
UK	The United Kingdom of England and Northern Ireland
USA, US	United States of America
VK	Vkontakte
VPN	Virtual Private Network

1. INTRODUCTION

'A free society should not have to choose between
more rational use of authority and personal privacy'
(Alan Westin – 'Privacy and Freedom')

Problem (gap) in the EU law

After the annulment of the Data Retention Directive in the *Digital Rights Ireland* case in 2014, European Union law faced a gap in its information law (regarding data retention). European Union's unifying law was dismantled, while national laws continued the mass data retention practices. As was claimed by Paul Bernal, 'full impact of the Digital Rights Ireland case is still not clear'[1].

According to Article 266 of the TFEU: 'The institution whose act has been declared void or whose failure to act has been declared contrary to the Treaties shall be required to take the necessary measures to comply with the judgment of the Court of Justice of the European Union.'[2] Data Retention Directive was a document of the European Parliament and the Council. Both institutions have opened a wide discussion of the data retention topic among experts and public, trying to take into consideration all the flaws of the previous document and evaluating the necessity of such measure as data retention. The Council had created 2 expert groups to examine and deliver deep analysis of data retention issues: DAPIX and TELE. At the same time, European Commission which has a right of legislative initiative 'does not plan to present a new legislative initiative on data retention'[3]. At least until proper research of the controversies is done. Nowadays, Commission is working on creating guidance to data retention for Member States.

CJEU participated in shaping the data retention by delivering judgment in the *Tele2&Watson* case. This made discussions in the retention topic clearer, but still not deprived of ambiguities. Such important questions as meaning of 'serious crime', categorization of time period for different types of metadata, authorities with access to retained data, and how to deal with professional secret metadata, remained unanswered. As a result, Member States continue to

[1] Bernal 2016, p. 246.
[2] TFEU, Article 266.
[3] Statement in Legislative Train, 04.2019, Data retention for the purposes of prevention, investigation and prosecution of crime, (http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-data-retention-directive, Accessed 28th May 2019).

interpret the law in their own way. As was stated in the Fundamental Rights Report 2017 by the European Agency for Fundamental Rights after the *Digital Rights Ireland*[4] and also *Tele2&Watson*[5] case: 'Member States made only limited progress in adopting new legal frameworks'.[6]

Moreover, scholars N. Vainio and S. Miettinen, claimed that 'several Member State governments have kept the data retention laws in place'[7]. Same scholars underlined that these are usually governments who want to remain the old regulations on data retention[8]. The constitutional courts, in contrast, tend to strike down the national laws[9], but the amendments or new laws are not built on a uniform understanding of the European Union law. As a result, national laws, which were build to respond to demands of disproportional Data Retention Directive were either a) remaining, b) stroke down with no proper substitution or c) replaced by the new, often inappropriate laws.

CJEU nowadays is facing a chain of new requests for preliminary rulings with regard to communications data retention from Belgium[10], Estonia[11] and France[12]. This proves that Member State authorities still does not have a clear understanding how to build their national metadata retention laws to be in compliance with European Union law.

As seen from described above, the topic of data retention in European Union is urgent and needs researcher's input. The aim of this thesis is to deliver new research based information for the ongoing discussion on European data retention. In other words the **main purpose** of this work is to deliver an analysis of fair limits to the right to privacy when using metadata retention. By the end of the thesis, the reader will be answered the main question: is it possible to build a national metadata retention law which is in compliance with EU law? In other words, as was stated by the

[4] *Digital Rights Ireland*, Joined cases C-293/12, C-594/12, EU:C:2014:238.
[5] *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others,* Joined Cases C-203/15 and C-698/15, EU:C:2016:970.
[6] European Union Agency for Fundamental Rights, Fundamental Rights Report 2017, p.163.
[7] Vainio – Miettinen 2015, p.290.
[8] Ibid. p.290.
[9] See for example: in Austria – Decision G 47/2012-49, Seitlinger and others, 27 June 2014; in Netherlands – Decision of the District Court of The Hague, Case Number C/09/480009 KG ZA 14/1575, 11 March 2015; in Germany – Data Retention Judgment of the German Federal Constitutional Court (BVerfG 1 BvR 256/ 08) 2 March 2010.
[10] Belgian Constitutional Court (Case C-520/18).
[11] Supreme Court of Estonia (Case C-746/18).
[12] Conseil d'Etat in France (Case C-511/18).

CJEU, 'in what circumstances and under which conditions'[13] can the metadata retention be implemented on national level without violation of the Charter?

The thesis is structured into 6 chapters. Chapter 1 Introduction contains explanation of the problem, limitations, description of the methods of research, structure and main research question.

Chapter 2 'Defining privacy' is aimed at discussing what privacy is and how it is regulated in the European Union. The Chapter continues by researching the correlation between right to privacy and right to data protection. In addition, the work analyses the limitations to the right to privacy established by the Charter of Fundamental Rights of the European Union.

Chapter 3 'Metadata retention' analyses what is metadata and its importance. This description is followed by illustration of the metadata retention practices of various states. Separate attention in this chapter is drawn to metadata retention practices in European Union. The study critically analyzes Data Retention Directive and two landmark cases: Digital Rights Ireland and Tele2&Watson.

Chapter 4 'Conditions for limiting privacy by means of metadata retention' is devoted to analysis of conditions established in European Union to limit right to privacy by metadata retention. In this part, the study critically oversees the objective of general interest. Also it points out what shall be included into national law to fully cover metadata retention. Among such points the work gives a suggestion on what might be understood as a 'serious crime'. The chapter describes data protection measures and other safeguards compliance with which ensure respect to the essence of the right to privacy. General description of the principle of proportionality closes up the Chapter.

In Chapter 5 'What is strictly necessary' we analyze matters that shall be limited to 'what is strictly necessary' to pass the proportionality test. Focus areas of limitations are: people concerned, categories of data retained, means of communication affected and time period of retention. This part of the work provides thorough analysis of the proportionality failures within Data Retention Directive, suggests shorter time periods of retention for Internet-based metadata and discusses few options for limiting the amount of people who undergo retention of their

[13] Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others,* Joined Cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 109.

metadata. Chapter 6 Conclusion sums up the made research and answers the main research question.

Limitations

Despite the thesis uses a lot of examples from national practices, it is not aimed at shaping specific provisions in Member State laws. Also the research does not discuss whether the CJEU had jurisdiction to regulate national retention laws by delivery of its decisions in the Digital Rights Ireland and Tele2&Watsons case. This, though, is a big question to consider. The thesis does not analyze the pending decisions in the CJEU from Belgium, France and Estonia with regard to metadata retention. This study, despite mentioning the discussion around the general interest question, does not query whether metadata retention is necessary in the democratic society. All the mentioned topics can be a separate research and, therefore, they are out of the scope of our paper.

Methodology

The main research method is legal dogmatic. It focuses on the current European Union understanding of privacy and data protection, and helps estimate the judgments of the CJEU. Secondary methods of research are: interpretative (in analysis of the meaning of the court judgments, concept of Data Retention Directive), comparative (in comparing the approaches to metadata retention in different Member States; in comparing the positions of the CJEU judges and Advocate General; in comparing opinions of legal scholars).

Sources

This thesis is based on European Union law: mainly CFREU and two landmark cases of the CJEU: Digital Rights Ireland and Tele2&Watson. Also the study is saturated with scholarly opinions on relevant issues, found in books, articles, case comments. Statistical data from reports, reviews and development frameworks helps the reader to understand the practical issues connected to metadata retention.

2. DEFINING PRIVACY

2.1 Modern privacy challenge

James Rule says that '[p]rivacy as an issue for legislation and policy is a relatively recent arrival in the public forum'[14]. It goes without saying that the disturbance around the privacy issues is predicated by the raise of informational technologies. Nowadays, Internet 'is a way that we manage our social lives, apply for jobs, seek information about our health, do our shopping, our banking, seek and find romance, choose and consume entertainment and much more'[15]. David J. Solove also claimed: '[…] new technologies have given rise to a panoply of new privacy harms.'[16] Indeed, the opportunities which the technology has brought in data harvesting and analysis are enormous. As recent cases like Facebook and Cambridge Analytica[17] and revelations of Edward Snowden[18] had shown, enforcing mass surveillance or even shaping the behavior of millions of people are now technically attainable.

Governments, in comparison to individuals and businesses, have more power and resources to get the best technological equipment possible for leading in information competition. Moreover, even if the government does not have equipment like that, it can always demand certain actions (retention of data) from businesses operating in their jurisdiction (like Russian Federation did by means of SORM system[19], like USA did by means of the PRISM programme[20] or like the European Union tried to do with its Data Retention Directive until the judgment of CJEU in *Digital Rights Ireland* case). It is hard to doubt that newest technical capabilities applied to the World Wide Web, which today accounts for approximately 4.4 billion active users[21], might, and eventually will, result in grave abuses of privacy by governments. As a counter argument, it is possible to claim that '[…] surveillance can serve as a deterrent to crime. Many people desire the

[14] Rule 2007, p.22.
[15] Bernal 2016, p.247.
[16] Solove 2006, p.478.
[17] See for example, *Transcript of Mark Zuckerberg's hearing in Congress of the USA* (Committee on energy and commerce),(https://docs.house.gov/meetings/IF/IF00/20180411/108090/HHRG-115-IF00-Transcript-20180411.pdf, Accessed on 19th Mar 2019).
[18] Elliott, Kennedy – Rupar, Terri, *Six months of revelations on NSA*, (https://www.washingtonpost.com/wp-srv/special/national/nsa-timeline/, Accessed 19th Mar 2019).
[19] The SORM system was established in Russia to give police and secret agencies direct access to the backbone of communication. SORM enhanced the possibilities of abuse. Additionally, the ECHR in case *Zakharov v. Russian Federation* recognized that legal system of RF 'do not provide for adequate and effective guarantees against arbitrariness and the risk of abuse'; See, *Zakharov v. Russian Federation*, no. 47143/06, ECHR 2009-X, paragraph 302.
[20] The Guardian, *NSA Prism program taps in to user data of Apple, Google and others*, (https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, Accessed 19th Mar 2019).
[21] See Statista: Global digital population as of January 2019, (https://www.statista.com/statistics/617136/digital-population-worldwide/, accessed 6th Mar 2019).

discipline and control surveillance can bring'[22]. But in this multidimensional game, where governments are fighting against other governments[23], governments are fighting against businesses[24] and businesses are fighting against other businesses for data of individuals, the last category remains the least protected and, moreover, poorly aware of the volume of real threats to their privacy. Unfortunately, in current state of technological development and commonly accepted pattern of using all available technologies 'our ability to shape these uses of 'our' data often appears minimal if not absent[25]'. The concept that privacy is only 'an illusion'[26] was introduced in the beginning of 90's, but nowadays, it seems to become strongly evidence-based. One of such evidences is that 'the technical capabilities and legal license to collect and store electronic data have been massively expanded, and the ability to exchange data between different authorities has been enhanced'[27].

The position of the individual in this informational competition is pitiable, if not victim. Despite the fact that 'privacy is an old and venerable subject'[28], it is only now that the right to privacy is sacrificed on the altar of efficiency in administering the society. This point of view is supported by James Rule, who says that 'privacy has simply become an anachronistic value'[29]. As a proof of that, today '[c]ourts and policy makers frequently struggle in recognizing privacy interests, and when it occurs, cases are dismissed or laws are not passed. The result is that privacy is not balanced against countervailing interests'[30]. This happens because members of society rarely create enough pressure on authorities to guarantee these rights. The best variant for individuals in this situation is to educate themselves in privacy matters, analyze the moves of main world players in data management and then directly influence legislators to work on excluding abuse. A successful example of social pressure to postpone the laws which infringed the fundamental human right of privacy can be seen from the Digital Rights Ireland and Tele2&Watsons cases, where proceedings brought in front of national courts against blanket national metadata retention

[22] Solove 2006, p.494.
[23] USA is playing the role of the worlds wiretapping leader with its NSA schemes to penetrate the core of communication. Russian Federation is installing the SORM system which obliges all the ISPs working on the territory of RF to store data on local services, China is trying to imitate the previous actions of USA through its companies like Huawei, ZTE and 5G technologies.
[24] USA had banned governmental agencies and stuff to use products of Huawei Technology Company and ZTE Corporation as companies that facilitates the China in wire tapping the world's communication. See for instance: The Verge, *Trump signs bill banning government use of Huawei and ZTE tech*, (https://www.theverge.com/2018/8/13/17686310/huawei-zte-us-government-contractor-ban-trump , Accessed 17th Mar 2019).
[25] Rule 2007, preface (ix).
[26] Flaherty 1991, p. 837.
[27] Thimm, 2018, p. 19.
[28] Simitis 1987, p. 707.
[29] Rule 2007, preface (x).
[30] Solove 2006, p. 480.

found approval in CJEU decision. Nevertheless, not all of the EU Member States had yet amended the laws in compliance with the new defined rules (established by CJEU in Digital Rights Ireland and Tele2&Watson cases).

2.2 Definition of privacy

The fathers of concept of privacy, Louis Brandeis and Samuel Warren, sum up privacy as 'the right to be let alone'[31]. A similar definition is offered by David Flaherty who claimed that privacy is 'the right not to be unnecessarily intruded upon[32]'. A feasible definition of privacy was formulated by Alan Westin: 'Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.'[33]

Despite efforts to create the uniform definition of privacy, the majority of scholars agree that privacy is too big and loose to try establishing one universal definition for it.

James Rule confirms it by stating that the term 'privacy' means many different things[34]. David Flaherty claims that concept of privacy is 'amorphous, ill-defined, and diverse'.[35] Daniel J. Solove underline that '[p]rivacy is too complicated a concept to be boiled down to a single essence. Attempts to find such an essence often end too broad and vague, with little usefulness in addressing concrete issues.[36] European scholars and advisory boards also underline that privacy is very hard to define because 'private life is a broad concept incapable of exhaustive definition' and 'the notion of private life is not limited to an 'inner circle''[37]. Additionally, efforts to draw out a single definition of privacy stumbles upon a claim that 'privacy' are dependent on a nation's culture'[38]. As an example: in Britain access to the tax payers' information is forbidden and kept secret, while in Sweden it is 'readily accessible'[39].

One of the most efficient solutions in defining privacy was offered by Daniel J. Solove. In his article 'Taxonomy of Privacy', he addressed a few fundamental issues regarding privacy. Firstly,

[31] Warren - Brandeis, 1890, p. 193.
[32] Flaherty 1991, p. 831.
[33] Westin 1967.
[34] Rule 2007, preface (x).
[35] Flaherty 1991, p. 850.
[36] Solove 2006, p. 485.
[37] Guide on Article 8 of the Convention – Right to respect for private and family life, 31st August 2018, (https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf, Accessed 18th Mar 2019).
[38] Walden 2011, p. 575.
[39] Ibid.

he recognized that the problem with giving a strict definition of the privacy and right to privacy is unsolvable. As a result of that '[…] our understanding of privacy remains fog and the law remains fragmented and inconsistent.'[40]

Secondly, he illustrated that the attempts of legislators and justice system to systemize privacy legal issues (at least in America) have been made for decades and they failed, because there is no single formula for defining privacy and its limits.

Lastly, the scholar highlighted that the best way to understand the essence of privacy is to analyze the cases in which it clashes with other interests (security, free speech, efficient consumer transactions[41]). According to the author's opinion, the evaluation of 'interferences and annoyances'[42] gives the key to understanding privacy. Such an idea is coherent with opinion of David Flaherty, who claimed that '[p]rivacy, like freedom, is difficult to define except in the negative'[43].

The 'negative' or 'interferences and annoyances' – are all kind of actions which may intrude into privacy. Taking into consideration the taxonomy offered by the Daniel J. Solove, these are actions which can be divided into 4 main categories: information collection, information processing, information dissemination or invasion[44]. If we describe wider: surveillance, interrogation, aggregation, identification, insecurity, secondary use, exclusion, breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, distortion, intrusion and decisional interference of any other subject of informational relations[45].

In the light of our research we will have a look on one 'negative' which intervenes with privacy: metadata retention (which is the closest to information processing). This critical analysis will be given in Chapter 3.

2.3 Right to privacy in the European Union

For understanding the privacy regime guaranteed for the population in EU, we have to analyze how this right is protected in European Union.

[40] Solove 2006, p. 562.
[41] Ibid, p. 480.
[42] Ibid.
[43] Flaherty 1991, p. 850.
[44] See the contents of the Article 'A Taxonomy of Privacy', Solove 2006.
[45] Ibid.

Europe has two legal frameworks which define the European law. The first one 'is that of the European Convention on Human Rights, as international agreement between the 47 States of the Council of Europe'[46] adopted in 1950 and the second, Chapter of Fundamental Rights of the European Union (hereinafter CFREU) with participation of 28 Member States, adopted in 2000.

The right to privacy was declared in the 1950 European Convention of Human Rights as Article 8. In 2000, European elites cloned it into CFREU under Article 7, but additionally, added the right to data protection in its next Article 8.

Article 8 of the ECHR declares: *1. Everyone has the right to respect for his private and family life, his home and his correspondence.*[47]

European Court of Human Rights has been successfully interpreting Article 8 of the ECHR for more than 5 decades. During the period from 1959 to 2018, the Court in Strasbourg had delivered 1.393 judgments on the Right to Privacy[48]. In its long practice the Court had extended the meaning of the term 'correspondence' to mean 'communications'. In case of *Niemietz v. Germany*[49] the word 'correspondence' meant 'letters of a private and personal nature', while later the term became the one which included: packages seized by customs (in other words 'irregular postal packets'[50]), communications made via phone[51], intercepted metadata such as date, numbers and duration of communications[52]. Recent case law made the meaning of 'correspondence' even more complex, adding to the list emails[53], Internet use evidences[54], data stored on servers[55], information stored on hard drives[56] and even floppy discs[57].

