RIGA GRADUATE SCHOOL OF LAW

The challange of personal data protection in the era of digital economy

MASTER'S THESIS

Author: Ilze Kaļķe
LL.M 2017/2018 year student
student number M016061

SUPERVISOR: Anna Vladimirova-Kryukova

LL.M

DECLARATION OF HONOUR:

I declare that this thesis is my own work, and that all references to, or quotations from, the work of others are fully and correctly cited.

(Signed) …….

RIGA, 2018

Table of Contents

INTRODUCTION

European Union (EU) is at the centre of the world's digital revolution. As the largest economy of the world and home to some of the world's wealthiest, technology and research advanced nations of the planet, EU is already facing the wide opportunities and challenges of the further digitalization of its economy and society. EU's readiness to effectively address, remedy and balance emerging large scale Information and Communication technologies (ICT) with the growing privacy concerns is a focal point for its future development as the world's power of the digital economy.

Digital economy of the EU is currently growing at seven times the rate of the rest of the economy as the labour market for ICT skilled workers is expected to rise to 16 million by 2020, while 90 % of jobs now require basic ICT skills.[1] The new technological paradigms like Internet of Things (IoT), Big Data ecosystems and Cloud computing services are fuelling and transforming the business world as businesses strive to boost productivity levels, cut costs and expand their markets with the help of technological know-how.

In the digital economy environment personal data is being compared to commodities as valuable as oil and gold. It is also perceived as a currency[2] of the digital economy. The significant reduction of costs for storing vast amounts of information has made it possible to capture, save, and analyse ever large amounts of data. Company's record details of each customer transaction, websites log customer behaviour as various data mining techniques aggregate information from variety of sources to compose individual preference profiles. The more organizations and individuals embrace digital technologies, the cheaper and faster become the production and processing of personal, and potentially sensitive, data. One of the immediate consequences of the rapid digitalization are the growing privacy concerns.[3]

The Digital Market Strategy (DSM) of the EU has set a goal of establishing strong digital economy and society. If the goals of the Strategy are reached it would result in vast positive impact on standards of living, employment rates, and new business opportunities, improved public sector services and overall economic growth. However, in order to be in a position to take full advantage of digitalization opportunities policy makers are required to proactively and effectively address upcoming challenges of further digitalization and innovation[4] especially in regards to emerging technical and legal uncertainties in the field of personal data protection.

As one of the steps in 2012 European Commission(EC) presented new legislative proposal to revive an obsolete, pan-European data protection rules and to better address the new scale

1 European Commission, "The EU explained: Digital agenda for Europe" Luxembourgh: Publication Office of the European Union, 2014, p:3

2 Reading, V., "Speech of Vice president of European Commission" Innovation Conference Digital, Life, Design, Munich: 22 January 2012 available at: https://ec.europa.eu/commission/commissioners/2014-2019/katainen/announcements/vice-president-katainens-speech-sustainability-and-innovation-conference-brussels-12-october-2017_en last accessed: 20 May 2018

3Acquisty A., College, C. "The Economics of Personal Data and the Economics of Privacy" OECD Conference Background paper, Centre 1 December 2010, p:3

4 Wauters P., Van Der Peijl S. et al. "Measuring the economic impact of cloud computing in Europe" Deloitte for European Comission, 2014 DOI:10,2759/75071 p:5

privacy concerns of the increasingly data driven Europe. As a result General Data Protection Regulation (GDPR) was adopted in 2016 with aim to effectively remedy the unprecedented scale of data collection and the transformation that technology has brought to the economy and social life[5]. The GDPR has been presented as:

> "a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market." [6]

The actual impact and effectiveness of the GDPR that comes into effect on May 25, 2018 will only be evident in the course of next years. Today, however it is crucial to understand how will the GDPR change the EU data protection playfield and if the new regulation is capable to address growing personal data and privacy challenges emerging from further digitalisation in the long term.

RESEARCH QUESTION AND STRUCTURE

The research question of this paper is: How capable and effective is the newly adopted EU data protection legislation to address the growing future privacy and data protection concerns associated with expansion of the Digital Economy?

The papers consist of three chapters and a conclusion. In the course of the research each chapter focuses on particular set of sub-questions that aim to provide for an understanding of crucial elements of the research question. Namely: Why is privacy important and what role does it play in social, legal and economic spheres? How is privacy linked to data protection? How did the data protection framework emerged and developed in Europe? What is the value of personal data and why is it important? How important is innovation for the EU? What are the new technologies that are key to the digital economy? How is the digitalisation threatening the future of privacy? How effective is the newly adopted EU legislation and have it taken into account all the aspects of rapidly changing digital world?

This paper is based on legal studies as well as descriptive and analytical research techniques. The literature used for the purpose of this paper was selected with priority given to the most recent publications, legislation and official documents.

First chapter sets the scope as it presents the key concepts and definitions as well as provides for brief overview of the development of the data protection legislation in the EU. Particular attention is given to the different concepts of privacy – its significance for social, legal and economic spheres. Second section presents how growing national level privacy concerns of the late 1960s developed into the data protection laws as we know them today. The legislation overview is concentrated on the motivation and triggers behind each of steps of the legislation as well as the time and processes of the adoption, since those are crucial indicators for assessing the ability of the EU law to address the challenges of digital era. Third heading presents the notion of protection of personal data; by exploring how is the personal data protection ensured in practice and what it implies under the EU law. First chapter concludes

5 Rec. 6 GDPR
6 Rec. 7 GDPR

with presenting the growing role and value of data in the EUs digital economy as well as the impact of the technological progress on people's welfare and on our society as a whole.

Second chapter starts with presenting vision and aims of the EU Digital Single Market Strategy(DSMS) and the added value of developing IoT, Cloud computing and Big Data infrastructures as part of the EU digital economy goals. It then proceeds to literature review and assessment of the new privacy and data protection challenges and threats that are increasing as a result of development of the three technological paradigms and the overall further digitalisation. Chapter concludes with singling out the high risk personal data protection concerns namely: data breaches, data mining and profiling and loss of control, it then further analyses the impact scale of these threats.

Third chapter presents two level analysis of the GDPR. First section provides comparative analysis of GDPR against the repealed Data Protection Directive with an aim to identify the newly introduced provisions and obligations and asses the new rules of the data protection playfield for both economic entities and data subjects. Second level of analysis is carried out by weighting the framework of the GDPR against the selected personal data protection threat areas identified in Chapter II. Third and last section of the chapter concludes by assessing the overall impact of the GDPR and elaborates on additional measures to be implemented and further promoted to improve the approach to privacy and data protection in order to maximize the potential of the Digital economy in the EU.

1. CHAPTER I - SCOPE AND CORE CONCEPTS

1.1 Conceptualizing Privacy

> "Privacy is the basic human need, and losing privacy is perceived as an extremely threating experience. Privacy embraces solitude; personal space, or intimacy with family and friends, it is a ubiquitous and trans-cultural phenomena. Privacy leverages well-being, without privacy we are at risk of becoming physical or mentally ill.'' [7]

Privacy is a multidisciplinary term that interprets depending on the subject area, point in time and variety of other factors. The definition is stretched out across legal, technological, socio-political and economical spheres and is highly dependent on context or individual's life experiences[8]. What's more, the concept is continuously further scoped in courts, political arena and literature, as it develops together with rapid technological progress of today and rapid changes in society and lifestyle. While the main focus of today's debate is the information privacy, privacy can also be viewed in forms of territorial and physical constrains and linked to concepts of surveillance, exposure, intrusion, insecurity, appropriation, as well as secrecy, protection, anonymity, dignity or freedom.[9] Privacy is of extreme importance, as

7 Trepte, S., Reinecke, L., "Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web" Springer Science & Business Media, 2011, p:5

8 Pomykalski J., "Discovering Privacy—or the Lack Thereof" Information Systems Education Journals, January 2017 p:4 availble at: https://files.eric.ed.gov/fulltext/EJ1135734.pdf: Last accessed: 16 May 2018

9 Acquisti, A. et al, "Privacy and Human Behavior In the Age of Information" American Association for the Advancement of Science, 2015 509-514

it is is rooted in the human nature and is viewed as form of dignity and autonomy.[10] Privacy is part of human anthropologically and psychologically and is manifested "in the sense of shame, need for personal space and bodily integrity"[11]. Even though privacy is at the centre of the debate of our century, it is not, as many would expect, the product of modern era. The need, recognition and core principles of privacy as well as the related concerns have been present over centuries of humankind. The notion of privacy originated already in ancient societies as a result of the emergence of first cities. Early urbanization opened doors to self-determination as an individual could now distinguish the *'self'* from the *'others'* (like village, church or state). The individual was then able to escape the ''constant moral control" of the small communities, while giving up "*physical privacy"* for crowded urban life.[12] Scholars have uncovered evidence of privacy-seeking behaviours across cultures separated by time and space: from ancient Rome and Greece as well as of in the texts ancient religions like The Quran and the Bible.[13]

The first legal views on privacy as a right to be preserved can be tracked back to 1890 Warren and Brandeis publication: *The Right to Privacy*[14]. Authors presented privacy as valuable social interest that must be legally protected and provide for famous legal definition of the privacy as 'Right to be left alone.'[15] Their law review article outlines the essence of the continuous development of privacy concept. And today the *Right to be left alone* definition remains active and widely recognized by "most lawyers and scholars whose work touches on the protection of privacy"[16] Despite being published almost 130 years ago it pinpoints the Privacy concept problems that are still relevant in the 21st century : clear need for a better definition and recognition of the privacy concept in order to better protect it, and the ways innovation and emergence of new "*business methods"* result in new privacy risks and generate need for modernization of legal instruments to ensure sufficient levels of protection.[17]

Today, in democratic societies privacy is considered a basic human right that goes in hand with independence, freedom of movement and speech, self-respect and integrity.[18] However, among all of the existing competing attempts define the privacy at its core there is still no comprehensive, all accepted definition[19]. As stated by Solove "the need to conceptualize privacy is significant, but the discourse about conceptualizing privacy remains deeply

10 Schoeman, F., " Privacy: Philosophical Dimensions" American Philosophical Quarterly Vol 21. No 3, 1984 p :200

11 Debatin B. "Ethics, orivacy and Self-Restraint in Social Networking" article in S.Trepte and L. Reinecke, "Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web" Springer Science & Business Media, 2011, p:47

12 Solove D.J., "Nothing to Hide: the False Tradeoff between Privacy and Security" New Haven & London: Yale University Press, 2011. p. 4.

13 Supra note 9.

14 S.Warren and L.Brandeis "The Right to privacy", Harwards Law Review, 1890 p:194-201

15 Ibid.

16 Ibid.

17 Ibid.

18 European parliament technology assesment, "ICT and Privacy in Europe", Final report October 16 2006, p:72 available at: https://teknologiradet.no/wp-content/uploads/sites/19/2013/08/Rapport-ICT-and-Privacy-in-Europe.pdf last accessed: 14 May 2018

19 Moore, A. D. "Privacy: Its Meaning and Value." American Philosophical Quarterly, vol. 40, no. 3, 2003, pp. 215–227. JSTOR, www.jstor.org/stable/20010117 last accessed 20 May 2018

dissatisfying.''[20] And as Moore have emphasized, "one of the direct consequence of the concept problem is that law sometimes proved ineffective and blind to the larger privacy protection purposes it must serve".[21] Therefore, the leading legal scholar's base they core works on conceptualizing the privacy with an aim to guide policy makers and legal interpretation to better address the privacy threats[22]. Available literature on the conceptualizing privacy is extensive, and while lack of universal definition persists, on a global level most authors agree that crucial aspect of the concept is one's ability to control information about oneself. Such approach is supported, among many, by Gryz: *"*an exclusive right to private information about oneself"*[23]* and Bélanger: *"*the desire of individuals to control or have some influence over data about themselves"*[24]* While, Parent proposes his conditions for privacy as: "not having undocumented personal information about oneself known by others".*[25]* Control over ones information[26] is also a focus of the concepts offered by Westin and Moore.