Article 7 of the CFREU, which is named 'Respect for private and family life', declares:

---

[46] Kokott – Sobotta, 2013, p. 222.
[47] European Convention of Human Rights, Art.8.
[48] Official Statistics of ECHR 1959 – 2018,
(https://www.echr.coe.int/Documents/Stats_violation_1959_2018_ENG.pdf, Accessed 22nd Mar 2019).
[49] *Niemietz v. Germany*, no. 13710/88, ECHR 1992 – XII, paragraph 32.
[50] *X. v. the United Kingdom*, no. 8160/78, ECHR 1981 -III, paragraph 34.
[51] See for instance the notion of 'correspondence' in cases: *Margareta and Roger Andersson v. Sweden*, no. 12963/87, ECHR 1992 – II; *Ludi v. Switzerland*, no 12433/86, ECHR 1992 -VI; *Malone v. The United Kingdom,* no. 8691/79, ECHR 1984 – VIII; *Amman v. Switzerland* [GC], no. 27798/95, ECHR 2000-II*; Halford v. the United Kingdom*, no. 20605/92, ECHR 1997-VI; and *Petrov v. Bulgaria*, no. 15197/02, ECHR 2008 – V.
[52] Judgment of the ECtHR on the 25 Dec 2001 *P.G. and J.H. v. The United Kingdom*, paragraph 42.
[53] *Barbulescu v. Romania*, no. 61496/08, ECHR 2017 – IX.
[54] *Copland v.The United Kingdom*, no. 62617/00, ECHR 2007-IV.
[55] *Weiser and Bicos Beteiligungen GmbH v. Austria*, no. 74336/01, ECHR 2008 – I.
[56] *Petri Sallinen and Others v. Finland*, no. 50882/99, ECHR 2005 – IX.
[57] *Iliya Stefanov v. Bulgaria*, no. 65755/01, ECHR 2008 – VIII.

'Everyone has the right to respect for his or her private and family life, home and communications.'[58]

As seen the Charter's Article 7 basically copies the wording of the European Convention. There are only two differences: 1) masculine construction 'his' was replaced by the inclusive 'his or her'; 2) word 'correspondence' was replaced by the more relevant 'communications'.

Praesidium which drafted the European Charter of Fundamental Rights claimed that in analysis of the right to privacy declared by the Article 7 of the CFREU, it is reasonable to refer to ECHR framework, because the 'meaning and scope of this right are the same as those of the corresponding article of the ECHR'[59].

As a comparison, in the United States, there is no law, which defines the right to privacy in the same way, as done by European acts. Indeed, even the term privacy cannot be found in the U.S. Constitution[60]. However, as was stated by an American scholar: 'although the word "privacy" is not explicitly mentioned anywhere in the [US] Constitution, the Court reasoned that the Constitution provides for a "right to privacy" in the "penumbras" of many of the amendments in the Bill of Rights'[61].

As well as in Europe, in the United States court practice can give an idea of how privacy is understood and what is meant by right to privacy. For example, in *Eisenstadt v. Baird* case, the court defined that right to privacy 'is the right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child'[62]. Another example is the American case *Roe v. Wade*, where the court made clear that right to privacy 'encompass [es] a woman's decision whether or not to terminate her pregnancy'[63].

2.4 Correlation between right to privacy and data protection

Ian Walden claims that '[d]ata protection and privacy are clearly substantially overlapping concepts, although certain distinctions have been drawn'[64]. Lee Andrew Bygrave has an

[58] CFREU, Article 7.
[59] Explanations of the Praesidium of the Convention which drafted the Charter of Fundamental Rights of the European Union, in Official Journal of the European Union C 303/17 - 14.12.2007.
[60] White 2009, p. 209.
[61] *Griswold v Connecticut*, 381 U.S. 484, 485-86 (1965).
[62] *Eisenstadt v. Baird*, 405 U.S. 438 (1972).
[63] *Roe v Wade*, 410 U.S. 113, 153 (1973).
[64] Walden 2011, p. 575.

interesting point stating that data protection (access to and security of data) refers to 'interests that relate to the quality of personal information and information systems', while the term privacy constitutes 'interests pertaining to the condition of persons as data subjects and to the quality of society generally'[65].

In my opinion, Alan Westin, by defining privacy as 'the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'[66], had given a pretty decent definition for data protection. What is interesting, such definition is close to current European understanding of data protection right. Indeed, the new European data protection act - General Data Protection Regulation provides data subjects with an opportunity to control how much of their information is shared with the other subjects of informational relations[67]. The obligation of the communication service providers to make separate consents of the various data usages is a proof of existence of choice. A person, if he/she wants to use the online service or get access to the website, can choose how much of personal data it is sharing with the service and further with other data subjects. The individual can also 'withdraw his or her consent at any time'[68].

Despite substantially overlapping, there are some issues which differ in data protection and privacy. For example, Ian Walden claims that 'an assertion of privacy is generally made by an individual before a court'[69], while data protection assertion is made in front of the administrative body. The task of the court is to balance the right to privacy with other conflicting rights, while the task of the authority in data protection regulatory action is to deliver 'supervisory remit over the actions of those that process personal data'[70].

Lindop Report on Data Protection also states that 'data protection law should be different from that of a law on privacy: rather than establishing rights, it should provide a framework for finding a balance between interests of the individual, the data user and the community at large.[71]' A good example of splitting the privacy and data protection provisions is seen in the CFREU. Declaration of right to privacy and right to data protection in 2 different articles was probably

[65] Bygrave 2002, p. 29.
[66] Westin 1967.
[67] See GDPR, section of Data subject's Rights.
[68] GDPR, para.3, Article 7.
[69] Ian Walden, 2011, p. 577.
[70] Ibid.
[71] Report of the Committee on Data Protection, (Sir Norman Lindop, Chairman) (Cmnd 7341, 1978).

made, because 'data protection laws do not map neatly onto a privacy framework, but rather represent a range of different interests[72]'.

In European Union data protection is understood as a 'distinct and stand-alone fundamental right'[73]. European Union practice over the last decade is demonstrating that right to privacy and right to data protection are 2 distinct rights. There are several proofs of that.

First of all, the structure of the CFREU in covering privacy and data protection has 2 different articles 7 and 8. If these rights are the part of one same right, they would, probably, be different paragraphs of the same article, but not 2 separate articles. Similar approach to my opinion is demonstrated by the CJEU in its case law: 'Article 8 of the Charter concerns a fundamental right which is distinct from that enshrined in Article 7 of the Charter and which has no equivalent in the ECHR'[74]. The same is proved by some scholars: 'the distinction between both rights in the EU Charter of Fundamental Rights is not purely symbolic'[75].

Secondly, the separation between these two rights is unambiguously demonstrated in Handbook on the European Data Protection Law: 'Under EU law, data protection has been acknowledged as a distinct fundamental right. It is affirmed in Article 16 of the Treaty of the Functioning of the EU, as well as in Article 8 of the EU Charter of Fundamental Rights.'[76]

Thirdly, the concept of existence of 2 different rights was supported by the Advocate General Cruz Villalon in *Digital Rights Ireland* case. The Advocate General recognized that right to privacy and right to data protection are two different rights. He claimed in his Opinion that data protection right 'is distinct from the right to privacy'[77]. Advocate General widen his claim by stating that 'although data protection seeks to ensure respect for privacy, it is, in particular, subject to an autonomous regime […]'[78].

The fourth argument is the existence of a separate set of acts, which is regulating specifically data protection right: General Data Protection Regulation and Directive JHA for investigation

[72] Walden 2011, p. 575.
[73] Handbook on European Data Protection Law, p. 43.
[74] Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others,* Joined Cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 129.
[75] Kokott – Sobotta 2013, p. 222.
[76] Handbook on the European Data Protection Law, 2018 ed, p. 17.
[77] Opinion of AG Villalon delivered on 12 December 2013, *Digital Rights Ireland*, Joined cases C-293/12 and 594/12, EU:C:2013:845, paragraph 55.
[78] Ibid.

and prevention of crimes. The fifth argument is that European Data Protection Supervisor states: 'Privacy and Data Protection, though connected, are commonly recognised all over the world as two separate rights'[79].

There are also some thoughts that merely present data protection and right to privacy in a different perspective. For example, Maltese lawyer Michael Grech claims that 'Privacy is a right whilst data protection is the legislation which implements that right'[80]. He has an interesting view saying that 'Privacy being a protection from possible abuses of personal information or searches by the state, while data protection is the tool the law uses to make sure that an individual is protected from abuse of his personal information by another individual'[81]. A similar approach was used in Canada in 1983; their "privacy laws" [were], in effect, data protection statutes for controlling the collection and use of personal information by the public sector.'[82] Privacy was the subject, while data protection laws were the tools to ensure it.

A great work on comparison of privacy and data protection has been done by European scholars J. Kokott and C. Sobotta. The scholars paid their attention particularly to European Court of Human Rights practice. Their research conclusion is that 'privacy and the protection of personal data are closely linked in the jurisprudence of the European Court of Human Rights and the Court of Justice of the European Union, but they should not be considered to be identical'[83]. The general statement is that 'despite substantial overlaps there are also important differences, in particular with regard to the scope of both rights and their limitation'[84]. In the *Bavarian Lager*[85] case the CJEU claimed that 'compared with the right to privacy, the EU rules on data protection create a specific and reinforced system of protection'[86]. They claim that in Europe both CJEU and ECtHR 'tend to treat data protection as an expression of the right to privacy' but 'the specifics of each right must be respected'[87]. The scholars have raised one more important issue:

---

[79] Explanation article on European Data Protection Supervisor's website, (https://edps.europa.eu/data-protection/data-protection_en, Accessed 20th Mar 2019).
[80] Michael Grech, *Data protection vs. The Right to Privacy*, (https://www.gvzh.com.mt/malta-law/data-protection/vs-the-right-to-privacy/ Accessed 20th Mar 2019).
[81] Ibid.
[82] These acts were: Privacy Act, R.S.C. ch. P-21 (1983); An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information, Que. Stat. ch. 30 ('1982); and Freedom of Information and Protection of Privacy Act, ONT. REV. STAT. ch. 25, in Flaherty 1991, p. 851.
[83] Kokott – Sobotta, 2013, p. 228.
[84] Ibid, p. 222.
[85] Judgment of 29th June 2010, *Commission v Bavarian Lager,* Case C-28/08 P, EU:C:2010:378, paragraph 60.
[86] Kokott – Sobotta, 2013, p. 222.
[87] Ibid.

that the Charter's right to privacy or right to data protection do not create obligations to private parties[88].

The right to data protection appeared as a solution in protecting informational privacy. Since the legislator understood the importance and crucial need to regulate the sphere of data communication it has not only provided data protection right as a separate right in the CFREU, but also offered Data Protection Directive in 1995, and later substituted it in 2018 with General Data Protection Regulation and JHA Directive on data protection for the purposes of the prevention, investigation, detection or prosecution of criminal offences. Also it shall be mentioned that the European tradition of data protection has been known before the unified efforts made by the European Union. For example the earliest European law on data protection was adopted in Sweden in 1973. Some countries even had a strategy of splitting the data protection regulations for private and public sectors (Denmark and Lithuania) [89]. Interestingly that in USA the first efforts to regulate privacy issues were also made in 1973. US Department of Health, Education and Welfare in their report established the equivalent of today's data protection principles; they were called 'Fair Information Practices'[90].

In my opinion, privacy has to be understood more like a state: a state of being left alone. Right to privacy is a right to be let alone. Data protection is a right to have information about you undisclosed in cases, where you have a 'reasonable expectation of privacy'[91].

Data protection right had grown from informational right to privacy: if right to privacy is seen as a tree, than data protection is one of its brunches that became too heavy and was replanted as a separate tree. This example can explain why these rights are often intertwined, commonly used together and have the same origin. As was delivered in European Data Protection Supervisor's opinion '[t]he notion of data protection originates from the right to privacy'[92]. At the same time it 'has inevitably extended to wider questions regarding an individual's 'right to privacy'[93].

---

[88] Opinion of AG Kokott delivered on 8th May 2008, *Satakunnan Markkinapörssi et Satamedia*, Case C-73/07, EU:C:2008:266, paragraphs 102-104.
[89] Table I. in Rule 2007, P.31; and Privacy and Human Rights 2004: An International Survey of Privacy Laws and Developments. Washington, D.C.: Electronic Privacy Information Center.
[90] The Report of US Department of Health, Education and Welfare, Records, Computers and Rights of Citizens U.S. Dep't of Health, Educ, & Welfare, Records, Computers, and the Rights of Citizens xxxii (1973).
[91] This notion was established in *Murray v. Express Newspapers* [2008] ENWA Civ 446.
[92] Explanation article on European Data Protection Supervisor's website, (https://edps.europa.eu/data-protection/data-protection_en, Accessed 20th Mar 2019).
[93] Walden 2011, p. 576.

In other words, right to data protection was established as an effort to ensure informational privacy of the individual, which in the new technology age became so important that European legislators had provided a separate set of acts to regulate them. Data protection is a separate right, but it serves as a tool to guarantee the protection of one dimension of privacy: informational.

2.5 Limitation to the right to privacy (Article 52(1) CFREU)

The right to privacy belongs to a category of 'qualified rights'[94]. 'Such rights are often termed 'qualified' rights on account of their limitability'[95]. The opposite term for qualified right is 'absolute'. In other words, an absolute right can never be limited (freedom from torture and other cruel, inhuman or degrading treatment or punishment). Therefore, being a qualified right, there are certain measures up to which such a right can be executed. These measures might be a) natural: you have as much privacy as it does not violate the rights of others; and b) imposed by law: limitations which the state create to be able to execute its state functions: crime investigation, providing environmental and health safety, etc.

One useful aid for understanding how the limitations to any declared by the CFREU rights is made, can be found in EU Commission's Checklist: 'any limitation must: a) be formulated in a clear and predictable manner; b) be necessary to achieve an objective of general interest or to protect the rights and freedoms of others; c) be proportionate to the desired aim; and d) preserve the essence of the fundamental rights concerned.[96] Also as was delivered by CJEU in *Österreichischer Rundfunk* any limitations to the fundamental rights have to be 'precise and enable foreseeability'[97].

Question of limitations to the right to privacy is a basis of our research. We put the limitations, enshrined in the CFREU in the structure of our work.

The list of requirements for limiting any right in the Chapter of Fundamental Rights of the European Union is presented in the Article 52. Part 1 of the Article 52 CFREU states:

[94] Law – Martin 2009, p. 1490.
[95] Rivers, 2006, p. 174.
[96] Commission's Fundamental Rights Check-List for all legislative proposals in Commission Communication COM (2010) 573/4, 'Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union'.
[97] *Rechnungshof v. Österreichischer Rundfunk*, Joined Cases C-465/00, C-138/01 and C-139/01, EU:C:2003:294.

'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.'[98]

Based on this article of the CFREU and previously used procedure of CJEU in justifying interference with the right to privacy (in *Volker und Markus Schecke and Hartmut Eifert v. Land Hessen*[99] case), we can clearly state that in limiting privacy by metadata retention, it is vital to comply with 5 main requirements: meet the objective of general interest, achieve that conditions for such action is provided by law, provide respect to the essence of right to privacy, keep the interference proportional and limited to what is strictly necessary. These points will be precisely addressed in the Chapters 4 and 5 of this thesis.

[98] CFREU, Article 52(1).
[99] *Volker and Markus Schecke GbR v. Land Hessen*, C-92/09, EU:C:2010:662.

3. METADATA RETENTION

3.1 What is metadata?

Reilly Claire suggests that metadata is 'digital information that accompanies electronic communication'[100]. This definition is very close to the outdated notion that content is a letter, while metadata is an envelope. Using this notion is impossible, because metadata nowadays is more complex. According to Judith Rauhofer, metadata consist of traffic data, location data and subscriber data[101]. She makes such a statement by referring to the s 21 of the UK's RIPA[102] act. The mentioned three types of information combine into one thing – metadata, or also called 'communications data'. In my opinion, communications data is a better term, because it represents the importance of such type of data. Metadata sounds more technical and does not bare in minds of people the necessity of sharp attention to the topic. However, in the course of the research both terms will be used.

For clear understanding of the essence of communications data it is possible to use the definition given by Christine Kirchberger: '[t]raffic data is information that is processed in order to transmit an electronic message in an electronic communications network or in order to bill this message. Commonly, traffic data includes information on which numbers or addresses have been used for communication and the date and time of the message. Traffic data can also include location data, which indicates the geographical position of the terminal equipment, such as mobile phone or computer, of a user. Network operators traditionally also process information about the subscription, including the name and address of the subscriber.'[103] From this paragraph we can clearly see that the communications data is a conglomerate of subscriber, traffic and location data, some of them are interconnected: you cannot understand properly the traffic data if you do not pay attention to the subscriber data.

Approximately the same approach to defining metadata was seen in the Data Retention Directive. Despite the fact that the Directive was annulled by the decision of CJEU in Digital Rights Ireland case (2014), the concept of the invalid document is a great aid to understanding what is metadata. In the definitions section of the Data Retention Directive it is clearly said that

[100] Reilly 2009.
[101] Rauhofer 2009, p. 578.
[102] UK Regulation of Investigatory Powers Act, 2000.
[103] Kirchberger 2011, pp.414-415.

the scope of the document was applied only 'to traffic and location data' and 'to related data necessary to identify the subscriber or registered user'[104].

The Directive was not applicable to the 'content of electronic communications, including information consulted using an electronic communications network'[105]. It makes us clearly understand that metadata is different from content. Judith Rauhofer underlines that metadata 'includes data such as when and where the communication is made, rather than what the message itself is about'[106]. Svetlana Lane adds to the discussion saying that 'metatadata is information or documents about communications, as opposite to their content or substance'[107].

One more legally important factor is that metadata belongs to the category of 'personal data'[108] in the meaning of Article 4 of the GDPR, because it can easily be 'linked to a natural person'. Therefore, it shall receive the bundle of protection defined for that type of data. The principles of processing such personal data are also defined by the GDPR framework.

3.2 Importance of metadata

Metadata has extreme importance, because 'if enough communications data is retained for a sufficiently lengthy period of time, it is possible to gain a complete picture of the individuals to whom it relates, their actions and their beliefs'[109]. According to Judith Rauhofer communications data 'allows the identification of behavioural patterns for the purpose of profiling individuals'[110]. Another similar thought is presented by W. Mbioh who summes up that metadata can 'reveal a great deal about the social, personal and political lives of individuals'[111].

Caspar Bowden claims that metadata is clearly a 'complete map of private life: everyone one talks to (by e-mail and phone), everywhere one goes (mobile phone locations co-ordinates), and everything one reads online (website browsed)'[112]. A similar thought was presented by Kai Bierman: metadata, indeed, 'reveals an entire life'[113]. Metadata in its essence constitutes extremely valuable thing for real deep understanding of the person, its motives for actions and

[104] Data Retention Directive, Article.1, paragraph 2.
[105] Ibid.
[106] Rauhofer 2009, p. 575.
[107] Lane 2016.
[108] GDPR, Article 4.
[109] Rauhofer 2009, p. 576.
[110] Ibid.
[111] Mbioh 2017, p. 274.
[112] Bowden, 2002.
[113] Biermann 2011.

lifestyle. The same was recognized by the CJEU in its case law: metadata 'as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them'[114].

A great example of metadata providing precise conclusions about personal life can be seen from the Malte Spitz case. A German citizen has sued a German telecom giant Deutsche Telekom after they have presented him a hand over six months of his phone data[115]. The metadata collected revealed on a hour-to-hour basis complex information: where the user were, whom he made calls to, when he was offline and other personal data.

In comparison to the content metadata is recognized as 'more revealing than content'[116], because 'content may be what we say, but metadata is about what we actually do'[117]. In the opinion of Matt Blaze 'unlike our words, metadata doesn't lie'[118]. In the technical sense metadata provides 'the availability of historical data'[119], therefore, it is based on the activities which already happened. Again, Matt Blaze claims that 'Metadata is our context. And that can reveal far more about us – both individually and as groups – than the words we speak.[120]' Content might touch from 2 to several individuals and is not always true. Indeed, content is subject to interpretation; it can also be a made-up story, lie or not fulfilled plan. In contrast, metadata, if collected in systematic way, is a strict protocol of actions. We can compare content and metadata to words and actions. What is more important, 'metadata can be more helpful for surveillance than content' because 'it is more easily analysed and aggregated'[121]. Svetlana Lane emphasizes that the distinction between the importance of content and metadata 'forms a basis for a common governments' defence, emphasising innocuous nature of metadata and allegedly non-intrusive character of its collection'[122]. In other words, governments always rely on unawareness of the majority of population about the value of metadata to seize social approval for continuation of communications data retention. By claming not touching the content, governments successfully

[114] Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others,* Joined Cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 27.
[115] *How metadata retention works*, published to ZEIT ONLINE by the Malte Spitz, (https://www.zeit.de/datenschutz/malte-spitz-data-retention, Accessed 27th Mar 2019).
[116] Blaze 2017.
[117] Ibid.
[118] Ibid.
[119] Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), Brussels. 18.04.2011, p. 4.
[120] Blaze 2017.
[121] Bernal 2016, p. 246.
[122] Lane 2016.

calm down the society. Indeed, these 'tales for naive' does not represent the truth. A good point with regard to this was made by Paul Bernal: 'metadata is not less intrusive than content: it might best be described as 'differently intrusive'[123].

The importance of metadata will only increase in future as the amount of devices grows; they are becoming interoperable and connected to Internet. Internet of things will lead humanity into a new phase, where metadata will be the only thing that matter. This prediction is supported by Judith Rauhofer who affirms that 'the importance of communications data will increase rather than diminish'[124]. In the light of such imminent developments, the need to regulate metadata usage will become more and more urgent.

3.3 Retention of metadata

Retention of metadata in the context of our research means processing of metadata by communications operators for 'compliance with a legal obligation to which the controller is subject'[125]. In other words, it means withholding of the information about the communication service users, their traffic and location data and later giving access to it for the law enforcement agencies. Communication service providers possess a lot of individuals' metadata because they need it 'to successfully connect your communications'[126].

It is also vital to clarify that according to EU legislation processing means: 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'[127]. As can be logically admitted retention of metadata perfectly fits into this range of activities.

In explaining retention, we might take into consideration the position of Paul Bernal who had indicated that retention of metadata is when law enforcement agencies 'use commercially

[123] Bernal 2016, p. 246.
[124] Rauhofer 2009, p. 577.
[125] GDPR, Article 6, paragraph 1, (c).
[126] *Why metadata matters?* Electronic Frontier Foundation, 21 March 2019, (https://ssd.eff.org/en/module/why-metadata-matters, accessed 27th Mar 2019).
[127] GDPR, Article 4, (2).

gathered data and commercial surveillance' and 'benefit from the profiling and analysis methods of commercial operators'[128].

In Europe the obligation for retention of metadata is created by the national legislations in Member States. The Evaluation report on the Data Retention Directive, claimed that 'data retention is a valuable tool for criminal justice systems and for law enforcement in the EU'[129]. Moreover, it is 'among the criminal investigation tools necessary to equip law enforcement authorities to address contemporary crime challenges in their diversity, volume and speed in a manageable and cost-efficient manner'[130].

Retention of metadata is clearly understood through the objective as it is meant to be a tool for providing security 'in the face of an imminent threat'[131]. Member States recognize that the role of data retention is 'very important' and some crimes 'might never have been solved'[132] without it. Also it helps in 'acquittals of innocent persons'[133] and, in this sense, the reduction of intrusion into privacy. 'Location data […] exclude suspects from crime scenes and to verify alibis. This evidence can therefore remove persons from criminal investigations, thus eliminating the need for more intrusive inquiries, or lead to acquittals at trial'[134]. As a proof for that, 'Germany, Poland, Slovenia, UK claimed that the use of retained data helped to clear persons suspected of crimes without having to resort to other methods of surveillance, such as interception and house searches, which could be considered more intrusive'[135].

Metadata retention, indeed, can play beneficial role for society. Investigating crimes had never been easier than today. At the same time, governments tend to use metadata retention for control purposes, and that is the situation which shall find solution. Civil society and legal scholars upraise the issue that unlimited metadata retention is an unacceptable threat for the fundamental right to privacy and a tool of control. Illustrative is the case when governments are asked directly by members of civil societies 'are you using metadata retention as a method of control?' the

[128] Bernal 2016, p. 247.
[129] Evaluation report on the Data Retention Directive (Directive 2006/24/EC), Brussels, 18th of April 2011, COM(2011) 225 final, p. 1.
[130] Ibid, P.25.
[131] See arguments in *Privacy International v FCO, Home Office & GCHQ & Others,* [2017] IPT/15/110/CH.
[132] Evaluation report on the Data Retention Directive (Directive 2006/24/EC), Brussels, 18th of April 2011, COM(2011) 225 final, p. 31.
[133] Ibid, p. 31.
[134] Ibid, p. 24.
[135] Ibid, p. 23.

most typical answer of the state officials, according to Paul Bernal, can be described as 'neither confirm nor deny'[136].

The authorities do not want to give up blanket data retention practices, because, as formulated by Kai Bierman: '[p]ossibilities offered by such seemingly harmless data are just too seductive'[137]. Metadata in hands of security agencies can help them influence any person's behavior. While in Europe, where the majority of states are built on the principle of balance of powers it constitutes only disturbing tendency, in more authoritarian states, this can be a disaster, comparable only with George Orwell's '1984'.

The fight on blanket communications data retention between conscious society members and governments occurs not only in debates. Lydia Morgan states that in Europe the governments argue against the courts' positions that 'national security is the paramount government responsibility and sits squarely within the realm of prerogative power. In other words, the courts, UK or European, have no business of telling the government what it can and cannot do.'[138]

James Rule convinces that governments also do not want to put the data retention to public scrutiny. He claims that [c]learly many organizations— law enforcement and intelligence agencies, most obviously— would zealously insist that their record-keeping must remain secret and unaccountable to those targeted in it[139]'. The total governments' rejection of the dispute on whether the retention of metadata shall be available to public scrutiny is seen from the situation around Edward Snowden. As soon as the former NSA agent raised a question about the appropriateness of blanket data retention facilitated through the NSA programs, he was declared a state traitor and had to flea from USA.

Blanket metadata retention regimes are successfully functioning in United States of America (hereinafter – the USA or America) and Russian Federation (hereinafter – Russia). The conditions of this 'mass surveillance' in the USA can be seen from the cases like *Hepting v. AT&T* and *Jewel v. National Security Agency*, where plaintiffs claimed that monitoring the communications of users, through interception and copying of internet backbone

[136] Bernal 2016, p. 246.
[137] Biermann 2011.
[138] Morgan 2018.
[139] Rule 2007, p. 24.

communications stream[140], contradicts the Constitution of America. A disturbing tendency is coming also from Australia, where recently legislators offered a law which will establish a 'mandatory blanket collection and potentially indefinite retention of personal data (with a minimum requirement of two years)'[141].

American cases show that the government (which participates as a defendant in *Jewel case*, but only as a third party in *Hepting case*) is highly reluctant to accusations in abuses of metadata retention. Moreover, the state is likely to avoid public reviewing of the metadata retention cases by claiming that litigation 'would require the government to disclose privileged "state secrets" and that it [is] immune from suit.'[142]

In Russian Federation the situation is even more severe, because with imposition of new laws[143]: the retention is not only aimed for metadata, but also for content. In case *Zakharov v. Russian Federation*[144] the European Court of Human Rights found lots of failures in Russian legislation regarding limitations and providing guarantees from illegal data retention, which made possible to assume that the interventions into privacy by state security services are highly admissible and real.

Unlimited use of retained metadata has proven itself to be no different from surveillance. If we consider surveillance to be 'the watching, listening to, or recording of an individual's activities'[145], as provided by Daniel J. Solove, then it seems that metadata retention perfectly fits into this definition. Unrestricted metadata retention and surveillance are considered to be one thing by UK scholar Paul Bernal. He calls blanket metadata retention 'communications surveillance'[146] and emphasizes that metadata retention belongs to 'new' forms of surveillance'[147]. This point of view is demonstrated despite the facts that 'there do appear to be some identifiable characteristics that differentiate these forms of surveillance [metadata

[140] *Carolyn Jewel v. National Security Agency*, (complaint), no. 4373 CRB, U.S. (2008), see Apellants' Opening Brief, referring to PCLOB Report explaining the technology of interception, p. 18.
[141] Lane 2016.
[142] Electronic Frontier Foundation, *NSA Spying on Americans, Jewel v. NSA*, (https://www.eff.org/cases/jewel, Accessed: 16th Dec 2018).
[143] See for instance, Russian federal bills, 374-FZ and 375-FZ, also known as 'Yarovaya package'. See also Electronic Frontier Foundation, Russia asks for the impossible with its new surveillance laws, 19th July 2016, (https://www.eff.org/deeplinks/2016/07/russia-asks-impossible-its-new-surveillance-laws, Accessed 6th Jun 2019).
[144] *Zakharov v. Russian Federation*, no. 47143/06, ECHR 2009-X.
[145] Solove, 2006, p. 490.
[146] Bernal 2016, p. 244.
[147] Ibid, p. 244.

retention] from the more 'traditional' techniques such as analogue phone-tapping, photography, listening devices and so forth[…]'[148].

Retention of metadata will always be a divisive topic - it is attractive as a crime-fighting tool for police and spooks, but also raises the hackles of privacy advocates who argue that the ends do not justify the means[149].

Average user might ask: what can be done to make it more just and less disturbing? The best solution up to now is to forbid blanket metadata retention, but allow usage of this tool in a very narrow range of situations. Usage of metadata retention shall be limited to certain people, accompanied with relevant safeguards and guarantees. This is the path walked by European Union in the development of its metadata retention framework. We will have a precise look at European Union way to deal with communications data retention in the next part of this chapter.

3.4 Data retention practices in the European Union

In European Union the blanket metadata retention was a general practice. Member States decided the issue of metadata retention on their own discretion: the rules varied from state to state. The limitations for usage of metadata retention were relatively loose. For example, before the Data Retention Directive came into force (official European Union unifying law for data retention), the Irish national law established the regime of retention for 6 years[150], 4 years, 3 years and had foreseen other severe conditions[151]. Imagine having your communications data be stored for 6 years. It is disproportional and extremely costly for communication service providers. Member States like Slovakia, Austria, Sweden were known for their contradictory laws regulating data retention.

3.4.1 Data Retention Directive

Data Retention Directive appeared in 2006 as an effort of the European Union to unify the laws of Member States in aspects of metadata retention. This piece of Union legislation had positive and negative effect on the state of privacy in the EU. Positively, the Directive restricted the terms

[148]Ibid, p. 246.
[149] Reilly 2014.
[150] Statement by Joe Meade, Data Protection Commissioner at the Forum on the Retention of Communications Traffic Data on 24 February 2003, (https://www.dataprotection.ie/docs/Press-Release-Retention-of-Communications-Traffic-Data/i/224.htm, Accessed: 12th Dec 2018).
[151] McIntyre 2008.

of retention to shorter periods than were existent in some of the Member States (like mentioned before Ireland); but, negatively, it established an obligation to create retention laws in the states, where this practice was unknown or not developed.

The main objective of the document was removing 'distortions in the internal market'[152]. The Directive in its recitals recognized that retention provisions had already existed in national legislations of Member States, but '[t]he legal and technical differences between national provisions … present obstacles to internal market.'[153] Therefore, such situation 'led to the enactment of the Data Retention Directive'[154].

Aim of the mentioned Directive was constructed as following:

'to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.'[155]

The Directive was creating a regime where all publicly available electronic communication service providers were obliged to retain (in other words copy and store) all communication data about all users for at least 6 months period. This legislation covered 6 types of metadata that fall within the retention obligation:

> *'(a) data necessary to trace and identify the source of a communication;*
> *(b) data necessary to identify the destination of a communication;*
> *(c) data necessary to identify the date, time and duration of a communication;*
> *(d) data necessary to identify the type of communication;*
> *(e) data necessary to identify users' communication equipment or what purports to be their equipment;*
> *(f) data necessary to identify the location of mobile communication equipment;'*[156]

If to translate these categories into more simple language, the Directive required providers to retain data about: a) who? (phone number/Internet service name/IP of the user); b) to whom? (phone number/Internet service name/IP of the receiver); c) when? for how long? d)

[152] Evaluation report on the Data Retention Directive (Directive 2006/24/EC), Brussels. 18.04.2011, p. 4
[153] Data Retention Directive, paragraph 6.
[154] Woods 2016.
[155] Data Retention Directive, Article 1.
[156] Data Retention Directive, Article 5.

texted/called or Internet called/messaged? e) from what device? (computer, phone, tablet, e-book, etc) f) which connection point were used to perform communication (precise location of the user and receiver of the communication).

A telephone number present mass information about individual, because the number allows to actually defining the subscriber. In the meaning of the GDPR, it belongs to the category of personal data, because it constitutes 'information relating to an identified or identifiable natural person'[157]. If someone can access the number, it is most probable that the name of the subscriber is also no more a secret. The chain continues to the fact that 'a name can provide the key to a broad array of information about the person […]'.[158] At minimum, it will give you the chance for assuming basic issues about the person: first of all, person's sex (male or female), nationality or religious and ethnical origin. For instance, name 'Roosa' is typical only for Finnish lady, while Mohammed could seldom belong to someone who is not somehow connected with Islam. These issues alone, obviously, constitute the part of privacy matters which are protected by article 7 and 8 of the CFREU. Data retention regime which was offered by the Directive appeared to be too threatening to the essence of privacy in the EU. Moreover, as was discussed before, metadata is much more revealing than content.

Reaction of the society and Member States

The directive enforced was negatively estimated by the European Data Protection Supervisor, who 'expressed doubts about the necessity of the measure'[159]. He claimed that the European Directive on Data Retention 'does not meet the requirements imposed by the fundamental rights to privacy and data protection'[160].

Irish Community tried to stop the action of Data Retention Directive in CJEU. Claimants were contesting the legality of directive 'on the basis that the principal objective was the investigation, detection and prosecution of serious crime'[161]. The real aim of the Directive was, indeed, a disputable aspect. Taking into consideration the fact that '[t]he EU adopted the Directive at a

[157] GDPR, Article 4.
[158] Opinion of Justine Stevens in *Hiibel v. Sixth Judicial District Court*, 542 U.S. 177, 189, 190-91 (2004).
[159] Evaluation report on the Data Retention Directive (Directive 2006/24/EC), 18.04.2011 COM (2011) 225 Final, p.29.
[160] Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), European Data Protection Supervisor, 31 May 2011.
[161] *Ireland v Parliament and Council*, C-301/6, EU:C:2009:68.

time of heightened alert of imminent terrorist attacks'[162], it is doubtful that the aim of removing obstacles of internal market was the case. The action was made to claim that the Directive was put into force on the wrong objective: removing obstacles for internal market, while the true objective was fighting crimes. In that case[163], the outcome was negative; the CJEU confirmed that Directive was adopted on an appropriate legal basis.

In addition to Irish efforts, whole European Union's society was against the implementation of Data Retention Directive, because of obvious privacy infringements. The Directive, which was validated as a European Union 'federative' law on the 13 of April 2006, seemed to be very controversial from the very beginning and 'has faced intense criticism'[164], especially, in Ireland and Germany[165], as it aimed for retention of unquantifiable data from all public available communication services and regarding all users without any exceptions and limitations. In Germany, the society reacted extremely sharp and even won a case. The Court of Wiesbaden rendered that 'data retention violates the fundamental right to privacy. It is not necessary in a democratic society. The individual does not provoke the interference but can be intimidated by the risks of abuse and the feeling of being under surveillance…'[166] As a result of that the same court recognized that 'directive does not respect the principle of proportionality guaranteed in Article 8 ECHR, which is why it is invalid'[167].