Other scholars avoid providing for concise definitions for term of such complexity and suggest approach of multiple levels, value sets and principles. Clarke, who was the first privacy scholar to elaborate on the types of privacy in a logical, structured, coherent way,[27] identified four dimensions of privacy: privacy of a person, personal behaviour privacy, personal communication privacy, and personal data.[28] Solove on the other hand, had criticized all of earlier attempts to conceptualize privacy term and suggests that privacy definition might *not have a single common characteristic*[29] and instead presents the six core principle for privacy: the right to be let alone, limited access to the self, secrecy, ability to exercise control over information about oneself, the protection of one's personality, individuality, and dignity; intimacy-control over one's intimate relationships or aspects of life.[30] In similar way Finn *et al.* distinguishes seven types of privacy: Privacy of the person, privacy of behaviour and action, privacy of communication, privacy of data and image, privacy of thought and feelings, privacy of location and space and privacy of association.[31] The debate remains active as the current social changes outdate the previous definition and introduce new privacy norms and conditions.

---

20 Solove, J.S., "Understanding Privacy", Harvard University Press, May 2008 GGWU Law School Public Law Research Paper No. 420 availble at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1127888 last accessed: 20 May 2018

21 Supra note 19

22 Sololve J.,S., "Conceptualizing Privacy", California Law Review, Volume 90, Isssu 4. P: 1091

23 Gryz, J., "Privacy as informational commodity." Proc IACAP, philpapers. org (2013). p:2

24 Bélanger, F.,R. "Privacy in the digital age: a review of information privacy research in information systems." MIS quarterly 35, no. 4 (2011): 1017-1042. p:1020

25 Parent, W., A., "Privacy, morality, and the law." In Privacy, pp. 105-124. Routledge, 2017. P:106

26 Moore, A. D., "Privacy: its meaning and value." American Philosophical Quarterly 40, no. 3 (2003): 215-227 p:2 Available at: http://www.jstor.org/stable/20010117 last accessed: 20 May 2018

27 Clarke, R., What's privacy? In *Australian law reform commission workshop* (Vol. 28) July 2016 p:3 available at: http://www.cse.unsw.edu.au/~cs4920/resources/Roger-Clarke-Privacy.pdf last accessed: 20 May 2018

28 Ibid.

29 Supra note 22. p:1091-1092

30 Ibid.

31 Finn, Rachel L., Wright, and Michael Friedewald. "Seven types of privacy." In *European data protection: coming of age*, pp. 3-32. Springer, Dordrecht, 2013.

Privacy concepts is as crucial for legal scholars as it is for the economists, as it helps to predict and identify the consumer behaviours and as stated in the introduction of this paper: can also stagnate certain positive development of the economy if not addressed effectively. Economists therefore approach the privacy concept from the lenses of the marketplace and its impact on behaviours of economic actors and on economy as a whole. The below economic theories applied to the privacy problem demonstrate how standpoint dependent is the concept. Economists have been debating the privacy issues since, at least, the 1970s. Posner studied effect of privacy on the marker relationships and decision making process. And found that unequal distribution of private information among economic actors lead to uninformed decisions and subsequent costs and losses. Stigler studied inefficiencies of potential governmental interference in the market of personal information, since the data subjects are motivated to disclose only positive information that could lead to misleading information flows to the marketplace. In 2006, Calzorali and Pavan research found that personal data sharing between two economic entities could increase the overall levels of social welfare, including that of the customers. While Noam's arguments that are based on Coase theorem, presented that protection of individuals data does not depend on law ensuring such protection but rather on how much the consumer values their data. Taylor have studied the risk of over investment of the economic entities into personal data collection and describes the coloration between the levels of digital competence of the consumer and need for regulation of personal data protection. He then concludes that the regulatory intervention would not be necessary if the consumer is highly competent on the use of his data.[32]

As it can be seen privacy lays its roots in the human nature and will remain a basic need of individuals regardless the changed of the society, modernization or increased use of digital tools. Privacy has direct effect on marketplace relationships and behaviours, consumer decision making and welfare thus lawmakers have to approach the privacy preservation with caution and by taking into account the rights of individual as well as potential impact on the development of society and economy. Therefore the privacy and data protection issues must be addressed simultaneously for both legal and economic reasons. Another important aspects is that privacy is dynamic and fluid context dependent term. Therefore, when exploring the privacy related problems and concepts it is crucial to review it from multiple standpoints as well as take into account various influence areas. First, the need and expectation of the individuals need to be identified. Second, legal aspects and risks for preserving such rights have to be weighed against other impact areas that these rights my influence (i.e. economic or social warfare). With these points in mind, this paper further presents the role of privacy and, more specifically – personal data in the context of its role and value in the context of EUs digital economy of today.

1.2 From privacy concerns to data protection laws: European road to the GDPR

It is not in the aims of this paper to go in detailed provisions of the historical data protection legislation in the EU, however in order to understand the law-making processes as well as the

[32] Supra note 3. p:3-4 (Theroies of Posner, Stigler, Calzorali and Pavan, Noam, Taylor summarised)

overall EU stance and origins of the data protection law this section provides a brief overview of the historical legislation background of the EU. An emphasis is put on the scope of each legislation, triggers and motivation behind its adoption as well as on the timeline and procedure for the adoption and implementation of each piece of legislation or instruments.

In Europe the need for addressing the growing privacy concerns emerged after the World War II with the expansion of new ways of communication like press, radio and photography topped with rising concerns over the exercise of government surveillance throughout the Cold War Era[33] as well as developing computer dependence of economy. As a result clear call from the public emerged for defining rules that require governments and businesses to be transparent about how they use their private information.[34]

First to address the growing concerns of their citizens was Swedish government as they passed the first ever data protection law – Sweden's Data Act – in 1973. The Act made it illegal for any person or company to use information systems of any kind to handle personal data without a license[35]. What's more it required those who wish to export the data outside Sweden to obtain a license that were similar to an export license and allowed various interest group such as labour unions and political parties to present arguments against and prevent such exports. On top of that if the established Data Inspection Board would suspect that the business relocation outside Sweden occurred due to entities aiming to avoid Data Act provisions, such relocation would be denied.[36] Other national governments soon followed the Swedish practice: The French (Tricot) Commission adopted the Law on Informatics and Freedom in 1978, while Netherlands lead to proposal on Act on Personal Data Registration.[37] By 1980s Austria, Germany, Luxembourg and Norway have introduced different national level data protection safeguards, while Belgium, Iceland, Denmark, Spain and Switzerland had drafts in the pipeline.[38]

International and pan-European trade and development organization understood that further emergence of different national rules could constrain or even paralyses the global trade that was coming to depend on the use of computers. Clear need emerged for some degree of regularization of the rules at higher levels.[39] Therefore, the growing data protection concerns were simultaneously addressed by two bodies: Organization for Economic Cooperation and Development (OECD) and the Council of Europe. Both organizations were established in the aftermath of the World War II, OECDs mission was promoting of international trade and global economic growth, while the Council of Europe was formed to aftermath to promote the rule of law, democracy, human rights and social development in Europe.

33 Levin, A., "Has the Era of Privacy Come to an End?" 2016 Canadian Journal of Law and Technology 15 (1) pp.17-24, p: 17-19

34 Tzanou, M., "The Fundamental Right to Data Protection Normative Value in the Context of Counter-Terrorism Surveillance" Bloomsbury Publishing, 2017. p: 19

35 Sweden Data Protection Act (No. 289 of 1973), unofficial English translation available at: www.skolverket.se

36 Madsen W, "Handbook of Personal Data Protection", Palgrave Macmillan,1992 p:63-64

37 OECD, "30 Years After: the Impact of the OECD Privacy Guidelines" Conference held at the OECD Conference center Paris, France, 10 March 2010. availble at:
http://www.oecd.org/sti/ieconomy/30yearsaftertheimpactoftheoecdprivacyguidelines.htm accesed 20 May 2018

38 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Prefrace, 1980 availble at: www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.html last acccesed 20 May, 2018

39 Kuschewsky, M., "Data Protection & Privacy", European Lawyer, 2016 p:1-7

As a result of the legislative work over period of 4 years, in 1980s the OECD produced "The Protection of Privacy and Trans border Flows of Personal Data guidelines" (Guidelines*)* adopted in in 1981; in the course of the same year Council of Europe passed for signature the Convention for the Protection if Individuals with regard to automatic processing of personal data (Convention 108).

1.2.1 Convention 108 and OECD Guidelines

The motivation for OECD to work on data protection standards were originated mainly from the growing fears that national level legislations would restrict the movement of the personal data and create unproportioned trade barriers. Therefore, the Guidelines aimed at fostering economic stability and encouraging trade by addressing key concerns of the time: need of the citizens for protection of automated and conventional personal data, while preventing that the disproportional and differing national rules on data privacy would lead to high economic losses and constrain on cross border trade.[40] The Preamble of the OECD Guidelines emphasizes the need:

> "to prevent interruptions in international flows of data and invites states to adopt measures for unlawful storage of personal data, the storage of inaccurate personal data'', or the abuse or unauthorized disclosure of such data, while at the same time "not restrict the flow of personal data across border not to cause serious disruption in important sectors of the economy, such as banking and insurance.''[41]

The Guidelines recognizes the delicacy of their tasks that include balancing opposing interests (those of the public and the economy) and aim to safeguard the invasion of privacy of an individual while allowing a full exploitation of the potentialities of data processing technologies in so far as it is desirable.[42] In sum, from the perspective of public interest for privacy protection OECD advices the following: data should be obtained by lawful and fair means and relevant to the purpose it is intended to be used and such purpose needs to be specified not later than during the submission of the data; the data should be accurate, completed and up to date and it is not to be disclosed to the third parties irrelevant to the initial purpose of the collection, furthermore it is advised that data subjects shall be informed about the identity and contact data of the data controller and basic rights for the data subjects are envisaged: to obtain information on the data that has been collected, and to have their data erased, rectified, completed or amended, having fulfilled certain obligations.[43]

The Council of Europe Convention share multiple basic concepts and overall principles with the OECD Guidelines: the definition of personal data is identical, similar data security and data quality principles apply, Article 8 of the convention data subjects are envisaged to have access to same set of rights as in OECD: to obtain information on set of personal data from companies, receive the information regarding the data processed, erase or rectify the data in some cases and to challenge the actions of the processor. As for the interests of economic activities Paragraph 18 of the Guidelines Member States (MSs):

[40] Supra note. 37
[41] Ibid.
[42] Ibid.
[43] Ibid.

> "should avoid developing laws, policies, and practices in the name of protection of privacy and individual liberties, which would create obstacles to trans-border flows of personal data that would exceed requirements for such protection. " [44]

In similar the provisions of Article 12(2) of the Convention 108 states that a party to the Convention shall not:

> "for the sole purpose of the protection of privacy, prohibit or subject to special authorization transborder flows of personal data going to the territory of another Party" [45]

While both instruments recommend to be applied in both private and public sectors, the provisions of the Convention are applied solely on automated data processing. The instruments also leave room for the Member States to derogate from the provisions in a way more appropriate to the national rules. Convention 108 was revised in 2011 following a public consultation and it remains the only binding international instrument of the data protection field.

1.2.2 Directive 95/46/EC – Data Protection Directive

As a result of the adoption of the Convention 108 data protection laws became more widespread in Europe, and while they all followed the similar pattern there was still a considerable divergence within the norms of convention. European Commission (EC) was once again facing concerns over that the lack of harmonization would create trade barriers. [46] Similar as with the adoption of Convention 108 motivation behind the proposal for new legal instruments was further harmonization of the national rules. By then multiple member states have had their national level rules adopted and EC now called for further actions for giving more substance to the principles of the right to privacy already contained in Convention 108, and to expand them[47]. In 1990, failing the call for ratification of Convention 108 Commission issued number of proposals for draft measures: Directive on the protection of the individual with regard to processing of data and free movement of data, directive concerning the protection of personal data and privacy in the telecommunication sector as well as proposals for police sectors and Commission data protection policy. Process until the final adoption of all four measures took 18 years in total[48]. The principal EU legal instrument on data protection is Directive 95/46/EC of the European Parliament and 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 (DPD)[49] was adopted in 1995, after having been redrafted in total of three drafts in 1992 and 1993.