Another country where the Directive created resonance was Austria; '[t]he Austrian Constitutional Court (CC) had before it several actions filed by a large number of applicants seeking the annulment of the Austrian telecommunications law that transposed the Data Retention Directive into national law'[168]. Indicative of the controversial nature of the Directive, many Member States faced domestic obstacles in the process of transposing the Directive into national law. The European Commission chose to bring infringement actions against Greece, the Netherlands, Sweden, and Austria[169] for not transposing the Directive into national systems.

---

[162] Evaluation report on the Data Retention Directive (Directive 2006/24/EC), 18.04.2011 COM (2011) 225 Final, p.30.
[163] *Ireland v Parliament and Council*, C-301/6, EU:C:2009:68.
[164] Electronic Frontier Foundation, *How Digital Rights Ireland Litigated Against the EU Data Retention Directive and Won*, (https://www.eff.org/node/81899, Accessed: 8th Dec 2018).
[165] Deutsche Welle World, *"Germans file mass lawsuit against sweeping data retention law"*, 31 December 2007, (http://www.dw.com/en/germans-file-mass-lawsuit-against-sweeping-data-retention-law/a-3025009, Accessed: 12th Dec 2018).
[166] Administrative Court Wiesbaden, Decision of 27th February 2009, Az 6 K 1045/08. WI.
[167] Ibid.
[168] Library of Congress, *European Union: ECJ Invalidates Data Retention Directive*, (http://loc.gov/law/help/eu-data-retention-directive/eu.php, Accessed: 14th Dec 2018).
[169] Feiler 2010.

The reaction of Member States' governments on validating the Directive was a bit different: they understood that by supporting metadata retention they will gain two invaluable instruments: firstly, legitimate advanced tool for criminal prevention, investigation and prosecution and, secondly, legal, but not legitimate, tool for mass surveillance. During the voting for Data Retention Directive general 'surveillance' provisions were welcomed by governments, however, some Member States (like Ireland and Slovakia) also tried to sabotage the voting for implementation because the authorities realized that despite enabling mass data retention, EU regulation will take away the autonomy from the Member States to decide the matter on their own. This appeared to be a huge issue, because before the Data Retention Directive (with retention period measurements: from 6 months to 24 months), Ireland enjoyed the rule, by which it obliged publicly available communication services to retain data for the period of 3 years[170]. This aspect matters when one analyze how many international communication companies are located in Ireland.

In the next 2 parts of this subchapter we will have a look at two landmark cases which are considered to be a continuation of one long process of re-estimating the surveillance in Europe. Both of the cases are touching the metadata retention before and after the cancellation of Data Retention Directive.

3.4.2 Digital Rights Ireland case

Firstly, it shall be mentioned that *Digital Rights Ireland* is a case that was aimed to give answer 'whether the Data Retention Directive is valid within the scope of provided by EU right to privacy'. The inquiry for this case derives from two Member States: Ireland and Austria.

In Ireland the non-governmental organization, Digital Rights Ireland, sued the Ministry of Justice, Law and Reform before the Irish High Court, because the Criminal Justice (Terrorists Offences) Act (2005) allowed Irish national security service Gardaí to access the data of DRI's users without having a specific crime to investigate. The organization was disturbed by the unrestricted ability of security services to have access to private data of the users. To decide the matter the Irish High Court addressed the CJEU with the question 'regarding the legality of national legislative and administrative measures concerning the retention of data relating to electronic communications.'[171]

[170] McIntyre 2008.
[171] Judgment of 8 April 2014, *Digital Rights Ireland*, Joined cases C-293/12, C-594/12, EU:C:2014:238, paragraph 2.

In Austria the Constitutional Court faced a landmark lawsuit from the State Government of Carinthia and 11 131 individual claimants. The applicants trying to challenge the validity of the Directive, forced the Austrian Constitutional court (Verfassungsgerichtshof) to refer to Court of Justice of the European Union 'regarding the compatibility with the Federal Constitutional Law (Bundes-Verfassungsgesetz) of the law transposing Directive 2006/24 into Austrian national law[172].'

As it was mentioned before the CJEU declared as a main task – 'examine the validity of Directive 2006/24 in the light of Articles 7, 8 and 11 of the Charter'[173]. Although the Court recognized the potential impact of data retention on freedom of expression, it chose not to examine the validity of the Directive in light of Article 11 of the Charter[174].

After examining the relevance of these Charter provisions with regard to the validity of the Data Retention Directive, considering whether there was an interference with the rights laid down in Articles 7 and 8 of the Charter, assessing whether these interferences with the Charter rights to privacy and data protection were justified[175] the ECJ declared the Data Retention Directive invalid because of mass infringements of CFREU. After that '[i]n several Member States, the domestic implementation laws were declared unconstitutional by constitutional courts'[176]. The CJEU emphasized that Data Retention Directive respected the essence to the right to privacy, as it required proper data protection measures and other safeguards. Also the CJEU approved that the Directive as such satisfied the objective of general interest. At the same time it declared that Directive violates the principle of proportionality. The document did not establish any limitations for people concerned, types of communication data and means of communication in question. In addition, the Directive failed to install objective criteria for defining who can access the data, how to differentiate the time period and how to secure data from abuse or illicit access.

3.4.3 Tele2&Watson case

Tele2&Watson is a case-continuation of the dispute about legality of blanket metadata retention in European Union. As we know after the Digital Rights Ireland case the Data Retention Directive became invalid. After the annulment in the majority of Member States 'the conditions

[172]Judgment of 8 April 2014, *Digital Rights Ireland*, Joined cases C-293/12, C-594/12, EU:C:2014:238, paragraph 3.
[173] Ibid, paragraph 23.
[174] Lynskey (A) 2014.
[175] Ibid.
[176] Vainio – Miettinen 2015, p. 290.

– in particular those identified in *DRI* – were not satisfied'[177]. EU Member States continued to regulate the retention questions in accordance with their national laws. As soon as all the national laws were amended to comply with Data Retention Directive, the national authorities faced a new challenge: Member State retention laws' validity was under threat. The domino principle: Data Retention Directive lost its judicial power, so the next cell of the chain to be circumvented is national legislation, which transposed that directive. For Member States there were 2 ways out: 1) to amend the national law to consider requirements installed by the DRI case and conditions of Privacy and Electronic communication Directive; OR 2) to continue using the same legislation with a risk of a lawsuit. Some Member States until now continue to enforce the obligation which indirectly leads to mass metadata surveillance.

Tele2Watson case is a joined case from 2 Member States: Sweden and the UK.

In Sweden:

The next day after the Data Retention Directive annulment in *Digital Rights Ireland* case, one of the communication service providers –'Tele2 Sverige, stopped retaining communications data, on the basis that the applicable Swedish law (Chapter 6 of Sweden's Law on Electronic Communications) no longer conformed to European fundamental rights law'[178]. Moreover, they sent a notification that they will delete all previously retained data. Indeed, the act which obliged communication providers to save the metadata was annulled; it comes logically that national requirements based on that directive became void as well. Tele2 Sverige decided to keep the rule of law on the level which was required by the Privacy and Electronic Communication Directive: to erase the recorded communication 'as soon as possible and in any case at the latest by the end of the period during which the transaction can be lawfully challenged'[179]. Such a choice by one of the Swedish communication providers was understandable, because the costs for retaining the copies of all the communications are colossal: 'the cost of setting up a system for retaining data for an internet service provider serving half a million customers to be around €375 240 in the first year and €9 870 in operational costs per month thereafter[180], and the costs of setting up a

[177] Woods 2016.
[178] Case analysis, Global Freedom of Expression, Columbia University, Joined Cases Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v. Watson, (https://globalfreedomofexpression.columbia.edu/cases/joined-cases-tele2-sverige-ab-v-post-och-telestyrelsen-c-20315-secretary-state-home-department-v-watson/ accessed 9th Apr. 2019).
[179] Privacy and Electronic Communications Directive, paragraph 23.
[180] Gansterer –Ilger 2008.

data retrieval system to be €131 190, with operational costs of €28 960 per month.'[181] Retention required a lot of additional money, staff members and data protection solutions. Swedish governmental authorities were not satisfied with such a notification of non-compliance with national legislation. The Swedish law still required 'the providers of electronic communications services to retain, systematically and continuously, and with no exceptions, all the traffic data and location data of all their subscribers and registered users, with respect to all means of electronic communication'[182]. Swedish National Police Board was afraid to face a big problem with non-compliant communication operators and without a comfortable tool to fight crimes; therefore, they sent a complaint to Post and Telecom Authorities. As a result Swedish Post and Telecom Authority (Post-och telestyrelsen) filed a lawsuit against the Tele2Sverige in front of the Court. The case, after it reached the Administrative Court of Appeal in Stockholm, was addressed to the CJEU for a preliminary ruling. The Swedish court formulated the questions like this:

'(1) Is a general obligation to retain traffic data covering all persons, all means of electronic communication and all traffic data without any distinctions, limitations or exceptions for the purpose of combating crime ... compatible with Article 15(1) of Directive 2002/58/EC, taking account of Articles 7 and 8 and Article 52(1) of the Charter?

(2) If the answer to question 1 is in the negative, may the retention nevertheless be permitted where:

(a) access by the national authorities to the retained data is determined as [described in paragraphs 19 to 36 of the order for reference], and

(b) data protection and security requirements are regulated as [described in paragraphs 38 to 43 of the order for reference], and

(c) all relevant data is to be retained for six months, calculated as from the day when the communication is ended, and subsequently erased as [described in paragraph 37 of the order for reference]?'[183]

In the United Kingdom

Digital Rights Ireland judgment of CJEU also 'prompted proceedings in the U.K. and an application was made to the High Court requesting judicial review of the U.K.'s data retention

[181] Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), 18.04.2011 COM (2011) 225 Final, p. 26.
[182] Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others,* Joined Cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 51
[183] Judgement Tele2&Watson case, para. 51.

regime as set out in the Data Retention and Investigatory Powers Act (DRIPA)'[184]. The requirements placed by the DRIPA were indeed much wider than what was allowed by CJEU interpretation in DRI case. The group of individuals filed a lawsuit to the UK High Court. The national authorities lost the case in the High Court of Justice (England & Whales), but, UK Home Department brought proceedings in the Appeal Court claiming that CJEU 'had not laid down specific mandatory requirements of EU law with which national legislation must comply'[185]. As a result, it is up to Member states to define the policy of data retention inside the Member State, as soon as they provide appropriate safeguards for the processing of retained data. The period of retention was established as the one which 'must not exceed 12 months'[186]. The national process was postponed until the decision from CJEU would be received regarding the following questions:

'(1) Does [the Digital Rights judgment] lay down mandatory requirements of EU law applicable to a Member State's domestic regime governing access to data retained in accordance with national legislation, in order to comply with Articles 7 and 8 of [the Charter]?

(2) Does [the Digital Rights judgment] expand the scope of Articles 7 and/or 8 of [the Charter] beyond that of Article 8 of the European Convention of Human Rights ... as established in the jurisprudence of the European Court of Human Rights ...?'[187]

Both described cases 'asked about the impact of the DRI reasoning on national regimes, and whether Articles 7 and 8 EUCFR constrained the States' regimes'[188]. In other words: is it in compliance with the European Union law to impose national requirements to metadata retention?

The CJEU confirmed its previous judgment in DRI case that retention on national level of metadata that covers 'all subscribers and registered users and all means of electronic communication as well as all traffic data, provides for no differentiation, limitation or exception'[189] is ***unacceptable*** and in conflict with the European Union law. Also the CJEU clearly highlighted that for the Member States 'retention of traffic and location data is the rule,

[184] Case analysis, Global Freedom of Expression, Columbia University, Joined Cases Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v. Watson, (https://globalfreedomofexpression.columbia.edu/cases/joined-cases-tele2-sverige-ab-v-post-och-telestyrelsen-c-20315-secretary-state-home-department-v-watson/ Accessed 9th Apr. 2019).
[185] Ibid.
[186] Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, Joined Cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 29 p.5.
[187] Ibid, paragraph 59.
[188] Woods 2016.
[189] Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, Joined Cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 105.

whereas the system put in place by Directive 2002/58 requires the retention of data to be the exception'[190]. Metadata retention can only be justified 'if deployed against specific targets to fight serious crime'[191] and when the connection between retained data and suspected crime is proven in front of independent authority (judge or other instance that will approve such a metadata usage). After the decision of the Court in those two cases it became obvious that 'blanket data retention measures are incompatible with EU law, read in light of the Charter'[192]. However, Member States may use targeted data retention if they build the balance correctly. Member State's authorities shall limit the scope of intrusion by restricting: categories of data, means of communication, time period, and amount of people concerned[193]. More precisely about limiting communications data retention is described in Chapter 5 of this work.

3.4.4 Criticism of CJEU decisions on metadata retention

Expanding EU jurisdiction

There has been some criticism with regard to the Courts position in the mentioned cases. From legal perspective, some scholars emphasize that effort to harmonize provisions on metadata retention and forthcoming cases constitute intrusion into the competence of the Member States. For instance, Gunnar Beck thinks that data retention decisions of CJEU constitute intrusion of the EU 'into areas of law that have nothing to do with the EU's classical internal market economic governance competences'[194]. The question of metadata retention intersects with national security and defense and not all of the Member State's representatives and scholars are satisfied with limitations input by the CJEU's decisions in this sphere. Indeed, the States which have more information (or can access more data in an easier manner) are stronger and have so called 'wider hand' not only to fight serious crimes, but also to counteract foreign threats on state's security. As was claimed by Guilia Formici, when referring to Privacy International conclusions, 'compliance with the principles set by the ECJ could frustrate the core of the Security and Intelligence Agencies' activities.'[195]

---

[190] Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, Joined Cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 104.
[191] European Union Agency for Fundamental Rights, *Data Retention Across the EU*, (https://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention, Accessed 10th Apr 2019).
[192] Lynskey (B) 2017.
[193] Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, Joined Cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 108.
[194] Beck 2017.
[195] Formici 2019.

Other feasible solutions

There were scholars who expected the CJEU to decide Tele2&Watson case in a different manner. In the opinion of UK's independent reviewer of terrorist legislation, David Anderson QC, the 'position taken by the ECJ was wholly impracticable: what Watson et al. had been wanting was much tighter controls on access, not an end to general retention'[196]. This opinion has rational seed: general retention in itself does not do any bad or good for an individual. It is the abuse of access by state or not diligent communication service providers that can make general retention dangerous. However, in estimating the threats and modeling the disaster which may occur in case such wide big data is leaked or stolen, the CJEU, in my opinion opted for less harm.

Open questions left by CJEU

Despite the fact that two described decisions are 'game-changer for state surveillance in Europe'[197], CJEU still left some questions unanswered. For example, in the decisions there was no mentioning of categorization for time period of retention for different categories of metadata, the court failed to elaborate properly on the concept of 'serious crime', the panel did not specify about the retention of metadata which belong to professional secret and using metadata for search and rescue purposes, the CJEU did not comment on the objective criteria for limiting geography of retention appropriately. As a result of these ambiguities, the Court met criticism. For instance, Gunnar Beck exclaimed that 'the Court implicitly opened the door to further legal uncertainties and future litigation'[198]. The scholar doubts that 'the question of data retention for the benefit of anti-terrorist agencies has been settled for good, or even for long.'[199] As was mentioned before, CJEU nowadays is facing a chain of new requests for preliminary rulings with regard to communications data retention from Belgium[200], Estonia[201] and France[202]. They are all connected to the gaps left unanswered by the CJEU. For instance, Belgian case is asking about 'serious crime' clarifications[203]. The Estonian Supreme Court with regard to internal case 'Prokuratuur' asked about applicability of metadata retention in criminal cases of minor gravity

[196] Cameron 2017, p. 1494.
[197] Lynskey (B) 2017.
[198] Beck 2017.
[199] Ibid.
[200] Belgian Constitutional Court (Case C-520/18).
[201] Supreme Court of Estonia (Case C-746/18).
[202] Conseil d'Etat in France (Case C-511/18).
[203] More precisely you can see the questions at: http://curia.europa.eu/juris/document/document.jsf?docid=207616&doclang=en, Accessed 06th Nov 2019).

and time period of metadata retention. The French case is connected with clarifying the questions of applicability of metadata retention for the sake of protecting state security and data protection measures to be taken during such activities.

As we see the gaps left after the CJEU rulings are significant and need scientific research, our next chapters 4 and 5 are devoted to discussion of these gaps and how to build the national laws to be in compliance with European Union law.

4. CONDITIONS FOR LIMITING PRIVACY BY MEANS OF METADATA RETENTION

If any Member State of the European Union strives for using data retention as a tool of executing its powers in investigation, prosecuting crimes; fighting terrorism or providing public security, such Member State shall strike appropriate balance between data retention and right to privacy. In other words, if by data retention the Member State wants to intrude into privacy rights it shall comply with limitations imposed by Article 52(1) of the Charter of Fundamental Rights of the European Union. Namely, such interference: 'must be provided for by law and respect the essence of those rights and freedoms.' These interferences shall be the '[s]ubject to the principle of proportionality and […] 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.[204]' In this chapter we will discuss each condition for limiting privacy by metadata retention.

4.1 General interest

One of the objectives of general interest recognized by the European Union, and consequently by every Member State, is public security. Fighting serious crimes and fighting terrorism can be claimed a grave objective of general interest. This derives not only from the essence of Treaty on the European Union, Treaty on Functioning of the European Union and Charter of Fundamental Human Rights, which by Article 6 claims that: 'Everyone has the right to liberty and security of person'[205], but also from the CJEU case law: *Kadi*[206], *Al-Aqsa*[207]and *Tsakouridis*[208]. Two first cases are proving that fighting terrorism, maintaining international peace and security can be accepted as objective of general interest, while the third case is proving the same message, but with regard to ensuring public security. Coming out from such argumentation, the ECJ concludes that data retention law (performed in a way which was foreseen by Data Retention Directive) 'satisfies an objective of general interest'[209].