Article 1 of the DPD presents the scope and objective of the Directive inviting the Member States(MSs) to protect the fundamental rights and freedoms of natural persons, in particular

[44] Supra Note. 38 Artilce 18
[45] Convention 108 Article 12(2)
[46] Jay, R., "Data protection law and practice" 4th edition, Thomson Reuters, 2012, p:8-9
[47] European Union Agency for Fundamental Rights, "Handbook on data protection", 2014, p:17
[48] R.Jay "Data protection law and practice" 4th edition, Thomson Reuters, 2012, p:8-9
[49] Directive 95/46/EC

that of the processing of personal data. MSs are also invited to not restrict the free flow of such data between MSs as part of the rights of the protection. [50]

In EU law the legal basis for any secondary measure legislation must be found within the Treaty (primary law). In legal terms, the existence of the DPD rests on Internal Market grounds: Article 100a (now Article 95) of the Treaty. However, the proclamation of the Charter and in particular Article 8 thereof which incorporates the right to data protection, has given added emphasis to the fundamental rights dimension of the Directive.[51] The Commission memorandum of Understanding explanatory paper states:

> "The diversity of national approaches and the lack of a system of protection at Community level are an obstacle to completion of the internal market. If the fundamental rights of data subjects, in particular their right to privacy, are not safeguarded at Community level, the cross-border flow of data might be impeded"[52]

1.2.3 E-privacy Directives

First Directive on E-privacy (97/66/EC) was another instrument that originated from of 1990 Commission proposal. The Directive applied to the processing of personal data in connection with the provision of publicly available telecommunications services in public telecommunications networks. The first e-privacy directive provided for specific requirements for telecommunication service providers on processing of personal data and cross-border development of new telecom technology. The directive constrained terms for processing of traffic and billing data, connected line identification, call forwarding and guidance on other sector-specific technical features. It was repealed in 2002 with Directive 2002/58/EC that incorporated new technological trends like emails and digital mobile networks as well as elaborated on the inconsistencies of interpretation. The Directive 2002/58/EC was then again amended and repealed in 2009 with Directive/2009/136 that once again incorporated new technology trends namely, the response to data breaches, use of 'cookies', requirements for prior consent for marketing service promotions. The E-privacy directive currently in force is expecting a similar fate as DPD as it has a proposal for a regulation currently underway. Involving a lot of debate regarding its role in complementing the GDPR, it is expected to come into force in the end of 2019, after being heavily scrutinized by European Parliament and the Council.

The nature of the E-privacy directive is crucial, as it demonstrates that additional, sector-specific measures can be adopted in parallel to the primary data protection legislation in case it is necessary.

1.2.4 Article 8 of the Charter of the Fundamental Rights of the Lisbon treaty

[50] Directive 95/46/EC Article 1
[51] Report from the European Commission "First Report on the implementation of the Data Protection Directive (95/46/EC)" /COM/2003/0265 final
[52] Ibid.

As EU institutional direction gradually shifted from the sole economic cooperation principles to a more political Union. In 2000 EU proclaimed the Charter of Fundamental Rights of the European Union (The Charter). The Charter proclaimed common EU values, ever closer Union, human dignity and peaceful future[53]. Moreover it recognized:

> "the need to strengthen the protection of fundamental rights in the light of changes in society, social progress and scientific and technological developments by making those rights more visible in a Charter. "[54]

Charter combined the constitutional traditions with the international obligations applicable to the Member States,[55] by covering wide range of rights such as, liberty, economic, social and political rights. These liberties are presented under six main categories: dignity, freedoms, equality, solidarity, citizens' rights and justice. Articles 8 of the EU Charter of Fundamental Rights recognize protection of personal data as separate fundamental rights. Article 8 reads:

> "1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
> 3. Compliance with these rules shall be subject to control by an independent authority."[56]

The adoption of The Charter did not provide for the legal status of the established rights. First, it was intended to incorporate the Charter within draft proposed Constitution that was planned to replace the treaty of Amsterdam. As the ideas for the Constitution was later abandoned, the charter remained legally ambiguous[57] for 9 years, until it was incorporated in the Treaty of Lisbon. With the adoption of the Treaty of Lisbon Charter became legally binding on the institutions and bodies of the European Union, and on the Member States when implementing EU law.

Another key provision that was incorporated in the Lisbon treaty in 2007 was the abandonment of the pillar structure due to which previously legislation of data protection was divided between first (private and commercial purposes) and third pillars (law enforcement purposes). The Lisbon treaty provisions under Article 16 of Treaty of Functioning of the European Union (TFEU) now provided for clearer, more effective data protection system. Article 16 of the TFEU provides that Parliament and the Council lay down rules relating to the:

> "protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law"[58]

[53] EU Charter of Fundamental Rights
[54] Ibid.
[55] Supra note. 47 p:20
[56] EU Charter of Fundamental Rights Article 8
[57] R.Jay "Data protection law and practice" 4th edition, Thomson Reuters, 2012, p:33
[58] TFEU Article 16

Article 16 TFEU provides for more freedom for the EU beyond the traditional limits of the Union law, signalled the emancipation of the right to data protection from right to privacy [59] and for the first time separates data protection primary law grounds from the internal market purposes.

1.2.5 GDPR

The proposal draft of the GDPR constituted the main legislative response to the provision of Article 16 TFEU[60]. In 2012, after review process that lasted over two years European Commission present a reform package, containing a legislative proposal for a Regulation that would repeal the DPD. The explanatory memorandum, of the proposal explains the need for the reform in the data protection. Commission motivates the need for change in current data protection legislation as a response to rapid technological developments, dramatic increase of data sharing, unprecedented scale of use of personal data and the need to build trustworthy online environment for consumers in order to reach the aims set by the Digital Agenda of Europe, Europe 2020 Strategy and better respond to globalization.[61] More than 4000 proposed amendments to the draft regulation were proposed in the European Parliament, after which the EP Lead committee on Civil Liberties, Justice and Home Affairs (The LIBE Committee) adopted 300 compromise amendments[62] after which it was finally passed to Council for evaluation and further negotiations.

Ironically, the proposal that aimed to better address the rapid developments of the digital economy world came into force 4 years later with the effect date in 6 years. The Regulation maintained the general data protection principles but introduced additional obligation and extended the scope. The key new rules and obligations contained in the GDPR are: Geographical scope, extended definition of personal data, stricter consent policies, data breach fines, as well as some new rights given to the data subjects. The comparative analysis of the GDPR against the provision of the DPD is detailed in Chapter 3.

It is evident that in the the 60 years of the developments and further harmonization's of the EU Data protection legislation two core aims dominated: Ensuring free flow of personal data across broader, thus strengthening the internal market as well as safeguarding the rights of the individuals to privacy and data protection. The initial need for data protection was addressed at national levels by the governments to the direct growing needs of their citizens (electorate) with a direct focus on protection of the data subject within the borders of the state. As a response international organizations like OECD and Council of Europe shifted the direction to shared common goals: ensuring fair levels protection while at the same time placing the main focus on the economic growth goals and trade. Each next step for legislator data protection reform further harmonized the national laws up until the directly applicable GDPR. While it may seem that the aims of each legislation failed the common goal of ensuring harmonization

[59] De Hert, P., "The Right to Protection of Personal Data. Incapable of Autonomous Standing in the Basic EU Constituting Documents?" Utrecht Journal of International and European Law .31 (80), 2015 pp .1–4 . DOI: http://doi.org/10.5334/ujiel.cz
[60] Ibid.
[61] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data
[62] Supra note. 39. p:257

of the rules, therefore another measures had to be undertaken. The developments of the data protection law must however be viewed together with the complex nature and development and growth of the EU as a supra national organization. Therefore gradual member state integration from Convention to finally adopting a directly applicable Regulation can be viewed as a success, given differing stances and laws of the member states as well as of the EU institutions.
In practice, adoption of new legal instruments in the EU takes time, series of readings and negotiations due differing position and roles of the EU bodies and the MSs as well as the bureaucratic legal procedures. The existing structure of the ordinary legislative procedure might become a future issue for addressing rapid development of digital economy and innovation in the future. Another point to be highlighted for the further context of this paper is the nature of e-Privacy directive that particularizes and complemented the DPD as *lex specialis*, in similar way the new (currently draft) e-Privacy Regulation will apply to the GDPR. Since GDPR might need further sector specific adjustments in the future, similar approach as in the ePrivacy is a viable option. As we can see the data protection in the EU originated from privacy concerns as these two notions are closely interlinked. Having overlooked the different concepts of privacy term it is necessary to review what exactly the current EU Laws offer under the notion of protection of the personal data. While absolute protection of personal data would not be viable, the current changes in the world might require the shift from the term of protection to accountability and transparent. These points are further discussed in the next chapter.

1.3 Notion of protection of personal data

This section focuses on exploring the degree of rights and protections ensured under the notion of protection of personal data. The notion of data protection originates from the right to privacy and both are instrumental in preserving and promoting fundamental values and rights. While need for privacy lays roots in the human nature and has been present over centuries of humankind, the need for protection of personal data is a creation of modern era. As already explained, such need originated when individuals (data subject) were threatened with the loss of control over the use of their personal information by third parties. The use and collection of private data by third entities created increasing gap of knowledge and power between various players[63]. The new order shifted the need of simple privacy preservation to need for recognition of information privacy as a right[64].

Data protection law in the EU in its core is about encouraging data processing, not forbidding it. It enables the data protection processes by imposing system of checks and balances and providing rules. What's more processing of personal data is not interfering with Article 8 of the Charter – in fact it is the basic condition for its application.

In order to gain an understanding on how EU law on personal data protection *protects* in practice, it is crucial to point out that Personal Data Protection as provided by the EU law is

[63] Hijmans, H. "The European Union as a constitutional guardian of internet privacy and data protection." 2016,Digital Academic Repository; 2016 p:55
[64] Ibid.

not an absolute right and is fairly limited under certain conditions according to the EU Charter of Fundamental Rights[65]. As provided in Article 52(1) of the Charter:

> "any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others. ''[66]

Ensuring personal data protection as absolute right would not be a reasonable option in the context of modern digital society and legal order, as it does not exist in legal vacuum,[67] and it has to be balanced against multiple other rights, freedoms and public interests like freedom of expression, freedom to conduct business, national security and economic prosperity interests.[68]

The Article 4(1) of the GDPR defines personal data as:

> ''any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.'' [69]

Article 4(2) then provides definition of 'processing' as all-inclusive term:

> "any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available alignment or combination, restriction, erasure or destruction." [70]

Thus, data protection in practice applies to of any information relating to an identified or identifiable living person, including names, dates of birth, photographs, video footage, email addresses and telephone numbers. Following the technological advances the definition of what is considered personal data has further extended, as example Case 582/14 – Patrick Breyer v Germany[71] judgment that held that IP addresses are personal data in certain circumstances[72].

As provided in Article 1 - *'Subject matter and objectives'* of the GDRP the definitions of *'personal data'* and *'processing'* are all inclusive and non-exhaustive, as well as their scope might be further extended. The extent of the level of *protection* and rights of data subjects as provided in the GDPR are limited. In practice the GDPR gives limited range of rights to the

[65] EDPS "Data Protection" https://edps.europa.eu/data-protection/data-protection_en last accessed: 15 May 2018
[66] EU Charter of Fundamental Rights
[67] Cellarius, M., "The right to informational self-determination: Keep it simple!" available at: https://www.europeanfiles.eu/digital/right-informational-self-determination-keep-simple Last accessed: 20 May 2018
[68] Supra note.65
[69] GDPR Article 4(1)
[70] GDPR Article 4(2)
[71] Case 582/14 – Patrick Breyer v Germany
[72] Ibid.

data subjects: such as information and access to the personal data, right to rectify, erase (right to be forgotten) and restrict processing. It also enforces certain levels accountability and transparency and requires fair processing (collection, use, storage) from the data processors and controllers both public and private sectors. "The ultimate objective of data protection is limited to ensuring fair processing of personal data, and: fairness in outcome of such processing."[73]

EU objectives on the personal data protection are based on two contrasting policy: protection of natural persons with regards to the processing of personal data on one hand; and "rules relating to the free movement of personal data"[74] on the other. The balances of these two objectives are at the centre of scholarly and legal debate, as they represent the two main approaches to protection notion of personal data: Economics and Fundamental Right approach. Early critics of first 1970s data protection measures in Europe argued that behind the claim of data protection, the European countries are instead creating barriers in order to ensure their market protection from US suppliers of computer services.[75] Economic approach views the data protection regulation from the perspective of solely economic motivation and benefits. It argues that while preserving privacy is a common interests of the countries, the actual grounds of any data protection law lays in the fear *that uncoordinated domestic legislation may hinder trans-border data flows that can contribute to economic development*[76] and that data protection at its core was born out of internal marker concerns as it continues to foster international economic aims.[77] The example of this perception and motivation can be found in previously described OECD privacy Guidelines[78] as well as the Directive/95/46/EC and they do not completely cease in the aims and provisions of the GDPR.

Fundamentalists on the other hand, focus on the move from initial economic interests of the EU to recognition of personal data protection as a fundament right. And hold an argument that with the adoption of Lisbon Treaty the focus of the EU have shifted to the direction of personal data protection in the interests of individual. And that the legal recognition of the Charter, and subsequently – right to data protection as a fundamental right is new and fresh approach to the data protection in the EU.[79]

1.4 Privacy and Data in the Digital Economy: Changing Role and growing value

While Privacy could still be viewed as "Right to be left alone", in the digital age of today there might just not be such opportunity. New technologies worldwide have affected different

[73] Bygrave, L., "Data protection Law: approaching its rationale logic and limits" in M. Tzanou "The fundamental Rights to Data protection", Oxford and Portland, Oregon, 2017 p:9

[74] GDPR Article 1(1)

[75] Bing, J., "The Council of Europe Convention of the OECD Guidelines on Data Protection", MICH. J. INT'L L. 271 (1984). Available at: https://repository.law.umich.edu/mjil/vol5/iss1/13 Last accesed: 20 May 2018

[76] Stewart, B., The Economics of Data Privacy: Should we place a dollar value on personal autonomy and dignity? The 26th International Conference on Privacy and Personal Data Protection, Poland, Worclaw. Vol. 14. 2004.

[77] M. Tzanou "The fundamental Rights to Data protection", Oxford and Portland, Oregon, 2017 p:16-17

[78] Ibid. p:14

79 Ibid. p:18

aspects of dealing with private information in the areas of commerce, governments as well as in the everyday private life. As world around is growing increasingly digital, technologies have become a part of everyday life: gadgets become smarter, more user friendly and accessible to ever large proportion of the society.

Innovation and technology is the new fuel to the traditional economy and its rapid and continuous development is generating the need for higher level of awareness as well as concurrent reorganization of regulation and legislation. Rapid innovation of the past decades has forever changed the ways businesses all over the world operate, compete and create value. Easy access to volumes of information and web environments that allow to review, rate and compare the services have forever changed the modes of consumption. Constant innovation, targeted, personalized service and e-logistics now are compulsory for business to remain competitive in today's world of e-commerce.[80] Technologies are transforming marketplace actors as well as the forms of goods and services in the market. Today economy deviates from market consisting of physical goods and standard services to web-based online services, such as: content streaming, gaming, social media, and online data storage or search engines. As pointed out by Vittet-Philippe Expert Advisor of DG Enterprise: Europe is in the middle of an e-business revolution driven by the ICT sector, however it is not just about the technology or cutting costs. It is about structural, in depth changes in the economy and changes within relationships of the traditional intermediaries.[81]

According to Eurostat, in 2017 - 97 % percent of businesses in the EU used internet access in their daily operations; 80 % of them had their own website and 43% used social media websites such as Facebook or Twitter for promotion of their activities. One fourth of the businesses trade goods and services online[82] while 70% receive orders over websites or apps.[83]

Collection and use of data sets in today's business world has acquired enormous economic significance. Successful economic activity is often based on the client databases and the technological know-how on effective use of this data. Multi-billion web companies like Google or Facebook are built on economics of personal data. Personal data is not just viewed as a mean for operation, but as valuable asset of production, just like hard assets and labour.

Estimates calculate that the data volumes are doubling every 18 to 24 months.[84] European Commissions data measurement study future suggests that by 2020, revenues of data companies could grow as high as 20.6 % with overall growth of data market projected to 15.7%. What's more, the EU data economy is expected to contribute up to 4% on the EU

80 Zekos, Georgios, Risk Management and Corporate Governance in 21st Century Digital Economy. (New York: Nova Science Publishers, 2014) p: 274-275

81 Vittet-Philippe, P., "EU policy for the e-economy Europe in the e-economy: challenges for EU enterprises and policies" Computer Law & Security Report Vol. 18 no. 1 2002 p 24-26

82 EUROSTAT: Digital economy and society statistics enterprises: Statistics explained available at: http://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_enterprises 23 July 2017 Accesed on : 21 May 2018

83 EUROSTAT, "E-Commerce statistics" Available at: http://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce_statistics Last accesed: 21 May 2018

84 Kemp, R. "Legal Aspects of the Internet of Things", Kemp IT Law, London, June 2017 p:1

DGP if the high growth scenario, characterized by strong role of digital innovation with high levels of ICT investment is implemented as planned.[85]

As a result of rapid digitalization and growing unprecedented amounts of data shared, stored and proceeds an active debate persist regarding the impact of the further digital processes on people's welfare and the ability of individuals to navigate and control their information and how or if it could be resolved at the policy level.[86] The direct consequence of rapid digitalization is the loss of control over the full extent of individual's personal data collection, as most people lack knowledge and digital competence to assess what is happening to their private information. Individuals can easily lose track of their personal data collected by smart devices, applications and contracting parties, while commercial services providers are targeting their audience and use aggregated data collection that further misleads the end users. Media further contributes to the confusion and alert by reporting over hacking of pacemakers and defibrillators[87] and Samsung Smart TV privacy policies that warn against disclosing sensitive information in front of TV, as it might be transmitted to the third parties[88].

The economic consequences of growing scale of information sharing for all parties involved can be welfare enhancing or diminishing as individuals and organizations face complex, sometimes intangibles, and often ambiguous trade-offs consisting of benefits and losses.[89] The erosion of privacy and misuses of data can threaten ones autonomy, not just at the consumer level but as a citizens.[90] Study by computer science researchers at Karlstad University found that despite high concerns over handling personal data to third parties, generally people have low awareness about the data portability and no clear understanding of their rights as well as processed behind data sharing. [91] There are multiple risks that emerge from lack of the awareness from the side of data subjects, such as: Loss of control over your personal data, as it is complex to erase or track once processed; uncontrolled transmission of sensible personal data, like sexual preferences, political views or sensitive medical records or even identity theft. Other risks factors are directly linked to misuses of personal data by economic entities. These risk could be expressed in data being sold to third parties, as some businesses base their core operation on accumulation, processing and selling of personal data; or risk of

85 IDC and Open Evidence, Study prepared for the EC "European Data Market SMART 2013/0063", February 1, 2017 p: 11-17

86 Acquisti A., Brandimarte L., Leowenstein, G., "Privacy and human behaviour in the age of information" Science Mag, Vol 347:Issue: 6221 p:509

87 Radick R for Forbes, "A Heart-To-Heart From The Hackers: Cyber-Vulnerabilities In Cardiac Devices" availble at: https://www.forbes.com/sites/insider/2017/04/26/a-heart-to-heart-from-the-hackers-cyber-vulnerabilities-in-cardiac-devices/#4e7eaab827b0 Last accessed: 20 May, 2018

88 Samsun Privacy Policy, Smart TV Supplement. Availble at: http://www.samsung.com/hk_en/info/privacy/smarttv/

89 Supra note 38.

90 Cohen, J.E "Examined lives: Informational privacy and the subject as object." Stanford Law Rev. 52, 1373–1438 (2000)

91 Karegar, F., Pulls, t., Fischer-Hübner S. "Visualizing Exports of Personal Data by Exercising the Right of Data Portability in the Data Track - Are People Ready for This? IFIP Advances in Information and Communication Technology, 2017 DOI: 10.1007/978-3-319-55783-0_12

discrimination in the form of profiling and scoring of individuals based on the data that data collectors possess.[92]

EC has already acknowledged the extent of concerns over further digitalisation among EU citizens. Eurobarometer study carried out by EC as part of its mid-term DSM review summarizing the EU citizen opinion on the digitization and automation on daily life. The study finds that overall there is a positive outlook on the impact of digitalization on the economy and quality of life and the society. However study also finds that widespread concerns persist in areas like robotics, artificial intelligence, new technology, sensitive data as well as privacy and security areas. Concerns are mostly linked to data breaches, loss of control and impact of the automatization on the future employment. [93]

Digitalization has brought many benefits to consumers and businesses, but it has also generated new problems and policy issues that legislators are struggling to tackle and address.[94] There is therefore a call for further actions from the side of policy makers, cooperation and business in order to be prepared to better address the future technology with an aim to maximize the benefits and minimize the risks for all participating parties.

2. CHAPTER II - ASSESSING EMERGING PRIVACY THREATS IOF THE DIGITAL ECONOMY ERA

> "The main emerging markets in the short-medium term will be characterized by a combination of IoT with Cloud Computing and Big Data creating "smart environments" where hyper-connectivity and data intelligence generate multiple new services (also with other technologies such as robotics)."[95]

This Chapter presents the three technology paradigms: Internet of things, Cloud Computing and Big Data Ecosystem. These emerging and booming technologies, while an important instruments for the EU digital economy and society, are at the same time rising crucial concerns over privacy and data protection matters. The aim of this chapter is to present both: the prospects that the IoT, Cloud and Big Data hold for the society and economy as well as the vulnerabilities and concern areas associated with further expansion of these sectors.

First section of this Chapter reviews what role is dedicated to IoT, Cloud and Big data technologies within the EU Agenda and what goals are set by the EC for the development of these technologies. It then presents the core system architectures and summarizes the benefits that further development of these sectors could contribute to society and economy. Second section reviews the body of literature that elaborates the emerging privacy and personal data

92 Wolfie C.,Winter, R.,Schweinzer B. " Collecting, Collating and Selling Personal Data: Background Information and Research" Vienna, Austria May 6 2013 p:3-5

93 European Comission, "Special Eurobarometer 460:Summary" March 2017 Availble at: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2160 Last accessed: May 20, 2018

94 European Comission, EU Science Hub "Digital Economy" availble at: https://ec.europa.eu/jrc/en/research-topic/digital-economy Last accessed: 18 May 2018

95 European Commission DG Communications Networks, Content & Technology "Definition of a Research and Innovation Policy Levaraging Cloud Computing and IoT Combination" p:9

integrity threats and singles out and groups the high priority risks for further analysis. The high risks areas analysed are: Data Breaches, Data mining and profiling and Loss of control.

2.1 Vision of the EU Digital Single Market Strategy

> "Digital technologies are going into every aspect of life. All they require is access to high speed internet. We need to be connected, our economy needs it, people need it."[96]
> **Jean-Claude Juncker**

IoT, Cloud and Big Data technologies and their markets are expanding right at this moment. Therefore, the question for the EU policy makers is not whether to further develop them, but how to ensure the right path in order to maximize the benefits and recognize, asses and minimise the risks.

Article 3(3) Treaty of Functioning of the EU grants mandate to the EU to work towards stable and competitive internal market economy, price stability, with high rates of employment, social progress and scientific and technological advance.[97] Europe 2020 Strategy[98]further scopes these aims and sets goals for developing an economy based on knowledge and innovation and coming out of the crisis with smart, sustainable and inclusive economy. As one of the seven flagship initiatives for the achievement of these goals is the Digital Agenda for Europe (DAE).[99] DEA goals are to create a strong and connected digital single market, promote and develop e-commerce, digitalize public services and work on the digital inclusion – closing the digital skill gap among the EU citizens[100].

With the goals of DAE in mind, Digital Single Market Strategy (DSM) was launched under Commissioner Juncker in 2014. DSM aims to open up digital opportunities for people and business and enhance Europe's position as a world leader in the digital economy with an ultimate goal to merge 27 national markets to a strong and united digital marketplace. The DSM consists of 16 key initiatives that are arranged under three pillars: Better access for consumers and businesses to digital goods and services across Europe; creating the right conditions and a level playing field for digital networks; as well as creation of innovative services to flourish and maximize the growth potential of the digital economy.[101] The wide range of initiatives developed under the DSM includes tackling cybercrime, establishing European data Cloud and work towards more effective geo-blocking rules.

Midterm review of DSM carried out in 2017 overviews the performance of the EC on keeping up with its goals on the digital developments and calls for further actions in regards to

96 Jean-Claude Juncker, State of the Union Address, European Parliament,14 September 2016
97 Treaty on European Union Article 3(3)
98 European Commission "Europe 2020 Strategy" Availble at: https://ec.europa.eu/info/business-economy-euro/economic-and-fiscal-policy-coordination/eu-economic-governance-monitoring-prevention-correction/european-semester/framework/europe-2020-strategy_en
99 European Comission, " Europe 2020 Strategy : A strategy for smart, sustainable and inclusive growth" Document 52010DC202 p:8
100 European Comission, "European Union explained: Digital agenda for Europe" Luxembourg: Publications Office of the European Union, 2014 Availbale at: http://eige.europa.eu/resources/digital_agenda_en.pdf
101 European Comission, "A Digital Single Market for Europe: Commission sets out 16 initiatives to make it happen" May 2015 Availbe at: http://europa.eu/rapid/press-release_IP-15-4919_en.htm Last accessed: 15 May 2018

addressing emerging digital challenges.[102] Action plan is focusing on increasing trust in the emerging ICT technologies and preventing misuse, as well undertaking proactive actions against the cybersecurity threats.