---

[204] CFREU, Article 52(1).
[205] Ibid, Article 6.
[206] Judgment of 3rd September 2008, *Kadi and Al Barakaat International v Council and Commission,* C-415/05 P, EU: C: 2008:461, paragraph 363.
[207] Judgment of 15th November 2012, *Al-Aqsa v. Council,* Joined cases C 539/10 P and 550/10 P, EU:C:2012:711, paragraph 130.
[208] Judgment of 23rd November 2010, *Land Baden-Württemberg v Panagiotis Tsakouridis*, C-145/09 EU:C:2010:708, paragraphs 46, 47.
[209] Judgment of 8 April 2014, *Digital Rights Ireland*, Joined cases C-293/12, C-594/12, EU:C:2014:238, paragraph 44.

From governmental point of view, this argumentation, claiming for satisfaction of general interest, is very convincing and necessary, but there are some other thoughts on this matter. For example, some scholars, like Orla Lynskey, clarified that the most disappointing aspect of the *Digital Rights Ireland* case is that the CJEU 'does not query the appropriateness of data retention as a tool to fight serious crime'[210]. Instead, the CJEU accepts the fact that: 'data which must be retained pursuant to that directive allow the national authorities […] to have additional opportunities to shed light on serious crime and, in this respect, they are therefore a valuable tool for criminal investigations'[211]. Nevertheless, while CJEU failed to address the question of general interest in the DRI case, it fully explained it in the following case of *Tele2&Watson*.

Indeed, significant attention to the question of general interest was raised in the *Tele2&Watson* case. As seen from the case, the CJEU outlined 2 criteria for using general interest as objective:

1) the list of general interests is limited to safeguarding 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[212]; the exhaustiveness of this list was confirmed by the *Promusicae*[213] case delivered on the 29th January 2008. *Tele2&Watson* case had only approved that 'Member States cannot adopt such measures for purposes other than those listed'[214].

2) the last objective from the list is only applicable if the government aims for fighting serious crime; this derives from the position of the CJEU that 'only the objective of fighting serious crime could justify national data retention legislation'[215].

In *Tele2&Watson* case, the CJEU has analyzed Swedish law and the law of the United Kingdom and had drawn few conclusions from such analysis. First of all, it concluded that neither Swedish nor British law applied the concept of general interest correctly. Swedish law used metadata retention for investigation of wrongs which did not belong to the category of 'serious', while in the UK the list of general interests was not exhaustible.

---

[210] Lynskey (A) 2014.
[211] Judgment of 8 April 2014, *Digital Rights Ireland*, Joined cases C-293/12, C-594/12, EU:C:2014:238, paragraph 49.
[212] Privacy and Electronic Communications Directive, Article 15 (1).
[213] Judgment of 29th January 2008, *Productores de Música de España (Promusicae) v Telefónica de España SAU*, C-275/06, EU:C:2008:54 paragraph 53.
[214] Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others,* Joined Cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 90.
[215] Ibid, paragraph 102.

To be more precise, in Sweden, for using the retained metadata 'it is not necessary that the offence be a serious crime'[216]. In Swedish law, the national authorities can have access to the retained metadata when the investigated cases are 'offences punishable by a sentence of imprisonment of at least six months'[217]. What is more, in case the 'offence punishable by a sentence of imprisonment of at least two years'[218], the security agencies had access even to the content of the communications. This last fact is interesting, because if security agencies access the content of communication, then the respect to the right to privacy is violated and cannot anyhow be justified in a democratic society.

In the logic of many countries offences which foresee as a main punishment the imprisonment for the term up to 2 years is a crime of minor gravity[219]. Crimes which lead to punishment of up to 6 months of imprisonment obviously do not belong to the category of serious crimes. As an example, in the UK, 'serious crime is defined widely as any offence for which the person without any previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more'[220]. Despite the fact that Swedish penal code does not have a formal categorization of crimes by the seriousness, it obviously does not attribute a punishment of 6 months of imprisonment to a wrong that is recognized a serious crime[221].

In the law of the United Kingdom metadata retention regime was discriminatory, which is compliant with EU law, but the list of general interests that can be used to justify the use of metadata retention was extremely wide. It included: national security, preventing or detecting crime or of preventing disorder, economic well-being of the United Kingdom, public safety, protecting public health, assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department, emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health, any other purpose which does not belong to previously named categories, but are defined by the order of the secretary of state[222].

---

[216] Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others,* Joined Cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 25.
[217] Ibid, paragraph 26.
[218] Ibid, paragraph 27.
[219] See for instance Criminal Code of Ukraine, Article 12 part 2.
[220] Rauhofer 2009, p. 596.
[221] See for instance Swedish Penal Code, 1962, (https://www.government.se/contentassets/5315d27076c942019828d6c36521696e/swedish-penal-code.pdf, Accessed 6th Apr 2019).
[222] Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others,* Joined Cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 33.

Basically, the list was quite decent until we read the last point, where the UK government leaves to itself discretion for unlimited use of metadata retention. The wording 'any other purpose' in combination with 'defined by the order of the secretary of state' proves the limitless nature of metadata retention. With this opinion also agrees Will R Mbioh, who claims that because of this last provision 'Secretary of State can order the generalised retention of the metadata of all electronic communications transmitted or stored by operators of public networks.'[223]

As was mentioned before, in both Swedish and British jurisdictions the rules establishing the use of metadata retention for the sake of general interest were incompliant with EU legislation. The United Kingdom approach jumped out of that as they wanted the Secretary of State to decide when data retention is admissible; in other words, when metadata retention meets the criteria of general interest. While in Sweden the retention practices were not limited to usage only in 'serious crime' investigations.

The question of what can be a general interest is profound question in the PRISM-aftermath period[224]. Basically, it is a dispute on the effectiveness of blanket data retention (to which Data Retention Directive and many Member State laws were/are a part). The statements about ineffectiveness of mass data retention come from scholars; for example, Jeremy Malcolm claims that metadata retention 'provided minimal benefit in combating terrorism, and that traditional investigation techniques remain the most effective. There is no reported case in which metadata collection has helped prevent an actual terrorist attack or helped dismantle a terrorist network'[225]. Insightful opinion of Yochai Benkler confirms that 'bulk collection has never made more than a marginal contribution to securing Americans from terrorism, despite its costs'[226]. Benkler presented an argument that in US the Congress questioned the NSA representatives about the effectiveness of domestic surveillance program; consequently, it appeared to be the case of Basaaly Moalin (a guy sending 8,500 dollars to support al-Shabaab in Somalia) was 'the sole success story' for the NSA bulk domestic surveillance program'[227].

[223] Mbioh, 2017, p. 278.
[224] PRISM-aftermath is a period which started after the USA NSA whistleblower Edward Snowden leaked the data about US government's universal mass-surveillance. In his interview to the program: "Vice on HBO", Edward Snowden stated about having the widest meta-data: "we know for fact, that is not effective for stopping terrorist attacks and it never has been", time: 21:51 (out of 26:55), Interview (https://www.youtube.com/watch?v=ucRWyGKBVzom, Accessed: 11th Apr 2019).
[225] Reilly 2014.
[226] Benkler, 2013.
[227] Ibid.

Interesting evaluation can be found in American analytical circles; two independent reports: "Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies" by American National Security Agency, and "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act" by Privacy and Civil Liberties Oversight Board, constituted that society's primary task is to 'maintain a secure and open Internet[228]' and 'declassify information[229]', which is retained by security agencies. Summed up conclusion from mentioned reports is that surveillance and security programs like PRISM (that is a main source of metadata for security agencies in the United States) are less of the general interest than privacy issues and freedom of the Internet.

European statistics show a little bit different picture, for instance, '[t]he Netherlands reported that, from January to July 2010, historical traffic data was a decisive factor in 24 court judgments. Finland reported that in 56% of the 3405 requests, retained data proved to be either 'important' or 'essential' to the detection and/or prosecution of criminal cases. Slovenia stated that the absence of retained data would 'paralyze the law enforcement agencies' operation'; a United Kingdom police agency described the availability of traffic data as 'absolutely crucial…to investigating the threat of terrorism and serious crime.'[230]

In my opinion, metadata retention is certainly a crucial tool for investigation, but it has to be admitted that it is only effective for investigation of crimes, which already occurred. Metadata retention, as was already said provide a 'strict historical protocol of actions', therefore, using it for preventive or proactive investigations is quite challenging, if not impossible. What are the differences between a serious crime which is already committed and which is only supposed to be committed in future. The committed crime has geographical location, victims, witnesses, consequences: all these factors allow the security agencies to allocate the zone of effective usage of metadata retention. When the crime is only alleged to happen somewhere – the security agencies are forced to make wide bulk retention. The problem with bulk metadata retention was summarized by Edward Snowden in his interview to programme WICE on HBO: 'when you cast

[228] Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, National Security Agency, pub.12th September 2013, Available at: https://fas.org/irp/offdocs/ict-review.pdf, Accessed: 28th Mar 2019, p. 260.
[229] Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Privacy and Civil Liberties Oversight Board, pub. 2nd July 2017, Available at: https://www.pclob.gov/library/702-Report.pdf, Accessed: 28th Mar 2019, p. 149.
[230] Evaluation report on the Data Retention Directive (Directive 2006/24/EC), 18.04.2011 COM (2011) 225 Final, pp.23-24.

the net too wide, when you are collecting everything, you understand nothing'[231]. Security agencies struggle to use metadata retention appropriately when aimed at prevention of crimes. Bulk metadata retention is only applicable for prevention, which is rarely used appropriately, and targeted metadata retention is enough to investigate the already committed crimes.

4.2 Provided by law

The provisions by which the Member State wish to exercise data retention shall be clearly outlined by laws of the Member State. For the sake of transparency it seems to be reasonable to place all the provisions in a separate act, which refers to all vital issues regarding metadata retention. Practice of such countries as Ireland, Slovakia, USA, Russia, and Ukraine had shown that including provisions on data retention to criminal codes or criminal-procedural acts prevents regular citizens and communication service providers from finding and explicitly understanding their status regarding metadata retention. The law shall specifically designate that the aim and main objective of the document is to provide public security.

The Data Retention Directive established as a main objective: harmonization of internal market. In *Digital Rights Ireland* case, Advocate General clarified that the Directive was built on 'functional duality'. Firstly, the 'predominant' objective served by the Data Retention Directive is to harmonise national rules in order to ensure the proper functioning of the internal market'[232], but, secondly, 'seeks to establish' a duty of retention in Member States[233], basically choosing security as a secondary objective. This scheme is faulty, and need to have security as a first and main objective.

The need for having security as a primary objective was proven by the position of the CJEU in Digital Rights Ireland case. CJEU had confirmed security-objective because using that objective allowed justifying intrusion. The Advocate General stated that in case internal market objective will be taken for the basis, it may fail to justify the interference with privacy rights. In other words: AG 'found that the intensity of the DRD's intervention with regard to fundamental rights (and in particular its 'creating effect' in certain Member States where there was no pre-existing

[231] Edward's Snowden interview to the program: "Vice on HBO", time 21:45 (out of 26:55), Interview (https://www.youtube.com/watch?v=ucRWyGKBVzom, Accessed: 18th Oct 2019).
[232] Opinion of AG Villalon delivered on 12 December 2013, *Digital Rights Ireland*, Joined cases C-293/12 and 594/12, EU:C:2013:845, paragraph 1.
[233] Ibid, paragraph 46.

legislation) was manifestly disproportionate to this objective.'[234] Therefore, it has to be kept in mind, that security shall be stated in the law as the most important objective.

The aim of the document has vital importance, because security objective as a main aim allows limited intrusion into privacy, while benefit for internal market cannot compromise anyhow the interference with such a valuable right as right to privacy.

The law regulating data retention **shall provide** regulating the following issues:

1) Specific definitions on metadata retention

The best option for national law is to establish in clear wording what is metadata (subscriber, traffic and location data). Additionally, it shall define the precise procedure of metadata retention by authorized agencies. It is sensible to clarify how does retention corresponds with processing. In *Tele2&Watson* case, CJEU indirectly recognized that retention is a part of processing. Because of that the Court has not taken into account the position of respondent Member States, who 'argued that the national legislation in question concerned the 'retention' and not the 'processing' of personal data.'[235] The Court was referring to Privacy and Electronic Communications Directive 2002/58/EC, therefore, it considered it relevant to regulating metadata retention relations.

We can define metadata retention as a process of withholding the complex digital data about subscribers communications (including the traffic and location data, data-identifier of the subscriber or registered user) by the communication service provider for the interest of the state (primarily government).' In comparison, '[i]nformation processing refers to use, storage and manipulation of data that has been collected. Processing involves various ways of connecting data together and linking it to the people to whom it pertains. Even though it can involve the transmission of data, processing diverges from dissemination because the data transfer does not involve the disclosure of the information to the public – or even to another person.[236]' As it is seen metadata retention activity logically lies into the scope of processing.

There are few characteristics which describe this type of processing: a) subject of access; b) purpose; c) absence of data subject's consent. Subject of access: security agencies; purpose:

[234] Lynskey (C) 2013.
[235] Beck 2017.
[236] Solove 2006, p. 506.

metadata retention is done for the sake of investigating serious crimes; consent is not asked, because it may 'jeopardize the investigation'.

Another essential thing to specify is 'targeted data retention'? The CJEU in its decision claimed that data retention in blanket variant is precluded, but 'targeted data retention' is allowed[237]. Member States shall clearly define what that is and how by functional scope it is different from blanket retention? In some sources, there is a mentioning of 'data preservation', which, in my opinion, seems to be similar to (if not the same as) 'targeted data retention'. The EU Commission report states that: '[d]ata retention is distinct from data preservation (also known as 'quick freeze') under which operators served with a court order are obliged to retain data relating only to specific individuals suspected of criminal activity as from the date of the preservation order'[238] But in this context the EU Commission discuss the blanket data retention not the targeted. In this statement delimitation between blanket data retention and targeted data retention becomes vital. According to claims of the majority of Member States data preservation in no variations 'could adequately replace data retention', because 'data retention results in the availability of historical data', while 'data preservation does not guarantee the ability to establish evidence trails prior to the preservation order, does not allow investigations where a target is unknown, and does not allow for evidence to be gathered on movements of, for example, victims of or witnesses to a crime.'[239]

When talking about swiping metadata retention broadly, we need to keep in mind that several Member States reported uselessness of such wide data. For example, 'Czech Republic considered data retention 'completely indispensable in a large number of cases'; Hungary said it was 'indispensable in [law enforcement agencies'] regular activities'[240]. If the Member States limit their data retention to certain targets, localization and time (as a method that promises more efficient results), then there is a big doubt if they need a separate national data retention law. Criminal procedures of every EU Member State, undoubtedly, have provisions for data preservation.

---

[237] Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others,* Joined Cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 108.
[238] Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), Brussels. 18.04.2011, p.6. Also see the Convention on Cybercrime, Article 16.
[239] See for instance the decision of German Constitutional Court, when it was annulling the German law transposing the Directive; Bundesverfassungsgericht, 1 BvR 256/08 of 2 March 2010, paragraph 208.
[240] Evaluation report on the Data Retention Directive (Directive 2006/24/EC), 18.04.2011 COM (2011) 225 Final, p.24.

2) What is 'serious crime'?

Establishing a justifiable national data retention practices is impossible without clear definition of what is serious crime. It constitutes a problem for EU, because '[t]en Member States (Bulgaria, Estonia, Ireland, Greece, Spain, Lithuania, Luxembourg, Hungary, Netherlands, Finland) have defined 'serious crime', with reference to a minimum prison sentence, to the possibility of a custodial sentence being imposed, or to a list of criminal offences defined elsewhere in national legislation. Eight Member States (Belgium, Denmark, France, Italy, Latvia, Poland, Slovakia, Slovenia) require data to be retained not only for investigation, detection and prosecution in relation to serious crime, but also in relation to all criminal offences and for crime prevention, or on general grounds of national or state and/or public security. The legislation of four Member States (Cyprus, Malta, Portugal, United Kingdom) refers to 'serious crime' or 'serious offence' without defining it.'[241]

This continuing situation may lead to the situation when targeted data retention lawfully executed in one state may be illegal in another state, due to difference in understanding what is 'serious crime'. As a serious crime CJEU tends to recognize 'organised crime and terrorism'[242]. The Will R. Mbioh argues that such wording had put a rather high 'threshold of seriousness'[243].

The efforts for unification the grounds for targeted metadata retention were done by EU Commission, which suggested that for understanding the concept of serious crime 'the list of crimes in European Arrest Warrant should be considered'[244]. The European Arrest Warrant (2017 edition) offers a list of 32 crimes: participation in a criminal organisation; terrorism; trafficking in human beings; sexual exploitation of children and child pornography; illicit trafficking in narcotic drugs and psychotropic substances; illicit trafficking in weapons, munitions and explosives; corruption; fraud; laundering of the proceeds of crime; counterfeiting of currency, including the euro; computer- related crime; environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties; facilitation of unauthorised entry and residence; murder, grievous bodily injury; illicit trade in

[241]Evaluation report on the Data Retention Directive (Directive 2006/24/EC), 18.04.2011 COM (2011) 225 Final, p.6

[242] Judgment of 8 April 2014, *Digital Rights Ireland*, Joined cases C-293/12, C-594/12, EU:C:2014:238, paragraph 51; and Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others,* Joined Cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 103.

[243] Mbioh 2017, p. 280.

[244] Evaluation report on the Data Retention Directive (Directive 2006/24/EC), 18.04.2011 COM (2011) 225 Final, p.9.

human organs and tissue; kidnapping, illegal restraint and hostage- taking; racism and xenophobia; organised or armed robbery; illicit trafficking in cultural goods, including antiques and works of art; swindling; racketeering and extortion; counterfeiting and piracy of products; forgery of administrative documents and trafficking therein; illicit trafficking in hormonal substances and other growth promoters; illicit trafficking in nuclear or radioactive materials; trafficking in sto len vehicles; rape; arson; crimes within the jurisdiction of the International Criminal Court; unlawful seizure of aircraft/ships; sabotage; forgery of means of payment;[245] Apparently, the list is wide and might be a ground for debate, but it seems to present at least some offences that refer to the category of serious crime.