Three separate initiatives are currently dedicated to IoT, Cloud and Big Data development in the EU. Digitalizing European Industry initiative (DEIi) for the development of IoT[103]; European Cloud Initiative (ECI) for the Cloud service development and Building European Data Economy (BEDA) initiative for Big Data and European Cloud ecosystems[104]. DEIi is based on three pillars thriving IoT ecosystem, human-centered IoT approach and single market for IoT[105]. Goals set under the second pillar are crucial for understanding the current EC stance on the IoT future. EC acknowledges that IoT must provide for an environment that empowers citizens, not make them hostages of the technologies. Therefore the technologies and their application must be made trusted, accepted, wanted, accessible and usable. For this EC relays on the GDPR provisions to increase trust in the digital services and provide for rules fit for the digital age.[106] The two focuses of ECI are European Open Science cloud - environment processing and storing scientific data and EU Data infrastructure cloud: a world-class digital infrastructure to securely access, move, and share and process data in Europe. [107] While BEDA aims at maximizing the benefits of the use of the cloud computing for economy and society. The core of the initiative is to unlock the re-use potential of different types of data and ensure its free flow across borders.[108]

In terms of monetary gains EU is keyed up both for the investment and economic gain prospects. EC estimates predict that fully functional digital single market could contribute €415 bn per year to the EU economy, creating hundreds of thousands of new jobs.[109] Moreover, if favourable policy and legislative conditions are in place and further investments in ICT are encouraged, the value of the European data economy may increase to €739 billion by 2020 (threefold the increase of year 2015), representing 4% of the overall EU GDP.[110]

The future of digital economy heavily depends on the ability of industries to deploy the digital innovation across sectors.[111] As one important step, rising privacy concerns over the impact of the further ICT technologies must be effectively and proactively addressed in order to gain consumers trust and subsequent market demand for the services. If these goals are not reached the promised technology use areas might remain sector limited (i.e. manufacturing,

102 European Comission, Comission Staff working Document "Mid-Term Review on the implementation of the Digital Single Market Strategy A Connected Digital Single Market for All" May 2017 {COM(2017) 228 final} p:1-6
103 Ibid.
104 European Comission, "Policy: Cloud Computing" Available at: https://ec.europa.eu/digital-single-market/en/cloud Last accessed: 15 May 2018
105 Supra note. 102
106 Supra note. 102
107 Deloitte for European Comission, "Study on emerging issues of data ownership, interoperability,(re-)usability and access to data, and liability" doi 10.2759/781960 2017 p:363
108 European Comission, " Building European Data Economy" Availble at: https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy Last accessed: 20 May 2018
109 European Comission, "Digital Single Market" Available at: https://ec.europa.eu/commission/priorities/digital-single-market_en Last accessed: 20 May 2018
110 Supra note 108
111 Supra note. 102

transportation, health care)[112] and stagnate both the economy and innovation. The objective of the EC is to adapt the policy and legal framework according to the needs of growing data economy.[113] EC recognizes that healthy expansion is not given and will require series of technical and legislative actions to prevent national market level fragmentation[114], "removing remaining barriers to the movement of data and addressing legal uncertainties created by new data technologies, including the issues of data generated by the machines"[115]. It is evident that EC heavily relays on the ability of the GDPR to provide for strong data protection rules in order to strengthen the citizen trust[116] that will allow the digital economy to develop across the internal market.

The next two sub-sections are briefly presenting the system architecture and modes of application of the IoT, Cloud and Big Data and assess the potential impact on society and economy as a whole. Section 2 then moves on to presenting the emerging privacy and personal data concerns associated with the future large scale application of these technologies. It must be noted that of course not all of the IoT and Cloud and Big Data application imply use of personal data (i.e. industrial and agricultural use). This paper further focuses solely on application forms and sectors that imply use of personal data.

2.1.1 Internet of Things - System architecture and socioeconomic significance

System architecture

IoT is a multidimensional paradigm that enables technology with various levels of intelligence communicate, process and exchange knowledge and information by using different platforms[117] IoT is defined as:

> 'term used to describe the increasing connectivity of electronic smart devices and systems, whereby smart devices and systems are able to communicate with each other and share data. Usually the smart devices and systems will be connected wirelessly to local networks and the Internet, and they will communicate with each other without the need for human intervention.''[118]

IoT is often viewed together or applied as synonym with Machine to Machine Communication (M2M). While the IoT refers to interconnection and exchange of data among devices, in order to support the IoT, M2M communication is a necessary to support such data flow. M2M is defined as data communication among devices without the need for human

112 Sundmaeker,et al "Vision and Challnges for Realising the Internet of Things" Luxembourg: Publications Office of the European Union, 2010 doi:10.2759/26127 p:23-25
113 Euopean Comission, " Communication from the Commission to the European Parliament and the Council, The European Economic and Social Committee and the Committee of the Regions: Building a Eruopean Data Economy" Brussels, 10.1.2017 COM(2017) 9 final p:3-10
114 Supra note. 102 p:31
115 Supra note.113
116 European Comission, "The EU Data Protection Reform and Big Data Factsheets", January 2016 Availble at: ec.europa.eu/newsroom/just/document.cfm?doc_id=41523 Last accessed: 21 May 2018
117 Vermesan, O., Bacquet J. "Cognitive Hyperconnected Digital Transformation: Internet of things Intelligence Evloution" River Publishers, June 2017 p: 1-3
118 Definition provided by I-Scoop, https://www.i-scoop.eu/internet-of-things/

interaction.[119]. Further in the paper M2M and IoT shall be used as synonyms. Most known IoT technologies in use today are wearable like Apple watch, googles glasses and fitness and health trackers and home automation appliances that are connected to internet like: thermostats or refrigerators.

Socioeconomic significance

Further investment and deployment of the IoT technologies is of crucial importance both for innovators and policy makers. These technologies hold significant potential for the overall economic growth as well as important advances in diversity of socioeconomic fields like: healthcare, manufacturing, energy, transport[120] and environment. The IoT ecosystem in the EU is solidly established and currently remains at rapidly evolving shaping stage. IoT study carried out by the EC concludes that the IoT technology is already used in all of the sectors and across most of the member states. And even though The IoT ecosystem is currently predominantly supply-driven there are powerful demand forces persistent in the EU market both at public and private sectors. The demand will further emerge from changes of the society and needs of public sector:

Ageing EU population requires more efficient ICT automated healthcare system, growing culture of environmental consciousness, public sectors calls for the Smart Cities initiatives and businesses striving for ICT solution to increase efficiency and explore new smart business opportunities. Overall pace of further development is highly dependent on establishing equal balance between the providers of the horizontal solutions and the suppliers of vertical of vertical services.[121]

The IoT influence areas and practical application forms hold enormous social, environmental and sociocultural potential. Viewing IoT application forms through the lens of the physical settings in which these systems could be deployed provide for a broader view of potential benefits for the society[122]. The scope of application of the IoT includes already familiar technology of Smart Homes: where day to day household object communicate the necessary information for daily tasks. Smart home consists of network-connected ‘smart’ technology that allows controlling, atomizing and optimizing functions such as lighting, climate control, security as well as safety and entertainment features of the house either remotely or by phone, tablet computer or a computer.[123] Smart homes technology represent only narrow scope of the wide range of IoT potential. The full extent of the capacity of IoT could drastically reshape industries and market of good and services and even save lives by healthcare application or preventing natural disasters as well as physical security threats. For instance, Smart Cities technology include automated control over available parking places, regulating the traffic of cars and pedestrians and introducing intelligent highways, that are capable of taking into account road accidents, traffic jams or weather conditions, and based on the

119Ratasuk,R et al. "Overview of LTE enhancements for cellular IoT", PIMRC, Sept. 2015

120 Body of Europea Regulators for Electroncs Communcation Market, “ Enabling the Internet of Things” Availble at: https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-the-internet-of-things p:4-6

121 Supra note 95 p:20

122 McKinsey & Company “the internet of things: mapping the value beyond the hype”, June 2015 “Executive Summary”

123 Definition provided by Coldwell and Banker

processed information issues automated traffic messages to drivers or smart cars. Other Smart City features range from weather adaptive electricity consumption to detection of rubbish levels in containers to optimize the trash collection routes. Other IoT application form examples are wide ranged: from improving wine quality in vineyards, auto diagnosis of cars or aircrafts, remote collection and analysis of patients data, flood and fire detection to control and reporting of air pollution, prevention of landslides and avalanches and early detection of earthquakes.[124] The IoT has all the potential to improve and simplify the life of the citizens, contribute to sustainable growth and bring hyper connectivity and rejuvenate the productivity that has slowed down since the first large scale use of the internet emerged. The positive influences are however only possible provided it combines and guarantees trust and security from the side of consumers.[125]

EU has already invested almost €200 million in IoT research, innovation and deployment[126] and it currently holds around 40% share of the global IoT market, projected to reach a value of around €1.2 trillion in 2020.[127] Large scale lifestyle, market and industry changes brought in by the IoT will inevitably impact the economy both at micro and macro levels. The estimates provided by Ericsson forecasts there will be 29 billion connected devices in the world by 2022, of which around 18 billion will be connected via M2M/IoT. [128] More enthusiastic CISCO estimates that 500 billion devices are expected to be connected to the Internet by 2030. On top of that, McKinsey Global Institute estimate the IoT applications global economic impact (including consumer surplus) of as much as € 9.10 trillion per year in 2025.[129]

Cross sector economic study findings demonstrate how investment and development of the ICT sector has positive economic effect on economic growth both on macro and micro levels. Effective use of ICT can increase growth of enterprises of any size at any stage of economic development it also increases gross domestic product (GDP) and factor productivity(FTP) growth. Other indicators show increased levels of labour productivity, gains in employments, gender equality and overall rise in standards of life.[130]

While further expansion of the IoT will provide for efficiency and innovation gains, further cost saving and revenue opportunities, there are also range multiple challenges both at economic and legal levels to be addressed and considered. Such as, restricted employment market, deficit of skilled specialists and most importantly the privacy and security concerns. The overall scale of impact and pace of IoT effect on economic growth is highly dependent on the successful addressing the rising privacy and related security issues.

2.1.2 Cloud computing and Big Data Ecosystem

124 Libelium.com " 50 Sensor Application for a Smart Home" Available at: http://www.libelium.com/resources/top_50_iot_sensor_applications_ranking/ Last accessed: 20 May 2018
125 Bassi, A et al "Enabling Things to Talk", Springer, Berlin 2013, https://doi.org/10.1007/978-3-642-40403-0 p:5
126 Supra note 108
127 Ibid.
128 Forecast availble at: https://www.ericsson.com/en/mobility-report/internet-of-things-forecast
129 Supra note 122 p:4
130Yousefi, A., "The impact of information and communication technology on economic growth: evidence from developed and developing countries", Economics of Innovation and New Technology, 20:6, 2011 581-596, DOI: 10.1080/10438599.2010.544470

System architecture

Cloud computing is the backbone of the future digitalization. Cloud infrastructure holds major role for the IoT application forms described in previous section. In order for the world of networked devices to function and communicate there is a need for storage capacities, platforms for processing the data as well as data analysis (Big Data) systems in place. European Commission Cloud Expert Working group provides for broad definition of cloud computing as a

> "platformed infrastructure of resources involving multiple stakeholders and providing a metered service at multiple granularities for a specified level of quality."[131]

Cloud computing can be characters by five core attributes: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service[132]. The Cloud services are distinguished in database as service, software as service, platform as service, infrastructure as service and software as service.[133] There are also four key deployment models distinguished: private cloud, public cloud, community cloud and hybrid cloud.[134] In practice, Cloud services are network based access tools that are widely used by millions of EU citizens on daily basis. Some examples of services that are Cloud-based are: WhatsApp, Skype; catboats like Siri, Alexa and Google Assistant, online use Office tools of MS Office 365, online customer management tools, storage services like DropBox and Google Drive or platforms that allows developing of applications online.

Cloud computing is often addressed jointly with the Big data analytics- processing large amount of data by automated means and from various diverse sources. The source of such data comes either from manual encoding or is generated by various machines like satellite images, photos and videos, GPS signals.[135] With Big Data organization are able to combine the diverse data sets in order to use them for aggregations, statistics and other *data mining* techniques. Big data analysis can result in extraction of surprising correlation and hidden information[136]. The three defining features of Big Data are: First, collection of massive scale of data online, through smart devices and apps. Second, relying on Cloud computing for use of high speed, high transfer rate computers with millions of gigabytes storage volume and third: use of new computational frameworks for storage and analysis of the data.[137]

Socioeconomic significance

Cloud computing and Big Data, just like IoT currently are major trends in the European service outsourcing market. Industry experts predict it to develop into a standard for businesses in the future as increasing deficit of ICT filed professionals is creating demand for outsourcing some of the in-house services.

---

[131] Schubert L., " the future of Cloud Computing" By the Commission of the European Communities, Information Society & Media Directorate-General, Software & Service Architectures, Infrastructures and Engineering Unit. P:5
[132] National Institute of Standards and Technology, "NIST Definition of Cloud Computing," http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf, Accessed 21 May 2018
[133] Ibid
[134] Ibid
[135] European Comission, "The EU Data Protection Reform and Big Data Factsheet" January 2016
[136] Rubinstein, I. "Big data: the end of privacy or a new beginning?." (2012) International Data Privacy Law, 2013, Vol. 3, No. 2 p:74
137 Ibid. P:77

For the Cloud service markets projected is €44.8bn by 2020 (five times the market size in 2013)[138] with the public and private investments estimated at €6.7 billion.[139] Cloud services add flexibility to the local IT environments, as it is cost cutting, capital expenditure free. By using cloud computing entities are able to use online remote servers to store, manage and process their data with no need for local servers and hardware investments. Cloud computing has a potential to change the competition in the marketplace, as lower costs would increase competition by enabling the small and medium enterprises (SMEs) to compete with industry leaders by having immediate subscription or pay-as-you access to the same scale virtual technology as industry leaders.[140]

The EU supported Deloitte study "Measuring the economic impact of cloud computing in Europe" provides a series of projections of the development in cloud services. The study finds that currently the most intensive sectors to use Cloud are banking and finance, followed by public sector. And estimates multiple positive future impact trends of cloud on macro-economic level, such as: contribution of 0.71%(103.2 billion euros) to EU annual GDP in 2020, positive impacts on job creation and employment (as high as 2.3 million jobs created through Cloud Computing by 2020) as well as creation of new SMEs businesses (ranging from 100,000 to 800,000 new SMEs depending on the estimated scenario).[141] Other studies carrying out in-depth macroeconomics effect analysis finds other positive trends, among them: changes in the competition structure of the marketplace, increase in innovation, increase in production, potential for lower prices, markups and inflation in the long-run, increased non-ICT employment may increase tax revenues.

Biggest internet companies like Facebook, Google, Amazon and Microsoft use Big data in various forms of applications. Big Data enables business to infer previously unknown patterns in databases,[142] analyse the behaviour of the clientele, personalize the provision of services as well as automate some of the internal process such as recruitment or statistical analysis. With the outsourcing to the cloud and further cost reduction Big Data will stop being a tool accessible only to internet industry giants. Any business that requires statistical analysis or data mining algorithms will be able to afford the use of Big Data, thereby improving decision making, enhance efficiency and increase productivity.

IoT, Cloud and Big Data infrastructures at their core are based on various degrees of data processing, manipulation and data transfers and even though the risks and concerns over automated data processing have been addressed with legal and technological solutions as early as 1960s, it is the new enormous scale of the IoT, Cloud and Big Data technology application forms and unprecedented scale of the amounts of data that brings the privacy concerns and security risks to a new levels.

Here it is important to come back to the two approaches to the data protection presented in Chapter 1 – the economic and fundamentalist approach to the goals of the data protection law.

---

138 European Comission, "Cloud computing" Availble at: https://ec.europa.eu/digital-single-market/en/policies/cloud-computing Last accessed: 21 May 2018

139 Ibid.

140 Laverty et al. "Micro and Macro economic analysis of Cloud Computing" Issues in Information Systems, Volume 15, issue II p:293-302

141 Deloitte for European Comission : Measuring the economic impact of cloud computing in Europe" 2016 p:1-9

142 Supra note 136 p:76

While economists argued that the data protection in EU always aimed at the interests of the market and fundamentalists concentrated at the basic human right needs. It can be argued that digitalization of everyday life both in private and business sectors puts end to the separation between economic and innovation aims and the protection of the individuals rights. Innovation today is interest of everyone as public is the main beneficiary of new technology. Today one cannot simply weight the economic benefits against the threats to privacy. Pace of economic growth today are highly dependent on how efficiently are privacy and personal data concerns addressed.

While the furthers expansion of the IoT will provide for efficiency and innovation gains, further cost saving and revenue opportunities, there are also range multiple challenges both at economic and legal levels to be addressed and considered. Such as, restricted employment market, deficit of skilled specialists and most importantly the privacy and security concerns. The overall scale of impact and pace of IoT effect on economic growth is highly dependent on the successful addressing the rising privacy and related security issues.

2.2 IoT, Cloud and Big Data – assessment of the related privacy and personal data risks

This section presents the literature findings and identifies most commonly addressed privacy and personal data concerns in relation to IoT, Cloud and Big Data developments. It then provides an overall summary on the pattern of the threats as well as singling out the highest risk areas to be further analysis provided in Chapter III.

There is growing body of literature and research into the emerging personal data protection challenges and vulnerabilities in regards to further expansion of IoT, Cloud and Big Data infrastructure development. The reports and studies on direct effects of further digitisation of society on privacy and personal data preservation are approaching the issues with various intentions. Such as: provision of guidance to data processors and data controllers; addressing future legal challenges as well as for the purpose of rising the end-user caution and digital competence. Regardless the aim of the source, there is a clear pattern of agreement on the key high vulnerability areas.

Another important and evident pattern is that all but one of the mentioned thereat areas associated with the growing digitalization are associated with already established ICT vulnerabilities. Majority of the risks currently associated with the IoT, Cloud and Big Data have been present since the early spread of computation in the 1960s: Cyber-attacks, surveillance, data breaches, data mining, profiling and security related concerns have been well established for more than half a century. At the core of all privacy concerns of the future are the growing technical capabilities of technology, the further spread of technologies into private and business lives as well as the growing role of the so called *economics of personal data* analysed in Chapter I. The only new risk type that is emerging from the technologies like IoT, Cloud and Big Data is the possibility of total loss of control and accountability of the technological intrusion due to rapid development and lack of effective regulation.

Ziegeldorf et al. (2013) provides for detailed analysis of the privacy threats in IoT and proposes 7 core threat categories: Identification, localization and tracking, profiling, privacy

violating interactions, lifecycle transitions, inventory attacks and linkage. IoT technologies provides for new wide range of opportunities to trace an individual. Process of identification, of the individual in the IoT becomes more advanced, as IoT are capable to recognition voices, facial features and fingerprints, thus generating powerful databases full of parameters of the individual. Same applies for Localization and tracking opportunities, as it is often a basic functionality of many IoT devices. With further development of IoT individual will be tracked through *time and space*[143]. The developing IoT devices will further aggravate the identification and tracking features by making the data collection less intrusive and passive and collect information from multiple smart appliances and sources, like transportation, wearables, house appliances or IT equipment at work. In a similar way profiling and linkage will become more powerful as data collection becomes available from previously untouched parts of users private lives and linkage among different sources of data will result in aggregation of information that individual was not willing to disclose.

As things become more connected public services will require even more digitalized personal data in exchange for use of the service, therefore privacy violating interactions will be forced on the individual, resulting in need to disclose personal preferences and details to the unwanted audience.[144] Lifecycle transition and inventory attack risks refer to unwanted access of the third parties to the data held by the IoT devices either by being stolen, lost or resold or by other way of unapproved access from the third party. These accessed will be damaging for privacy, security and economic reasons as vast amount of information and possibly connection to other smart devices will become exposed.

Body of the European Regulators for Electronic Communication Market (BEREC) report *Enabling the Internet of Things* highlights the crucial importance of the respect and protection of end-users' privacy as critical success factor for the realization of the prospects and growth of IoT services. If users are not ensured that their data is being handled appropriately they might restrict or opt out of the use and sharing of the technology. BEREC report is addressing the IoT technical characteristics and assess potential future regulatory issues. The report highlights three core data protection threats associated with further development of the IoT in a similar manner as the study of Ziegeldorf et al.; BEREC puts emphasis on the possible damaging effect of new capabilities and scope of profiling technologies; highlights that the traditional security approaches currently applied in the electronic telecommunication may not be sufficient to address the low cost IoT devices, as an increasing number of less secured connected machines exposed to wider audience will become a target for attacks and breaches; and third major concerns is that data subjects might lose control over the dissemination of their data due to increasing uncontrollable scale of digital machine collecting the data.[145]

143 Ziegeldorf et al. "Privacy in the Internet of Things: threats and challnages" SECURITY AND COMMUNICATION NETWORKS Security Comm. Networks 2014; 7:2728–2742 p: 2728-2738 Published online 10 June 2013 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.795

144 Ibid. p:2736

145 Body of Europea Regulators for Electroncs Communcation Market, " Enabling the Internet of Things" Availble at: https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-the-internet-of-things p:35

Another EU body - European Data Protection Supervisor (EDPS) have also contributed towards identification and analysis of high level data protection concerns emerging from IoT and Cloud technologies. For the IoT the top risks identified by the EDPS are: Risk of eavesdropping when personal data is stored in tags or connected; profiling by tracing users without their knowledge and that by further expansion technology will be so integrated that it may become invisible, resulting in absolute loss of control and track of data.[146] For data protection in Cloud computing EDPS identified wide variety of sensitive areas such as: unauthorized access to data due weak cloud security and virtual machine vulnerability and subsequent abuse and data leaks, possible surveillance by governments or other interested parties, data subject losing control over their data as organizations are not able to comply with requirement for safeguarding that data and providing the information, as well as vendor lock-in risks, where data is lost if the service provider is experiencing technical or financial difficulties.

The list goes on and repeats, IoT Report of Center for Strategic and International studies point out that large scale IoT use will inevitably result in reorientation in perception of privacy and personal data protection, since practices of network security as well as of data processing differ on scale and application in IoT. The report again points a very similar risk patterns: unfeasible task to secure IoT networks from breaches and intruders; new scale challenges to data localization due to enormous expansion of the amounts of data processes – *'flood of new data on personal behavior'*, as well as other factors that might further deepen the future technological crisis: technological uncertainty, limited international cooperation, weak online identities.[147]

The IoT and Cloud computing challenges to data protection are equally applicable to the Big Data analytics, since the technologies are interlinked. There are however also separate set of threats emerging from the Big Data technologies. Rubinstein (2006) – compares the Big Data analytics as *data mining on steroids*[148] Rubenstein provides analysis on the effect of Big Data on the society and how it fits in the current Data Protection framework. Big Data intensifies existing privacy concerns over data mining, tracking and profiling. As profiling technologies now extend from already known cookies to advances profiling technologies that are capable to apply non-public algorithms to vast amount of data from every aspect and phase of individual and social life. *As a result, the produced information is not only unintuitive and unpredictable, but is also a product of rather opaque process*.[149]

Having presented the literature few additional conclusions can be made regarding the personal data preservation risks and concerns in IoT, Cloud and Big Data. First, overall, all of the reviewed sources show pattern to identify same or similar set of threats and concern areas, with different methodologies, level of details and scopes for the analysis (more technical, regulatory, purely legal or compliance orientated). Second, while the IoT, Cloud and Big Data have different system architectures and application forms, when it comes to privacy and

146 European Data Protection Supervisor (EDPS) presentation "EU data protection view on IoT: The EDPS experience" Enisa, 17 Septmber 2009
147 Lewis, J.A. " Managing Risk for the Internet of Things" – A Report of the CSIS Strategic Technologies Progam February 2016 p:7-15
148 Supra note. 136 p:76
149 Ibid.

personal data concerns assessment they all share common vulnerabilities and risks due to their important role in processing vast amount of personal data.