3) Specific authority to perform data retention and specific authority to control the use and misuse of data

National law shall clearly prescribe which authorities have access to the retained data, how do they cooperate with each other, who is establishing prior review of application for data retention. Also it is essential to foresee procedures which allow avoiding leaks and abuses of the gained information. Defining in the data retention law one specific authority to perform data retention will narrow down the scope of intrusion into privacy. Moreover, if the data retained is collected and used (or just used) only by one authority than it is more difficult to misuse such data, loose or disseminate. It is better to delegate such powers to a security institution (national security body or even separate department in that body), because they have technical capacities to secure information properly from misuses, as demanded by law. The law shall establish step-by-step procedure of how subjects to data retention can challenge the decisions of such authorized body in front of the courts. The institutions using data-retention and controlling such usage might be separate or single body. However, in case when such functions (use and control) are concentrated in the hands of one authority, the national court will perform the functions of superior controller. This question will be discussed more precisely later in the thesis.

4) Legal guarantees and safeguards

The question of safeguards and legal guarantees more belongs to the sub-question of respect to the essence of privacy, but here we will shortly mention what exactly shall be in the law. First of all the national law shall declare the list of legal guarantees, the effective remedy procedures, prior review authorities, regiment for processing of retained data. The legal norms shall be

[245] See for example the blank of European Arrest Warrant.

constructed in the way that nobody except the concerned person, authorized bodies and courts (ruling the proceedings on data retention issues) shall have access to the retained data. The safeguards shall also narrowly construct the bandwidth of retention, in other words, to categorize the data so the security agencies 'do not undermine the kind of society [they] are seeking to protect.'[246] As established by ECtHR in *Marper*[247] and *M.K. v. France*[248] case law, safeguards have special importance where there is an *increased level of risk* that the data might be illegally accessed or misused.

The general obligation to establish safeguards when limiting privacy was established in European legal framework by case law of ECtHR (*Copland v. the United Kingdom*[249]) and CJEU cases: *Volker und Markus Schecke*[250] and *Schrems*[251]. Specific safeguards in case with right to privacy and metadata retention were introduced by CJEU in *Digital Rights Ireland* [252]and *Tele2&Watson cases*[253]. Safeguards for the processing of metadata (which belongs to the category of 'personal data') are also established by the General Data Protection Regulation framework.

4.3 Respect to the essence of the right to privacy

Respecting the essence of right to privacy, while establishing data-retention laws, is vital because they may have direct and specific effect on private life. Data retention can 'cause person to alter her behavior[254]' and also 'lead to self-censorship[255] and inhibition[256]'. As Peter P. Swire, stated: 'If I know I am under surveillance, I might… restrict my activities, so that nothing embarrassing or otherwise harmful could be detected.'[257] The law shall execute minimal intrusion into one's life.

Respect to the essence of the privacy rights established in Articles 7 and 8 of the CFREU means that: *[s]uch data must be processed fairly for specified purposes and on the basis of the […]*

[246] McIntyre 2008.
[247] *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 102, ECHR 2008-V.
[248] *M. K. v. France*, no. 19522/09, § 35, 2013-IV.
[249] Judgment of the ECtHR, *Copland v. the United Kingdom*, (2007), paragraph 9.
[250] See for instance CJEU joined cases: C-92/09 *Volker and Markus Schecke GbR v. Land Hessen*.
[251] *Maximillian Schrems v Data Protection Commissioner,* C-362/14, EU:C:2015:650.
[252] *Digital Rights Ireland*, Joined cases C-293/12, C-594/12, EU:C:2014:238.
[253] *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others,* Joined Cases C-203/15 and C-698/15, EU:C:2016:970.
[254] Solove 2006, p. 493.
[255] Kang 1998, p. 1260.
[256] Swire 1999, p. 461.
[257] Ibid, p. 473.

legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.[258]*'* Also, as it was mentioned before: *[c]ompliance with these rules shall be subject to control by an independent authority.*[259] Advocate General in *Tele2&Watson* case stated that respecting the essence of privacy might be reached through 'stringent safeguards concerning access to the data, the period of retention and the protection and security of the data'.[260]

In general, CJEU sees the respect to the right to privacy in very strict safeguards which guarantees the appropriate minimal level of intrusion, and minimize the possibilities of loss or abuse of retained data. This became obvious from *Digital Rights Ireland*, *Tele2&Watson* and *Max Schrems* cases: the CJEU emphasized that safeguards for the person whose metadata was retained create a big share of respect to the essence of the fundamental right to privacy. In other words: if a concerned person does not have foreseen by the law effective remedy procedures for the intrusion into the right to privacy, if metadata retention is not a subject to prior review of the judge or other independent body, if the retained data is not a subject to effective data protection measures and the list of people who accessed the data, the means of communication and scope of data processed are not limited to what is strictly necessary, then the respect to the essence of the right to privacy is not kept as required by the EU law.

Metadata not content

The fact that security agencies get access only to metadata and not content plays an important role in recognizing such activities as such that respect the essence of the right to privacy. Based on what was mentioned before in Chapter 3 about importance of metadata, it is rather doubtful, but still access only to metadata is less intrusive than access to a combination of metadata and content. Iain Cameron by referring to paragraph 39 of the Judgment in *Digital Rights Ireland* case claimed that the Data Retention Directive respected the essence of the right to privacy 'as it did not permit the acquisition of content data'[261]. David Fennelly emphasized that the fact that metadata retention activities 'did not involve the retention of content data and was accompanied by certain data security measures'[262] played the role in recognizing the Data Retention Directive

[258] CFREU, Article 8 (2).
[259] Ibid, Article 8 (3).
[260] Opinion of AG Saugmandsgaard delivered on 19th July 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others,* Joined Cases C-203/15 and C-698/15, EU:C:2016:572, paragraphs 189, 228.
[261] Cameron 2017, p.1470.
[262] Fennelly 2019, p. 681.

as respecting the essence to the right to privacy. Indeed, the invalidated Directive was built as such that 'shall not apply to the content of electronic communications'[263].

Authorities with access

Authorities with access is a vital question with is relevant to the respect to the essence of the right to privacy. I believe that the amount of authorities with access to metadata shall be limited by the principle of what is strictly necessary.

How do we define which authorities can have access to retained metadata? As was mentioned before, the only few objectives that justify intrusion into privacy are: 'defence; public security; and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system'[264]. Therefore, only the agencies which are working with these objectives as their main task can have access to such method as data retention. The bodies which are working directly for these tasks in general are: military intelligence, security agencies, national police and customs. A good example of fairly defined agencies with access is Sweden; access authorities include 3 institutions: the National police, Swedish Security Service and Swedish Customs Authority[265].

The reasonable quantity of people who have access shall be dependent on the quantity of population. Indeed, the authorities shall have statistics on how many serious crimes occur on a certain territory, then they shall estimate how many investigators can cope with the certain load of investigating proceedings, and then define how wide shall the staff of the intelligence body with access to metadata retention be. According to Eurostat in 2016, 'there were 318 police officers per 100 000 people in the EU'[266]. It shall be kept in mind that not all of the police officers are dealing with serious crime; therefore, empowering all of them with access to metadata is redundant.

In certain countries there are too many state servants who have access to retained data. The excuse might be as following: the state has only 2 national bodies which have access, but the personnel can be enormous. The states have a sad practice of inflating the personnel. For instance State A and State B are approximately equal in population. State A has 5 bodies which

[263] Data Retention Directive, Article 1.
[264] Privacy and Electronic Communications Directive, Article 15 (1).
[265] Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, Joined Cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 21.
[266] Data of Eurostat, (https://ec.europa.eu/eurostat/en/web/products-eurostat-news/-/DDN-20190104-1, Accessed 10th May 2019).

claim access to the metadata for investigating crimes, their summed up personnel who is eligible to process the information within their territory is 15.000 people. At the same time, State B has 1 body, but its collective personnel accounts for 200.000 people. The difference is extreme and demonstrates that relevant evaluating accountings for amount of people with access to retained data are necessary.

The quantity of bodies that might have access or the list of specialists to have access to metadata shall be clearly defined. For example, in the USA there are lots of governmental security agencies, which might fall within the category of eligible to access the metadata: '[i]t's a veritable alphabet soup of 17 agencies and offices. The group includes agencies strictly focused on intelligence as well as the intelligence arms of other government agencies and of the military. Its total budget in 2015 was $66.8 billion.'[267] Obviously, allowing all 17 agencies the access to metadata is far too much than what is strictly necessary.

In Europe with such diversity in state organization Member States shall themselves define what their structures of administering are, and whom to empower with access to retained data. As an aid for understanding how this question was decided since 2006 we may have a look at the operations in Member States which had transposed the Data Retention Directive. When European Member states were transposing the Data Retention Directive they have defined the national authorities which will have access to the retained data. For instance in Hungary: Police, the National Tax and Customs Office, national security services, public prosecutor, courts; in Poland administration claimed that retained data might be accessed by the: Internal Security Agency, Foreign Intelligence Agency, Central Anti-Corruption Bureau, Military Counter-intelligence Services and Military Intelligence Services; in Finland: police, border guards, customs authorities (for retained subscriber, traffic and location data); emergency Response Centre, Marine Rescue Operation, Marine Rescue Sub-Centre (for identification and location data in emergencies)[268]. The question of the range of authorities was defined already at the stage of transposition of the Data Retention Directive. As it became obvious a little bit later, when the Member States provided statistical data on their data retention practices, the EU Commission wanted to deliver 'limiting the authorities authorised to access the data'[269]. This happened because the Commission saw some of the bodies which were able to access the retained data were not independent enough, while some of the authorities were too wide in personnel.

[267] Agrawal, 2017.
[268] See for Instance Table 2 in Evaluation report on the Data Retention Directive (Directive 2006/24/EC), Brussels. 18.04.2011, p.10-11.
[269] Evaluation report on the Data Retention Directive (Directive 2006/24/EC), 18.04.2011 COM (2011) 225 Final, p.32.

The misuse of metadata happened in the UK, where the authorities used communications data 'to check if parents were truly residing within school catchment areas, or to detect whether people were putting their bins out for collection on the wrong day or allowing their dogs to foul the pavement'[270]. Additionally, in the UK the 'local authorities have used the Regulation of Investigatory Powers Act (Ripa) more than 100 times in the last 12 months to conduct surveillance'[271]. Therefore, extending the personnel which have access to the retained data is proven to bare abuse. It is also disrespectful to the essence of the right to privacy.

Some agencies should only access subscriber and location data, by the example of Finland. When you make a call to the police office (emergency line), the GPS location on your phone automatically switches on. In this situation the security agencies do not have access to traffic data, but know who called and where the person is located in case they have to save the individual.

Access is not only needed for the security agencies. Access to the metadata at question shall also be given to independent post reviewers – usually judges. The Member States shall define if these judges belong to a separate category or it can be any judge.

Defining enough of appropriate bodies to facilitate targeted metadata retention is a difficult task, but it can be done if professionals apply the approach of CJEU to national circumstances. Member State legislators shall design the metadata retention law in a way which delegate access power to only as many agents as reasonably necessary to —cope the task of fighting serious crimes in a certain Member State.

Independent prior review

In *Tele2&Watson* case the CJEU clearly rendered that any metadata retention activity shall 'be subject to a prior review carried out either by a court or by an independent administrative body'[272]. Lydia Morgan claims that before this message was delivered, the UK's DRIPA act did not require prior approval at all[273]. It means that the law in United Kingdom did not impose

[270] Rauhofer 2009, p. 589.
[271] BBC News online, *Spy law 'used in dog fouling war'*, (http://news.bbc.co.uk/2/hi/uk/7369543.stm, accessed 4th Jun 2019).
[272] Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others,* Joined Cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 120.
[273] Morgan 2018.

enough safeguards and did not merely respect the essence of the right to privacy. In my opinion, the issue of prior review has 2 main problems: firstly, how to make this procedural requirement limiting; and, secondly, who shall be the reviewing authority.

With regard to the first issue, the way to make prior review provision limiting is to establish a renewable retention warrant. This approach was offered during Belgian presidency in the European Council. Renewable retention warrants were offered as a procedural limitation tool. Idea was simple: for every communications data retention security agencies have to obtain a warrant, after the warrant expires, security agencies have to prove in front of the court that the case needs metadata retention extension or loose the right to intrude into privacy. However, despite this idea had reasonable grounds and effectiveness proven by a Member State practice, the majority of representatives from Member States refused to support installation of this tool, because of the difficulty and incompatibility of their judicial and investigative systems[274].

With regard to the second issue: authority of the review remains a troublesome question. For example in Belgium the access to use metadata retention was granted by the decision of magistrate or prosecutor, whose independence might be doubtful. One more example of abuse on this ground was seen in Swedish law, where prior review of metadata retention was made 'by the director of the authority concerned or by a person to whom that responsibility is delegated'[275]. Basically, it meant giving authorization to himself / herself. In some Member States the prior reviewers varied from court to prosecutor, magistrate or major[276]. Countries with proper regime of access to retained data were Bulgaria, Denmark and Estonia, where the access was only available after the permit of a judge[277]. In UK the prior review was offered to be made by the personnel united under the term 'Single Points of Contacts', which were 'accredited officials trained to facilitate, review the lawfulness, necessity, proportionality and operational effectiveness of requests by public bodies to access data'[278].

In *Digital Rights Ireland* and *Tele2&Watson* cases, the CJEU left the discretion to decide whether the prior reviewer will be the judicial authority (namely courts) or independent

[274]Council of the European Union, Document 14319/18, (http://data.consilium.europa.eu/doc/document/ST-14319-2018-INIT/en/pdf, Accessed 08 Aug 2019).
[275] Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others,* Joined Cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 23.
[276] Evaluation report on the Data Retention Directive (Directive 2006/24/EC), 18.04.2011 COM (2011) 225 Final, p.10.
[277] See for Instance Table 2. Access to retained telecommunications data, in the Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), Brussels. 18.04.2011, P.10-11.
[278] See for instance, UK's Explanatory Notes to the Investigatory Powers Act 2016, paragraph 235.

administrative authorities to the Member States. It is, though, very disputable question how to identify the independent administrative body. There are no criteria which can help identifying whether a major of the city is independent enough to be eligible to permit/forbid using metadata retention.

Delegating the review function only to courts will cause new challenges and load on judicial system. It shall be kept in mind that the fewer (and more trustworthy) authorities can review the warrant the more limited usage of metadata retention is.

Data protection and security of retained data

Invalidated Data Retention Directive can serve as a good example how to respect the essence of the right to privacy, because in Article 7 it foresaw the requirements for data protection and security of the retained data. More precisely it put obligations on communication service providers to make sure that retained data: is a subject to data protection and security as all other data processed; it is protected from accidental or unlawful destruction, accidental loss or alteration or unauthorized or unlawful storage, processing, access or disclosure; it is subject to access only by specifically authorised personnel only; it is destroyed at the end of the period of retention[279]. Member States in this situation were obliged to ensure that companies provide such measures.

James Rule sensibly claims that '[w]ithout reassurance that their data will be properly treated, people will drag their feet— refusing to yield their data or otherwise resisting the orderly extension of surveillance.'[280] Legislators shall apply 'technical and organisational measures to ensure the effective protection of retained data against risks of misuse and against any unlawful access to that data'[281]. Scholars N.Vainio and S.Miettinen also emphasized that 'successful instrument must limit the number of persons authorized to access and subsequently use the data'[282].

Irreversible destruction of metadata in the end of retention period

[279] Data Retention Directive, Article 7 (a-d).
[280] Rule 2007, p.148.
[281] Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others,* Joined Cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 122.
[282] Vainio – Miettinen 2015, p. 298.

The retained data shall be made anonymous or deleted as soon as there is no need to keep it for investigation procedures. This is known as irreversible destruction. During the period when the data is processed by security agencies, all the activities with data shall be documented, all people with access shall be clearly defined, and all people outside the scope of access shall be kept away from examining the data. The insufficient statutory requirements regarding data security, not defined purposes of data processing, lack of transparency in dealing with data will lead to invalidation of national data retention law, even if the amount of the retained data is proportionate to the declared aim. This situation happened with German Federal Constitutional Court, which was overlooking the law that transposed the Data Retention Directive into German legislation[283].

Notification

Another measure of data protection which has to be dealt with is notification procedure: the agency responsible for metadata retention 'must notify the persons affected […] as soon as that notification is no longer liable to jeopardise the investigations being undertaken'[284]. This notification is the obligation created by the part 2 of the Article 15 of the Privacy and Electronic Communications Directive, also strengthened by the CJEU judgments in cases like: *Rijkeboer*[285], and *Schrems*[286]. Importantly that such notification shall be done even if nothing unforeseen happened to the retained data. For example, in UK the person was only notified, if retention led to negative consequences. CJEU, to the contrary, required that notification is provided always if the data had been retained, and '[t]here is no need to establish that individuals have been adversely affected'[287]. As was outlined in the paragraph 37 of judgment in *Digital Rights Ireland* absence of proper notification risk creating in the heads of people 'the feeling that their private lives are the subject of constant surveillance'[288].

Effective remedies

---

[283] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Mar. 2, 2010, 1 BvR 256/08, § 269.
[284] Privacy and Electronic Communication Directive, Article 15(2); and Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others,* Joined Cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 121.
[285] Judgment of 7th May 2009, *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer*, C-553/07, EU:C:2009:293, paragraph 52.
[286] Judgment of 6th October 2015, *Maximillian Schrems v Data Protection Commissioner,* C-362/14, EU:C:2015:650, paragraph 95.
[287] Mbioh 2017, p. 281.
[288] Judgment of 8 April 2014, *Digital Rights Ireland*, Joined cases C-293/12, C-594/12, EU:C:2014:238,paragraph 37.

Another issue to be regulated is effective remedies in case of loss of information, illegal access or dissemination of data. Restoring the previous existing situation in case of dissemination of vulnerable information is almost impossible task, but fair compensating of the loss and preventing precedents of misuse in future is what the laws regarding retention of metadata have to strive for.

Remedy is all necessary acts to allow the person to restore the violated right to status quo. In current European Union acts, there are several documents that declare the right for effective remedy. First of all, it is Article 47 of the Charter of Fundamental Rights of the European Union. It provides that 'everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article'[289].

In *Tele2& Watson* case, the judges referred[290] to Article 22 of Directive 95/46 'Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question'[291]. Nowadays, that Directive had been repealed by the General Data Protection Regulation and JHA Directive for the protection of personal data for the purposes of investigation crimes[292]; the last document requires that 'every data subject should have the right to lodge a complaint with a single supervisory authority and to an effective judicial remedy'[293]. Such remedy is available in a form of administrative or judicial review of the case.

As it is visible, respect to the essence of the right to privacy is vital for justifying metadata retention. Fabbrini[294] talks about 2 tests which any law regulating data retention shall pass. First of all the 'suitability' test: is the law suitable for the declared aim? This question is connected with respect to the essence of the right to privacy: are there enough safeguards from abuse? Does the law limit itself to metadata retention only? Is the status of data subject properly protected? Only when the law satisfies all these questions with positive answers, then one can move to 'necessity' test. This test is correlated to proportionality and discuss on the limits for application of metadata retention.

[289] Charter of Fundamental Rights of the European Union, Article 47 (1).
[290]Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others,* Joined Cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 12.
[291] Data Protection Directive, Article 22.
[292] JHA Directive.
[293] Ibid, paragraph 85.
[294] Fabbrini 2015, p. 79.

4.4 Proportionality

Proportionality is a key principle when it comes to limiting privacy. As was outlined by Emiliou, proportionality is a '[p]rinciple that requires a proper balance between the injury to the individual and the gain to the community caused by a state measure'[295]. In other words, the less the injury and the bigger the gain – the more justifiable is the intrusion. This scheme works also vice versa: the less the gain and the bigger the injury – the less justifiable the intrusion. So the task of any law that establishes metadata retention for providing security shall bring big benefits (presumably lead to investigation of serious crimes and public security) and do as little damage to individual and common values as possible. This is the question of strict limitations to the intrusion activities.

A great aid for understanding how to reach adequate proportionality can be gained from analysis of the *Marper case*, where ECtHR declared that 'area; nature of the right; nature and seriousness of interference'[296] shall be taken into account. As seen from the mentioned case: unlimited by the time frames retention of personal data creates big damage to the individual right to privacy and, therefore, is disproportional.

Also it has to be taken into consideration that the results of metadata retention shall be important and very valuable for the entire society. To provide such positive results, the law that aims for data retention in Member States shall be able to reach out every existing communication. If the law will be proven weak in its capacities, the courts might lessen its value and rule for the dominance of right to privacy.

One good example comes from *Digital Rights Ireland* case, where CJEU stated that Data Retention Directive approach was proportionate to a degree that it allowed the national security agencies to gain access to the data about crimes, which otherwise, would be unreachable. That was called by the court 'attaining the objective pursued by the directive'[297]. Nevertheless, CJEU remarked the fact, that there are some types of communication that anyway cannot be reached by the security services even in case they are using metadata provided on basis of Directive.[298]

---

[295] Craig 2011.
[296] *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 102, ECHR 2008-V.
[297] Judgment of 8 April 2014, *Digital Rights Ireland*, Joined cases C-293/12, C-594/12, EU:C:2014:238, paragraph 49.
[298] See Portuguese Government – Mr. Tschol and Mr. Seitlinger comments about anonymous communication (in Digital Rights Ireland case).

According to Advocate General in DRI case it was possible 'to escape the application of Directive 2006/24 by using certain methods of communication is undoubtedly such as to limit considerably the actual effectiveness of the system of collection of traffic and location data which it imposes[299]'. Later, however, the AG stated that this fact did not make method offered by Directive 'totally inappropriate for achieving the objective'[300].

The methods which allow suspects to avoid data retention are splendid but doubtfully commonly used. One important source of uncontrolled communication nowadays is game environment. From the leaked by Edward Snowden documents of US National Security Agency, it is obvious that potential criminals '[…]will be making wide use of the many communications features offered by Games and Virtual Environments (GVE)[…]'[301]. According to Phil Owen, the fact that such technologies had been used are doubtful[302], but the most important fact is not whether they were used by terrorists, but whether the game networks have enough capacity to provide all range of communication without proper control of security agencies. The game environments do provide all possible means of communication and according to what was stated in the NSA report 'with a few exceptions, NSA can't even recognize the traffic'[303]. The conclusion is simple: the game environment was not reachable by the Data Retention Directive and barely reachable by national retention laws; even the most powerful security agencies (such as US NSA) can not control that sphere. The games, which might be used as a platform for communication in planning criminal activities, are various, but the major attention is captured by the super popular ones, which involve millions of people all over the world, like World of Warcraft, Counter-Strike[304]. Games with flexible environments, such as Second Life[305] might present even bigger challenges for law enforcement agencies, as they allow new uncontrollable communication.

Other lately discussed methods to avoid legislative reach of data retention laws are VPN networks and prepaid anonymous SIM cards. For example, 'anonymous prepaid SIM cards, especially when purchased in another Member State, could also be used by those involved in

[299] Opinion of AG Villalon delivered on 12 December 2013, *Digital Rights Ireland*, Joined cases C-293/12 and 594/12, EU:C:2013:845, paragraph 137.
[300] Ibid.
[301] See for instance, leaked by E.Snowden Top secret documents of NSA regarding games and virtual worlds, (https://www.documentcloud.org/documents/889134-games, accessed 17th Apr 2019), p. 3.
[302] Owen 2018.
[303] Leaked by E.Snowden, Top secret documents of NSA regarding games and virtual worlds, (https://www.documentcloud.org/documents/889134-games, accessed 17th Apr 2019), p. 3.
[304] See the table on Global Pattern in Game Play in leaked by E.Snowden, Top secret documents of NSA regarding games and virtual worlds.
[305] Famous game described by Yochai Benkler as flexible environment for entertainment, see for instance: Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom*. New Haven: Yale UP. p. 75.

criminal activity as a means of avoiding identification in criminal investigation'[306]. 'Virtual Private Networks (VPNs) in, for example, universities or large corporations, allow several users to access the internet via a single gateway using the same IP address.'[307] Lukas Feiler also concludes that usage of 'Internet anonymising services, pre-paid cell phones, Internet cafés and WiFi hot spots also allow circumventing the retention of traffic and location data in a personally identifiable form'[308]. He argues that because of that the value of retention itself is diminished.

As we can grasp there are ways to avoid retention by either private means of communication or by using technologies which are outside the scope of current regulation. If the channels of such communication beyond the reach of law are wide-spread and commonly used, then the equation between the injury and benefit becomes uneven and law might be recognized as disproportionate and not worthy to intrude with privacy for such vague results. As was claimed by Yochai Benkler in the American discussion on far reaching results of metadata retention programme: '[i]f the NSA cannot show real, measurable evidence of its effectiveness, evidence that doesn't collapse as soon as it is examined and isn't a vague appeal to amorphous, measurement-free "peace of mind", its bulk collection program has to go.[309]'

Violation of principle of proportionality was seen in *Max Schrems case*, in which Advocate General Bot concluded that American intelligence agencies are able to conduct mass and indiscriminate surveillance.[310] The only way to keep within the principle of proportionality is to input strict limitations. How stringent shall the limitations be and to what matters shall limitations apply, we will discuss in the next chapter.

[306] Evaluation report on the Data Retention Directive (Directive 2006/24/EC), 18.04.2011 COM (2011) 225 Final, p.24.
[307] Ibid.
[308] Feiler 2010.
[309] Benkler 2013.
[310] Opinion of AG Bot delivered on 25th September 2015, *Maximillian Schrems v Data Protection Commissioner*, Case C-362/14, EU:C:2015:627, paragraph 36.

5. WHAT IS STRICTLY NECESSARY?

5.1 Categories which shall be limited

Legal provisions of the law striking the appropriate balance between data retention and privacy shall stick to what is strictly necessary. This limitative concept was introduced by the CJEU in the paragraph 39 of *IPI* case, where the court stated: 'protection of the fundamental right to privacy requires that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary'[311]. The CJEU recognized the necessity to use modern investigation technologies, but did not justify the scope of interference provided by the Data Retention Directive.

In *Tele2&Watson* case judgment, the CJEU defined that EU law '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 the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary'[312]. By this the Court had established 4 factors which require strict limitation.

From this clarification we receive a clear message what we shall strictly limit in order to make the national laws proportionate:

1) amount of people concerned;
2) categories of data;
3) means of communication affected;
4) period of metadata retention;

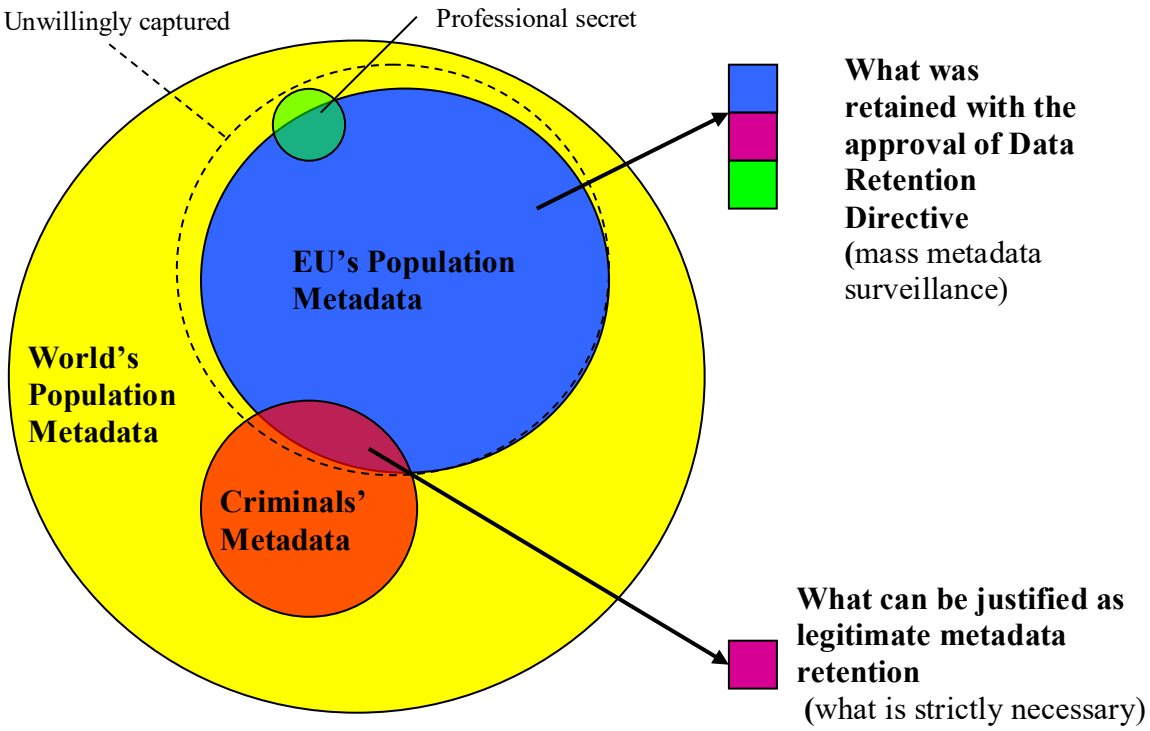
Further in the text we will have a look at each of these categories.

5.2 Amount of people concerned:

The amount of people concerned in metadata retention is one of the key issues to retaining appropriate proportionality. From picture below we can observe how many people were under

[311] Judgment of 7th November 2013, *Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert and Others*, C-473/12 EU:C:2013:715, paragraph 39.
[312] Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others,* Joined Cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 108.

the watch during the validity of European Data Retention Directive (2006-2016).



As it is visible from the diagram, European Data Retention Directive was a bad example of complying with what is strictly necessary with regard to quantity of people concerned. It seems like a concept of 'what is strictly necessary' was replaced by the concept of 'what is possible'. It covers all categories of people all over the EU and not only, as the wording of the document was not limited to the residents of EU. Therefore, it could not guarantee that the communication from residents outside the EU will not be unwillingly captured.

5.2.1 Link to criminal activity

Moreover, the retention had no differentiation between people who might be connected to serious crimes and people, who have no obvious links to any investigated crimes. In *Digital Rights Ireland* case, the Court underlined that the directive retained 'traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.'[313] The document was recognized by CJEU as such which implies also 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 crime'[314]. This issue was a huge problem for the

[313] Judgment of 8 April 2014, *Digital Rights Ireland*, Joined cases C-293/12, C-594/12, EU:C:2014:238, paragraph 57.
[314] Ibid, paragraph 58.

Directive, because it *de facto* constituted mass metadata surveillance. Due to Paul Bernal the risk of such non-discriminatory activity 'is that it treats all people as potentially violent offenders'[315]. In order to narrow the population categories eligible for data retention, the legislators might have used such categories as 'people with previous criminal records' or 'suspected for committing crimes on the territories of other state', etc. As a great aid for defining the people who might be tracked by metadata retention, the legislators might have used the databases of Europol or cooperative frameworks existing between some Member States.

5.2.2 Professional secret

The law foreseeing the appropriate regime of metadata retention shall also consider dealing with aspects of professional secret. This was another problem of the Data Retention Directive. The document applied 'even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy'[316]. Threats to governmental, medical, journalist, judicial and religious secret brings more vagueness to the law. Indeed, capturing by metadata retention some information which constitute, for example, secret of communication between a journalist and the interviewed person, lawyer and a client, a doctor and the patient, priest and parishioner, judge in a closed judicial hearing or parliamentary who have access to state secrets, means double violation: intrusion into privacy and into professional secret. Despite the fact that 'it is not always possible to distinguish clearly which of an individual's activities form part of his professional or business life and which do not'[317], in European framework, professional secret, as well as privacy, is a high-priority value, which cannot be easily neglected.

The solo fact of communication between an individual and doctor, lawyer or priest have importance, because as was well marked by Kurt Opsahl (deputy executive director and general counsel of Electronic Frontier Foundation), security agencies by accessing your metadata 'know you spoke with an HIV testing service, then your doctor, then your health insurance company in the same hour. But they don't know what was discussed'[318]. The fact that the check up does not touch the context of communications does not mean that individuals in charge of metadata check up can not connect certain dots by analyzing the sequence of your actions.

5.2.3 Geography

[315] Bernal 2016, p. 250.
[316] Judgment of 8 April 2014, *Digital Rights Ireland*, Joined cases C-293/12, C-594/12, EU:C:2014:238, paragraph 58.
[317] *Niemietz v. Germany*, no. 13710/88, ECHR 1992 – XII, paragraph 29.
[318] Opsahl 2013.

A feasible solution for limiting amount of people concerned is application of geographic criterion. In my opinion, the question has 2 main dimensions: 1) from where can the data be retained? 2) how narrow shall targeted data retention be?

1) from where can the data be retained?

There is no doubt that it is almost impossible to exercise the rule of law on the territory where the government does not have jurisdiction. For instance, if the data retained in outside the EU, Member State governments will have no jurisdiction to exercise activities with such data. Moreover, if they do, they might violate the jurisdictional sovereignty of other countries. The effective enforcement of the data retention law used for investigation of serious crimes can only be executed on the territory where the Member State has jurisdictional authority. It shall also be the territory where the security agencies can physically come and force the wrongdoers to comply with the obligations. It is a hard task when the world is so digitized and the law is trying to stick to the physical territory. Electronic communication territories are not delimitated. I emphasize that one of the features of Internet medium, which became a major tool of communication, is enormous geographical distribution. Exercising control over the means of communication that do not have the owner or possessor is extremely difficult task. As was stated by Reed Hundt: '[t]he Internet, of course, is not owned or controlled by the United States, or any other nation[319]'. In few simple words: you cannot exercise effective control unless the service provider and users are on your physical territory.

The geographical limitation of metadata retention goes not only to a state outside EU, but often even to another Member State. The European official statistics, received by the EU Commission from the Member States constitutes that 'less than 1% of all requests for retained data concerned data held in another Member State'[320]. This was, again, dictated by the difficulties of cooperation in trans-border data flow.

In *Digital Rights Ireland* and *Tele2&Watson* cases the CJEU clearly stated, that if the Data Retention Directive applies without limits to geographical location, than it have to be claimed as too broad. The Court and AG shortly raised a question about possibility to retain data outside the EU, as completely 'unacceptable'.

[319] Hundt 2012.
[320] Evaluation report on the Data Retention Directive (Directive 2006/24/EC), 18.04.2011 COM (2011) 225 Final, p.22.

2) how narrow shall targeted data retention be?

There is also a question of local usage of retention. How narrow shall the geographical retention be, to be justifiable in the court? Orla Lynskey argue that if 'generalised retention measures be replaced by ad hoc location-based retention measures, the legality of the latter would itself be the subject of much controversy.'[321] Indeed, if ad hoc location based measures applied, security agencies will always have a legal challenge to prove that the geography was reasonable and did not neglect the 'what is strictly necessary' limitation.

Despite the difficulty with establishing concrete criteria for geography of retention, some scholars continue to offer their interpretation of what the CJEU meant by 'targeted data retention'. Gunnar Beck suggests that '[d]ata retention might be lawful if limited on the basis of geography, such as a city centre, where there exists a high risk of preparation for or commission of such offences.'[322] By this action, the security agencies can exclude from retention the data of people, who is physically located outside the marked territory. There are, however, some other problems; imagine connecting the metadata retention to one location at the time, while the criminals move to another location. At this point all extracted metadata connected to the old geographical point is illegally processed. Also the security agencies are not flexible enough in changing the location in case the group of terrorists moves fast to another location.