Based on the findings of the above literature review for the purpose of this paper the risks are further aggregated into three categories:

1) Data breaches– referring to personal data being disclosed due to negligence, human mistakes and errors as well as hacking, malware, spyware and other types of cybercrime

2) Data mining and profiling – referring to collection of personal data by tracking behaviours and action of smart device and aggregating such data for creation of online statistics on individuals behaviour, actions, preferences and overall private life.

3) Loss of control – referring to individuals being incapable to follow increasing scale of data collection and intrusion of machines in their private life and the respective authorities not being able to react to rapid digitalisation and innovation.

The effect of these risks on society and economic actors are further analysed in sub-section. The analysis is presented with the assumption of the negative consequences if no legal boundaries are in place. Legislation analysis presented in Chapter III then further reviews how these vulnerabilities are addressed by the new EU data protection legislation.

2.2.1 Data breaches

Entrusting important function and private information to machines to act without human intervention is at the core of Cloud, IoT and Big data application forms. What's more these technologies are and will be operating in rather challenging security environments where no computer is fully protected from external manipulation.[150] Storing information in Cloud, be it business databases or photos from a mobile devices means that physical location of the data is with the third party. The IoT devices that are already in use today, security was an afterthought, creating vulnerabilities in the network and the potential for industrial process interruption, manipulation or espionage[151]. Data collected from fitness trackers, health monitors and household devices is aggregated and processed outside the actual device. The IoT device itself is therefore of simplistic structure, without option for the safeguard installations such as malwares and spywares.

Data breaches are costly in both monetary and reputational terms for both businesses and individuals. The Ponemon Institute's 2017 Cost of Data Breach Study found that an average cost of data breach for business is is €3.08 million. What's more, the likelihood of being breached is rising at the same time that companies are dealing with an "information explosion," collecting more and more data about a growing number of people.[152]

With growing use of Big Data, Cloud and IoT ever large databases will be created, including sensitive aspects of personal lives. Data breaches therefore could bring vast damage both for individuals and cooperation's. From the side of data subjects it will mean loss of trust,

150 Supra note.147 p:3
151 IBM Corporation 2018 "Internet of threats Securing the Internet of Things for industrial and utility companies" March 2018 p:2
152 Ponemon Institue "2017 Cost of Data breach Study" Research Report, IBM Security June 2017 p:6

exposure and giving up extensive amount of information that can have negative effect on private life. Negative and even fatal effect on ICT power and intrusion in personal life can already be observed: the suicide of the Italian woman, who won the Italian national 'right to be forgotten' case that ordered her revenge porn video to be removed from social media; [153] or a Frenchman bringing case against Uber for disclosing of his extramarital affair to his spouse by providing information on his route on her mobile device[154].

For cooperation large scale data breaches might result in reputational risks, loss of potential clients and subsequent economic losses in compensation and damages. As the worst case scenarios already mentioned: high impact/scale breaches could lead to consumers to opt out from the use of the service slowing down the demand that would affect pace of innovation and investment slowing down the overall economic growth.

Scholar J.A Lewis provides illustration of IoT security risks by comparing them to car accidents. While car accidents occur often and result in tragic, undesirable and expensive consequences overall they do not have crippling effect on the society. However the further development of ICT and smarter technologies might enable hundreds and thousands of smart devices to be hacked simultaneously resulting in catastrophic risks, mass fatalities and major economic damages.[155] The more digitalization will be introduced the more dangerous and costly will be the effect from the cyberattacks. Deploying technologies without being able to sufficiently secure them will result in "*dangers greater than negative public sentiment".* [156] Even at developing stage IoT is already accounting for 30 percent of all the cyberattacks. And as its use further expands into manufacturing, chemical, oil sectors, security breaches can result in large-spread contamination, environmental disasters and personal harm.[157] As an example, one of the most recent and widespread WannaCry ransomware attack in May 2017 already demonstrated its effect to paralyse business sectors and cause harm. National Health Scheme (NHS) in UK was one of the affected targets, causing havoc as hospitals were forced to cancel surgeries not being able to access any information on the patients, blood supplies and putting people lives in danger[158].

With further spread of IoT technology into more aspects of human lives, the cybercrime separation may cease as ICT will be used to commit robberies, fraud, and identity theft and cause physical harm or demolition and replace physical instruments.

2.2.2 Data mining and profiling

Data mining is process where multiple sources of information and data sets are used in order to collect and assess patterns of behaviour and eventually generate new information.[159]

153 Aprimo, S., " The Right to be Forgotten, determining the liability of ISP as media platforms and paving the way to a regulated future", law and Policy of the Media in a Comparative Prespectve: Law and Media Working Paper Series p: 8
154 BBC news, " Cheating Frenchman sues Uber for tipping off wife about affair" February 2017, Availble at: http://www.bbc.com/news/world-europe-38948281 Last accessed: 20 May 2018
155 Supra note. 47 p:4
156 Supra note 51 p:3
157 Ibid.
158 BBC News, " NHS cyber-attack: GPs and hospitals hit by ransomware" Available at: http://www.bbc.com/news/health-39899646 Last accessed: 15 May 2018
159 Definition as provided in: https://www.techopedia.com/definition/1181/data-mining

Profiling is the result of data mining, where users behaviour and personal information is aggregated in order to create their online identity. Example of simplistic data mining is popular in online commerce, when website logs customer behaviour looking at several items and then based on this data suggests another similar, items that would be appropriate.. Apart from commerce data mining and profiling can also be used for internal processes of the businesses, advertisements or social engineering.[160] In most cases data mining is used with positive intentions in mind: personalise user experiences, improve decision making and deliver better, targeted services and even applications in science where DNA is mined in order to discover and monitor health aspects and cure diseases. [161]

Nowadays data mining and profiling gains force *through availability of ever large amounts of data, faster computers, new often –automated machine generated analytic techniques*[162] and hyper connectivity as well as cheap and accessible storage space ensured by Cloud. Therefore the results of data mining and profiling could turn against the individual and become highly intrusive, for example by collecting and aggregating data individuals do not wish to be tracked nor associated with them or using the collected data against the best interests of the data subject. In the setting of Big Data and data aggregation, even if individuals initially consents to use of their data, the generated results of data mining and profiling as well as the further use and application is out of their control, thus they are not fully aware to what they consent to.[163] Another negative consequence would be discrimination of individuals, such as price discrimination or other unfair information practices.[164]

2.2.3 Loss of control

The loss of control mostly covered in the future ICT impact assessments are associated with the concerns and rights of the data subjects and their abilities to control and track what happens to their private information. Euroabemter study carried out by the commission prior the GDPR proposal showed that 80% of citizens did not think they had complete control of their personal data; 60% did ot trust online businesses; while more than 90% of Europeans say they want the same data protection rights across all EU countries.[165] There are however other areas where it is essential to maintain balance and control in order to achieve all of the economic and social prospects that the digital economy has to offer. Businesses need to be able to operate efficiently, while at the same time being accountable and transparent about the use of personal data. The legal system must therefore also be in control and guarantee appropriate, innovative safeguards and up to date laws to ensure the system of checks and balances.

As described in Chapter I, need for privacy and private life control is a basic need enrooted in human nature, therefore it is essential for individual to be able to safely navigate in the digital

160 Supra note 143. P:2736
161 Fan, W. and Bifet, A., 2013. Mining big data: current status, and forecast to the future. ACM sIGKDD Explorations Newsletter, 14(2), pp.1-5.
162 Supra note 136
163 Ibid.
164 Online price discrimination and personal data: A General Data Protection Regulation perspective
165 European Comission, "The GDPR ŅNew opportunities, new obligations" Luxembourg: Publications Office of the European Union, 2018 p:3

environments without negative sentiments as well as to be able to control the aspects of their lives that they wish to remain personal[166]. On the other hand if unproportioned *legal limitations and high regulatory costs*[167] are in place, digital market would not develop as economy, science and innovation in Europe would stagnate. Loss of control could also occur in relation to legislation not being able to ensure data protection and privacy safeguards; ensure healthy balance between needs of economy and those of the data subjects or not being able to keep up with the pace of the rapid digitalization and innovation due to restrictive legal procedures or limiting legal interpretations and definitions.

3. CHAPTER III: ASSEMENT OF REGULATORY AND LEGISLATIVE INSTRUMENTS IN THE LIGHT OF DIGITAL ECONOMY CHALLENGES

It is evident that GDPR will inevitably change the day to day operations and processes for each business who works with personal data of the EU residents. Global business study carried out by Ernst and Young in February 2018 demonstrates that only 33% of respondents had a clear plan to address the GDPR compliance, while other 39% admitted that they are not at all familiar with GDPR.[168] The existing state of alarm and discontent currently persistent across sectors serves as a proof that data protection obligations and overall awareness have been secondary in the day to day operations and processing of personal data, regardless the fact that the provision of the Directive have been implemented in the national law already since 1995.

While it is yet too early to assess the full extent of the GDPR impact as it is to be seen if it will result in a burdensome evolution or revolution of the data protection in the EU. Conclusions however can be drawn in regards to how much attention have been devoted to the growing digitalisation and new technologies in the newly introduced rights and obligations of the GDPR

This chapter aims to assess the existing legal framework on personal data protection in EU in the light of privacy concerns emerging from the digital economy and technological progress described in Chapter II. Two levels of analysis are provided under separate sections. First section presents overall analysis of new provisions of the GDRP in comparison to DPD with an aim to present the extent of the newly introduced legal instruments and asses their potential impact on further development of the EU digital economy as well as the balance between the economic interests and data subjects rights. Second moves to further asses how (and if) the core privacy concerns reviewed in Chapter II are addressed in the GDPR. Third and last section of this answers the research question and based on the analysis carried through the whole paper suggests additional measures to be further promoted in parallel with the existing

166 Centre for Buiness Research, "The Internt of things Shaping our future" , University of Cambridge:2-14 p:14
167 Ibid.
168 Ernst and Young, "Global Forensic Data Analytics Survey 2018" Availble at: http://www.ey.com/gl/en/services/assurance/ey-global-forensic-data-analytics-survey-2018

EU data protection system in order to maximise the benefit and minimise the risks of the digital economy.

3.1 GDPR vs DPD: Assessment of the new provision in the light of ICT and differing interests in digital economy

This section presents the core new provision of the GDPR as compared to the repealed DPD. The analysis is carried out with an aim to overview what new changes have been brought to the data protection playfield and elaborate what the set of new rights and obligations would mean for both business and data subjects in the light of the digital economy.

3.1.1 New geographical scope

Perhaps one of the most debated and significant change incorporated in the GDPR is the new scope of application of the data protection provisions on all EU residents data processed, regardless of where the data processors is located. Article 3 of the GDPR provides that the regulation applies:

> "if the establishment of the processor is located in the EU regardless if the processing takes places outside; if the data subjects are located in the EU and the intention of processing is either of commercial or monitoring nature"[169].

In practice this means that all companies all over the world that want to relate their business activities with the personal data of EU residents are obliged to comply with the GDPR. DPD was not near as expansive in its territorial scope, and if it would have been, the impact would not have been of the same force, due to its nature of a Directive and that of more narrow definitions and overall nature. While the new scope of application is definitely serving the best interests of EU residents, nevertheless it is, provided that all parties involved respect GDPR provisions, expanding the possibilities of the EU marketplace that will be crucial element through course of further expansion of the digital economy and markets. The new geographical reach is crucial for the described future of IoT, Cloud and Big Data as these paradigms are global and inevitably will imply large scope cross boarder functions and use. Therefore GDPR is in fact going ahead of time and despite causing today's uproar of the businesses abroad, it is in fact addressing some future ICT challenges ahead of time.

3.1.2 Personal data redefined

GDPR expands the definition of personal data. GDPR adds elements to the previous definition of DPD definition of:

> "reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" [170]

New definition of the GDPR now includes location data, online identifiers as well as genetic identity aspects. What more, unlike in DPD the list is now non-exhaustive. The new definition

169 GDPR Article 3
[170] DPD Article 2

of personal data will have important effect on for e-commerce, targeted online advertising and any other industry that base their activities on processing of information of IP address, mobile identifiers, biometric data or location trackers. What's more many types of cookies also become personal data under the GDPR, thus requiring informed consent and stricter rules for companies who continue to use them. Another important aspect is the non-exhaustive nature of the identifier list, meaning that when future technological identifiers are already covered under the GDPR.