A bright example of difficulty in defining appropriate geography for metadata retention with regard to geographic limitations was the usage of metadata to threaten the activists during Ukrainian revolution of Dignity in January 2014. People protesting against President Yanukovych's regime in the center of Kyiv had massively received threatening message with the next context: 'dear subscriber, you are registered as a member of public riots'[323]. Location metadata, which 'is ideally suited to automated analysis by computer[324]', had been extracted by the secret agencies from the communication providers and used to send warning/threatening messages. Usage of such a blanket panoptical method, definitely, had a chilling effect on the behavior of some activists. A disturbing point was that these messages were also received by the people who were physically located in the certain geographical area (apartments located near the Square of Independence, hotel rooms in the centre, etc), without slightest connection to alleged

[321] Lynskey (B) 2017.
[322] Beck 2017.
[323] The text is translated from Ukrainian to English by Andrii Konopko, original of the text: 'Шановний абоненте, ви зареєстровані як учасник масових заворушень'(in Ukrainian) (https://glavcom.ua/columns/gluhovskiy/123592-spetssluzhbi-na-shljahu-do-povnogo-kontrolju-za-ukrajintsjami.html, accessed 27th Mar 2019).
[324] Blaze 2017.

activities. The privacy of such people, who happen to be in the same territorial range, will be compromised for the sake of investigation benefits.

5.3 Categories of data

As we already discussed metadata consist of 3 main groups of data: subscriber/registered user; traffic data; and location data. Each of these categories has its own value and they only give clear picture of person's activities if used in complex. Subscriber data connects devices and numbers to real people. Location data identifies the geographical standpoint (or at least the closest antenna point) of the device, and traffic data allows to track the calls and communication data of the person, counter agents of communication.

For the sake of proper and justifiable investigation, the security agencies can ask the court to give permission to check all subscribers located on a certain territory: city centre, separate district, area with high concentration of people (can be metro or bus station, rock festival location, etc.) Afterwards, security agency defines the list of prioritized people by adding a criterion of 'link to criminal activity', excluding others from deep examination. The group of individuals located in the certain territory and with criminal link suffers the following proper check up of their traffic data. By establishing such sequence of actions, the signals agencies eliminate from examination people, who are unlikely to be connected to criminal activities.

The Data Retention Directive failed to make such categorization and foresee that subscriber and location data can be examined first as data of less intrusive nature. In *Digital Rights Ireland* case, the question of the limitation to the categories of data was not fully raised in the rhetoric of the CJEU. As it was mentioned before, the Court had mentioned that the Document which require the retention of data shall be powerful enough to reach any data applicable for the investigation of a serious crime, otherwise, it is not worthy to compromise privacy for such vague results. The same was indicated by the Advocate General in *Digital Rights Ireland* case.

Despite the fact that CJEU failed to deliver all the answers on categories of data in *DRI* case, it made more efforts to highlight that question in the following *Tele2&Watson* case. In the judgment the CJEU analyzed the provisions for categories of data accessed by data retention laws in Sweden and the UK. These examples give us an opportunity to see the attitude and interpretation of the court.

As was figured out by the CJEU, in the UK, with regard to the categories of data retained, authorities had access to such user's data as:

1) *any traffic data for the purposes of any postal service or telecommunication system;*
2) *any information about the use made by any person: of any postal service or telecommunications service; or in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;*
3) *any information that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service'*
4) *user location data*[325];

As we see, the first two are traffic data, second is subscriber data and the last category talks for itself – location.

In Sweden, the law was more precise about the types of data which was retained:

1) *calls and numbers called and the identifiable dates and times of the start and end of the communication*
2) *location data at the start and end of the communication.*
3) *data relating to the IP addresses of the caller and the person called*
4) *data relating to the numbers of senders and recipients, IP addresses or other messaging addresses*
5) *data relating to the IP addresses of users and the traceable dates and times of logging into and out of the internet access service.*[326]

Traffic data here is points 1 and 5, subscriber data is 3 and 4, while 2 is location data.

Both Swedish and British systems allowed the secret agencies to reach the majority of the available communication. These positions in the laws were not criticized in the Court judgment. The issue that shall be raised is the criteria by which some categories of data receive easier access and more use. Like was described above: subscriber and location data can be used on a bigger scale, because it allows providing alibis for people, who are in the area and have no link to criminal activity. Traffic data is already big intrusion into privacy, because it not only accesses the data about individual, but also his contacts and physical movement from location to location (between the telecommunication antennas). Therefore, it can only be allowed with regard to people, about whom there exists a reasonable suspicion of being involved in such activities.

[325] Regulation of Investigatory Powers Act, 2000, Section 22.
[326] Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others,* Joined Cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 18.

In my opinion, this question is not about limiting the categories of retained data which can help in investigation of the serious crimes, but more about building the correct sequence of actions for security agencies. If they follow the procedure of gradual clipping off people unlikely involved, then in the end, when security agencies came up to a very condensed group of individuals, they can exercise thorough examination of all types of their metadata.

The legislators can and should make the retention law strong enough to reach any communication possible despite the fact that some of the technologies can be new (like described previously Game Virtual Environments), belong to closed systems of communication and be out of the scope of regulation. The inapplicability of the data retention laws to certain category of data cannot itself be a ground of dismissal of such document, as soon as it afford the security authorities to reach other categories of the data, which constitute the majority.

My opinion might be also strengthened by the EU Council group of experts who are working on the development of new guidance for metadata retention. In November 2018 'experts considered that only very few additional data categories could be excluded from the list as not being necessary for the investigation and prosecution of crime'[327]. This is due to the fact that the standard list of categories of metadata useful for investigation activities was made by European Telecommunications Standards Institute. The organization had already filtered and excluded categories which have no value for law enforcement.

Additionally, in the Working document of the Data Matrix exercise, the participants agreed that categories of data which can clearly be excluded from data retention for the sake of investigation of serious crimes are: 'length of the antenna, value indicating the quality of communication and value indicating the number of ringtones'[328]. These issues constitute the part of metadata (traffic and location data), but barely have any value to the investigation of crimes. As it is understandable, unambiguous agreement about exclusions of the research groups did not touch any contextual information.

5.4 Means of communication

In defining the means of communication is it useful to have a look at *Tele2&Watson* case, where the court analyzed Swedish law. In Sweden the data retention law (lagen (2003:389) om

[327] The European Council Document 14319/18, (http://data.consilium.europa.eu/doc/document/ST-14319-2018-INIT/en/pdf, Accessed 07 Aug 2019).
[328] Presentation of Jan Ellerman, slide 17, WK 5900/2018 INIT (Outcome 2.Workshop).

elektronisk kommunikation & förordningen (2003:396) om elektronisk kommunikation) was obliging a huge amount of subjects to retain users' data. The categories were: a) telephony services; b) telephony services which used mobile connection; c) telephony services which used IP packets, d) electronic messaging systems; e) internet access services[329]. If we decipher these terms in understandable examples, we can clearly see that Swedish security agencies (provided by law) had access to all means of communication, created by the use of a) traditional wire phones; b) mobile phones; c) smart phones; d) online messengers without connection to device (WhatsUp, Viber, Facebook messenger, VK messenger); e) any communications service available online (again with no difference in the device which user use for connection: smart phone, tablet, e-book, laptop, stationary computer or other device).

In the UK's the DRIPA and RIPA acts did not specify which means of communication can be under retention. This gave the authorities a real discretion to justify interference into any system and reach any devices. From governmental point of view, such strategy obtaining access to all devices without exclusion is admissible, because it makes the law powerful enough to provide meeting its objectives. But categorization of relevant period of metadata retention for each mean of communication is essential. This is due to the fact that people use smart phones more like Internet devices, than like calling devices. As 'Internet is used for almost every aspect of our lives'[330] it has absorbed the unique value of telephony provided on regular wire phones or even mobile phones. People (and especially youth) would rather choose Internet connection to call in various smart phone applications (messengers, Skype, voice IP apps) than pay the telephony operator to make a regular call. In that case the value of Internet metadata is bigger: it combines not only calls, but also locations, apps usage, entertainment patterns, scheduling, life habits. Defining connection to serious crime of a separate subscriber through complex Internet metadata is less time-consuming. Therefore, it might be reasonable to define Internet-based data as more 'full' and require shorter period of retention. We will have a look at the periods of metadata retention in the next part of the work.

5.5 Time period of metadata retention

This question paraphrased sounds as: for how long shall the law provide data retention? The question cannot be answered in a simple way and shall consider the means of communication when seeking the answer.

[329] Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others,* Joined Cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 18.
[330] Bernal 2016, p. 247.

The annulled Directive established the period of retention for 6 months, whereas the longest period might last for 24 months in specific situations. The situation when the period may vary should have been highlighted strictly. This period of retention shall be strict rather than liberal, to avoid risks of abuse.

After the annulment the court remained silent about the change of periods. The CJEU in analysis of Swedish and UK's Retention laws did not suggest shorter periods than those defined by invalid Directive. In Sweden all the data was retained for a minimum of 'six months from the date of the end of communication'[331]. While in the UK, normal period of retention is established as 'must not exceed 12 months'[332]. In 2018, there were several Member States representatives who claimed that 'at least 12 months would be absolutely necessary for the purpose of effective law enforcement'[333]. However, settlement of the end boundary at 12 months was seen as excess of requirement by the Data Retention Directive. In *Tele2 & Watson* case, the Court claimed that UK's 12 months period was not consistent with what is required by CJEU.

Therefore, we assume that the basic requirements to period of retention remained the same: 6 months and no longer than 24 months (in specified cases of extreme importance). The term of retention for 6 months is reasonable, if the mean of communication at question – regular telephony data. This standpoint is based on the evidence from Member States, illustrated in the evaluation report of Data Retention Directive: '[…]around ninety percent of the data accessed by competent authorities that year were six months old or less and around seventy percent three months old or less when the (initial) request for access was made'[334].

The CJEU sensibly retained the scheme which allows longer retention of data, because '[a]ccording to most Member States, the use of retained data older than three and even six months is less frequent but can be crucial'[335]. This goes to investigation of serious crimes, which are planned for years, like terrorist attacks and other organized illegal activity. In investigating grave criminal offences security agencies need longer time as they 'tend to rely on older retained data reflecting the length of time taken to plan these offences, to identify patterns of criminal behaviour and relations between accomplices to a crime and to establish criminal intent.'[336]

---

[331] Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others,* Joined Cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 19.
[332] Ibid. paragraph 29 (5).
[333] The European Council Document 14319/18, (http://data.consilium.europa.eu/doc/document/ST-14319-2018-INIT/en/pdf, Accessed 07 Aug 2019), p. 6.
[334] Evaluation report on the Data Retention Directive (Directive 2006/24/EC), 18.04.2011 COM (2011) 225 Final, p.22.
[335] Ibid.
[336] Ibid.

There also has been a research on the topic of appropriate time limit for retention, which was held in 2004 by the EU Data Protection Commissioner and it clearly points out: 'analysis carried out by telecommunications companies in Europe reveal that the biggest [sic] amount of data demanded by law enforcement were not older than six months. This shows that longer periods of retention are clearly disproportionate'[337].

There are some arguments which stand for even shorter period of metadata retention. For example, in 2005 the UK commissioned a study to define the 'most popular' period of metadata retention without connection to means of communication; the results had shown that the majority of data generated for the law enforcement agencies were less than 3 month old[338]. Judith Rauhofer claims that '[m]andatory retention in excess of that three-month period therefore seem neither appropriate nor proportionate to the stated objective.'[339]

Some scholars emphasize that Internet-based metadata worth more than telephony services metadata. For instance, Brendan Molloy, president of the privacy-focused Australian political party, the Pirate Party, said that 'storing 24 months' worth of metadata from Internet-based communications is not comparable to storing the time and phone number of a phone call' and was a 'grotesque attack' on privacy.[340] In other words, there is an uprising need to establish different periods for each type of communication. This aspect also has reflection in the retention practices of Member States, for example out of 28 Member States, only 5 of them created differentiation of periods on the basis of categories of data. For example, Ireland and Italy retained traditional telecommunications data for 2 years and Internet-based data for 1 year; Slovakia required 1 year retention for general telephony and 6 months for Internet-related data; Slovenia's difference was 14 months and 8 months respectively; and, lastly, Member State (Malta), specifies one year for fixed, mobile and internet telephony data, and six months for Internet access and Internet email[341]. It is also necessary to take into account that by establishing such different periods of retention for different means of communication the Member States

[337] Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism. [Proposal presented by France, Ireland, Sweden and Great Britain (Document of the Council 8958/04 of 28 April 2004)], adopted 9th November 2004, p.4, (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp99_en.pdf, Accessed: 4th Apr 2019).
[338] See for instance: Liberty and Security – Striking the Right balance, paper by the UK Presidency of the European Union, (http://www.statewatch.org/news/2005/sep/ukpres-paper.pdf, accessed 4th Jun 2019).
[339] Rauhofer 2009, p. 599.
[340] Reilly 2014.
[341] See the statistics table in Evaluation report on the Data Retention Directive (Directive 2006/24/EC), 18.04.2011 COM (2011) 225 Final, p.15

might include 1 or 2 months period beyond strict necessity to create ‘safety pillow’. Therefore, in my opinion, the period of retention of Internet-based metadata shall be shortened to 3 months, while traditional telecommunications data might be retained for the previously established period of 6 months. Such limitations have little chances to influence radically the effectiveness of law enforcement agencies, but will be proportionate and necessary.

6. CONCLUSION

The development of technologies had brought society a chance to eliminate the majority of crimes. At the same time to reach this wanted target members of society have to face compromise between public security and privacy. Privacy is a valuable condition of being left alone. It is almost impossible to give a full and exhaustive definition for privacy because it is not limited to the inner circle of the individual, and it is based on the cultural acceptance of certain issues. Scholars agree to define privacy as a separate issue in every individual case by means of analyzing the negative thing which conflicts with privacy.

Privacy is legally protected in Europe in a range of documents: European Convention of Human Rights (Article 8), Charter of Fundamental Rights of the European Union (Article 7 and 8). The interpretation of privacy is visible in the decisions of European Court of Human Rights and Court of Justice of the European Union. Privacy and data protection are closely related rights which intertwine but do not constitute the same thing. Privacy is a condition in which the individual is able to define how much he or she is open to entire society, while data protection is the condition which defines how the information about the individual is processed, when such data is already possessed by the other subject of informational relations (mainly state or organizations, not another individual). Privacy claims are mainly made in front of a court regarding the balance with other social values, while data protection claims are brought in front of the administrative institution (data protection supervisor, national data protection board, European Data Protection Board), which decides whether the entity using the data of individual violated the law or not. Data protection measures constitute a basis necessary to establish respect to the essence of the right to privacy. Failure to establish proper data protection measures leads to disrespect and deep violations of privacy.

Metadata (also called communications data) contains 3 categories: traffic data, location data and data about subscriber (user). Metadata is always described as opposite to content. Also it is considered to be a strict historical protocol of actions of individual's everyday life: location, timing and contacts of communications. From analyzing big amounts of metadata one can draw precise conclusions on individual's habits and behavior patterns. In the legal sense metadata constitutes personal data, which enjoys the protection under the GDPR and JHA Directive.

Retention of metadata is a typical activity performed by the communication service providers to comply with the state legislation. Communication service providers were obliged to store the

communications data of individual and also share it with the security agencies in case they require doing so for the sake of investigating or prevention of crimes. Retention of metadata in legal sense constitutes 'data processing'. In technical sense it is copying, storing and disclosure to state security agencies of individual's traffic, location and subscriber data. In blanket variant such data is stored without 'preliminary request' from intelligence agencies.

The history of metadata retention in the European Union had suffered a long and complicated development: from uncontrolled usage of all possible metadata retention tools by the Member States with decisive discretion in the hands of Member States (before DRD), to usage of partially limited metadata retention on the basis of unified EU law: Data Retention Directive; and, finally, to usage of limited (targeted) metadata retention after the decisions of the CJEU in *Digital Rights Ireland* and *Tele2&Watson* cases. Despite the validity of CJEU decisions shaping metadata usage in the Member States, not all of the EU Member States understood the shift and reshaped their internal laws.

The intrusion into the right to privacy cannot be done unless the legislators foresee the measures to the use of metadata retention as declared by Article 52(1) of the CFREU. To intervene with privacy right of the individual metadata retention activities shall meet the criteria of general interest. Security is the only possible objective which allows justifying intrusion into privacy. Choosing as an aim protection of a single market is not enough. Metadata retention can only be used to fight serious crimes: the list of such criminal wrongs can be found in the European Arrest Warrant.

The law shall be clear and enforceable on matters of definitions, providing enough safeguards and guarantees from abuse: aimed only at metadata, shall limit the amount of security agencies allowed to access the retained metadata, it shall create data protection regime including security, notification procedures, prior review by the court or other independent authority. There shall be created procedures for effective remedy in case of abuse. If the law foresees all of this then it satisfies the suitability test and faces the next tests: necessity. Principle of proportionality has key importance when deciding on the limitation to the right to privacy.

Metadata retention activities shall be discriminate with regard to amount of people, categories of data, means of communication affected and time period. With regard to amount of people, it is only allowed to conduct it for a defined group of people, so called 'targeted metadata retention'. This group should exclude people whose data is protected by professional secret. Tools to limit

the amount of people influenced are: link to criminal activity and geography. Link to criminal activity can be defined by taking into consideration previous criminal records of the individual or illegal activity on the territory of the other state. Geography can be limited by certain geographical area (city centre, part of district, compact location) that is considered to be a place for serious crime.

Subscriber and location data shall be used in order to define a wider circle of people, while forthcoming examination of traffic data should touch only people, who reasonably may have connection to serious crime. Time period of metadata retention aimed at a certain group of people is dependent also on the means of communication. Internet based metadata should see no longer than 3 months period of retention, because it has more value and shows wider picture of individuals life. Telephony metadata can be withdrawn for the maximum period of 6 months. Building national metadata retention is possible with the requirements which were imposed by the European Union Law. However, if the Member State wants to use targeted metadata retention, it shall make sure that it goes through 6 steps marked in the Diagram below.