Overall as it will be shown in further analysis, provisions of the GDPR are constructed in the way to be technology-neutral, meaning that the drafters have aimed to take into account also the future technological developments. This could greatly benefit the rights of data subject in the future and ease the matter of interpretation, when in the result of future innovation new digital methods for processing personal data will emerge.

3.1.5 New rights for data subjects – access, erasure, portability

It is evident that the new provision of the GDPR are addressing the calls of the EU citizens for better data protection by providing set of new right to individuals as well as imposing new obligations on processors and controllers.

The right for access as provided in the DPD was limited to the obligation on the data controller to confirm if the personal data was processed and inform what type of data is being used. Article 15 GDPR now additionally obliges the data controller to provide the personal data itself (not just the information on type of data) in machine readable format and free of charge. Data subject must also be informed about the appropriate safeguard ensured in case their data had been transferred to third countries. New obligation envisaged under Article 15 might inevitably places more burden on the administration of data subject rights, what's more it might also require introducing significant changes in the software and databases so the personal information can be easily extracted from datasets. Thus, resulting in time and efficiency losses to the controllers and processors.

Another new provision and rights is envisaged under Article 20 – Right to data portability. This right now allows the data subjects to not only to obtain the personal data from the controller but also to transmit such data to another party of choice. This new provision will inevitably change the market relationship and overall perception of value of data, as business will have to compete and demonstrate what value they are producing by being the ones in control of processing ones data.

Another new right is provided under Article 17 GDPR -Right to erasure ('Right to be forgotten) this right allows the data subject to obtain from the controller the erasure of personal data concerning him or her without undue delay if certain criteria is fulfilled.

The criterions for legitimacy of request are: if data is no longer necessary for the purpose; data subject withdraws the consent; it has been unlawfully processed; personal data is related to an underage person. Controller may or might not agree to erase the data subject to list of exception as well as proportionality of request based on available technology and the cost of implementation.

Effectiveness of the new rights has yet to be seem once practically applied. One evident future problem would be that data controllers may be challenged with increasing burden of erasure of information. On one hand it will evolve new technology where erasure is an option integrated by design, but at the beginning stages, since all of the personal data is being treated as equally valuable, except the sensitive data categories, unnecessary resources might be wasted when erasing personal information that are fulfilling the criteria for request, but does not have any welfare added value to the data subjects.

3.1.3 Obligation for governance and security

GDPR introduced multiple new *ex-ante* action for better addressing the data protection. These action include privacy by design and by default, designation of data protection officers (DPO) and obligation for data protection impact assessment.

As provided in Recital 78 – *in order to be demonstrate the compliance, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and by default.*[171] Recital gives multiple examples of such measures: minimisation of use of personal data, pseudonymisation, transparency, enabling data subject to monitor the processes as well as improving the security features.[172] As provided in Article 25 the controllers are now responsible for investing in different types of safeguard and measures to ensure they comply with the provision of the regulation, including, if necessary designating a certified DPO, [173] which under the DPD was not required in private sectors. DPO will now be a must in public bodies, in entities that process large scale of personal data as well as in organisation who base their operation processing sensitive data.[174] Another new provision is the data protection impact assessment as provided in Article 35. The impact assessment is required in particular when using new technologies as well as in overall processing that could result in high risks for data subjects. What's more, in cases where the impact assessment results demonstrate that data controller cannot mitigate there is an obligation to priory consult the supervisory authority prior the processing.[175] As explained in the Recital 89 – DPD also imposed the requirement to consult the supervisory authority, which only resulted in financial and administrative burden without improving the quality of the data protection, therefore the mechanism of the ex-ante new risk assessment is introduced to better address high risk operations. [176]

The new obligation for governance and security are positive if viewed from the perspective of the emerging ICT and digitalisation, since: organisation dealing with large scale (scope yet to be clarified) of personal data processing will have a designated, field professional to monitor the processes, as well as the supervisory authorities will be required to be involved when particularly when new technologies will be used and developed to process personal data. On the other hand the new provisions again place significant burden on the data controllers and processors that will be costly as they will require resources.

[171] GDPR Recital 78
[172] Ibid.
[173] GDPR Article 25
[174] GDPR Article 37
[175] GDPR Recital 84
[176] GDPR Recital 89

3.2 Assessment of role of GDPR addressing growing privacy and personal data concerns

This section shall further focus on the assessment of the particular instruments envisaged in the GDPR for addressing the emerging digital economy risks identified in Chapter II, namely: Data breaches, profiling and data mining as well as overall measures for ensuring that data subjects, processors and controllers and the Regulation itself have effective and practical measures in place to control the data protection process.

3.2.1 Addressing data breaches and cybercrime

In regards to data breaches the GDPR provisions are detailed, strict and impose serious fines. Article 33 provides for rules on notification of a personal data breach to the supervisory authority. In case of data breach data controllers are required to notify the supervisory authority – *without undue delay, and, where feasible, not later than 72 hours after having become aware of it*[177] in case the deadline of 72 hours is not reached explanation must be provided on why was the deadline not respected. Article 33(3) details the obligations for content of notification, that must include the nature of the breach, number of data subjects concerned; categories of data; contact details of the data protection officer; description of likely consequences as well as the measure undertaken and proposed.[178] Article 34 obliges the controller to also notify the data subject under certain circumstances, especially if he data breach is likely to result in high risk.[179] Article 83 imposes stiff fines in case of infringement of the GDPR. Such fines will be imposed by the local supervisory authority. The amount of fines will be decided on cases by case basis taken into account multiple factors such as: the nature, gravity and duration of the data breach, whether the breach was intentional (cooperate negligence or cybercrime) or negligent; further action taken by the controllers; degree of controllers responsibility; if any previous data breeches occurred; whether the action following the breach where lawful and if authorities were notified. [180] The envisaged ceilings for the breaches are extremely high, with fines up to 20 million euros or 4% of worldwide annual turnover, which in case of internet giants like google or Facebook would amount to billions of euros.

Such strict rules might result in multiple different actions and patterns from the side of business. Under the best case scenarios these new obligations and fines of GDPR will encourage business to innovate and secure their environments by carrying out effective impact assessments and prior consultation (Article 35 and 36 GDPR), promoting data protection culture across their organisations and investing in malware, spyware and overall security in order to prevent data breaches. As a result insurance of the business data breach risks would likely develop as a new business models. Another effect could be move towards data minimisation, anonymization and release of personal data in order to avoid the damage in case of possible breach. Another less positive but likely scenario is that some data breaches

[177] GDPR Article 33
[178] GDPR Article 33(3)
[179] GDPR Artilce 34
[180] GDPR Article 83

will remain undisclosed as business will choose to hide the information in order to avoid fines and the reputational risks. In this scenario two major negative impact will take effect. First, data subjects will remain uninformed about the leak of their personal information with possible welfare diminishing risks as detailed in Chapter II. Secondly it might further promote the spread of cybercrime and blackmail as business will be faced with dilemma of either facing serious fines and reputational risks or to pay the ransom(in case of cyberattack) in order to keep the data breach undisclosed. Such strategy has already been applied by Uber in US as company hid breach by paying the hackers in 2016.[181]

Overall, even though the GDPR is already final and in force as of May 2018, the further developments and impact of the regulation are still highly dependent on future development and actions undertaken by multiple actors: policy makers, cooperation and especially the national level supervisory authorities.

3.2.2 Addressing profiling and data mining

It is evident that GDPR aims to limit the profiling and safeguard the data subject from dubious automated decisions. For the first time in EU data protection law profiling is separated from other forms of automated decision and broadly defines it:

"profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements"[182]

Throughout the provisions of the GDPR there is visible emphasis on the profiling activities clearly demonstrating that the risk and possible further wider extent of the activity has not been overlooked in the regulation. It is evident that GDPR intends to limit the extent and application of profiling together with usual solely automated decision making. Article 22 states:

"the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[183]

Profiling and automated decision making could still be applied under certain conditions – contractual relationship; if it is authorised under another EU or MS law, or it is based on explicit consent of the data subject.[184] The article 22(4) further states that special categories of data (such as racial, religious, biometric and sexual)[185] could only be profiled under two strictly limited circumstances if data subject has given his explicit consent for data to be

[181] New York Times, "Uber hid 2016 Breach, paying hackers to Delete Stolen Data" Availble at: https://www.nytimes.com/2017/11/21/technology/uber-hack.html Last accessed: 21 May 2018
[182] GDPR Article 4(4)
[183] GDPR Article 22(1)
[184] GDPR Article 22(1)
[185] GDPR Article 9 for full list

processed for one or many purposes, unless it is prohibited by MS or EU law [186] or for reasons of substantial public interest proportionate to the aim pursued[187]. Recital 71 gives examples of automated decision and profiling practices that are prohibited to be done without human intervention if they produce legal effects or *similarly significant effects* on data subject refusal for online credit applications, e-recruiting and evaluating personal aspects of life, such as performance at workplace, personal preferences and interests, behaviour, location or movements[188] In cases where profiling is lawfully applied safeguards such as appropriate statistical procedure, technical and organisational measures must be ensured minimise the risk of errors[189].

Obtaining consents under the GDPR cease to be an easy way out as much stricter new rules for obtaining consent are imposed. For entities who will wish to continue their profiling activities via obtaining consent from the data subjects there have new legal and administrative burdens to comply with. First, GDPR broadens the definition of the consent adding that consent shall be not only freely, given, specific and informed (is provided in the DPD) but also – *unambiguous*[190] and it shall be given by a *statement of clear affirmative actions*[191]. Article 7(1) GDPR places the burden of proof on the controllers as it requires them to be able to demonstrate the given consent, meaning the record of consents given will have to be kept. Article 7(2) detailed that information to data subject must be provided in an understandable manner – *using clear and plain language*[192] what's more GDPR give a right to the data subject the withdraw the consent at any time as the processor must provide for easy means to withdraw such consent. Recital 32 provides for details on the conditions for consent, which could be in form of ticking the box, choosing specific settings or another statement that clearly indicates the consent. No activity or pre-set settings shall not be accepted as for of consent. What's more one consent is valid for one data processing purpose.[193] In addition Recital 43 provides that consent will not be considered freely given if consent is given to one type of processing, while used for the other[194] and what's crucial – controller is prohibited to make the service conditional upon consent, unless in cases where processing is necessary for performance of the service.[195]

The above described GDPR approach to automated decisions, data mining as well as the new framework of obtaining consent demonstrates that the risks in regards to development of future profiling and data mining technologies and their impact as described in Chapter II have not been overlooked in the regulation. The GDPR provisions give more control and information to the data subject, while restricting but not completely paralysing the use of personal data for commercial purposes. In fact, the provisions could motivate economic entities to invest in the quality of their infrastructure, approach to data protection and their

[186] GDPR Article 9(a)
[187] GDPR Article 9(g)
[188] GDPR Recital 71
[189] GDPR Recital 71
[190] GDORArticle 4(11)
[191] GDPR Article 4(11)
[192] GDPR Article 7(2)
[193] GDPR Recital 32
[194] GDPR Rectical 43
[195] GDPR Recticel 43

clients, as consent of data subject now also becomes an asset for businesses, just like personal data. The new approach of the GDPR will also rise the overall digital competence of the EU residents, since there will be inevitably more qualitative information in regards to what happens to their personal data.

3.2.3 Future of data protection: Ensuring accountability and control

The task of the GDPR is not only to ensure balance between multiple actors and their interests on paper, but to guarantee the new obligation and rights are useful, effective and applicable in practice. For the latter the new regulation has already received wide range of criticism. As it has been demonstrated above, when assessing separate intention of the GDPR against the risks of the digital economy there are multiple positive patterns and controls in places that clearly indicates that at the EU level much thought and detail have been devoted to addressing wide range of current and future technology impacts on the data processing. However high risk uncertainty remains on capabilities of all actors involved in the data protection to handle both: the heavy weight of the GDPR and the rapid changes of the digital world. This section presents few crucial points of criticism already targeting the GDPR as an instrument and argues that ensuring the control in practice is the core weak point of the GDPR.

Koops, Dutch Professor of Regulation and Technology argues that data protection laws in Europe are disconnected from reality of the 21 century digital economy. Koops criticizes various aspects of the GDPR among them, the overall notion of consent serving as legitimate basis for data processing, since consent is *only theoretical and have no practical meaning,*[196] as individuals will not deny themselves use of popular service and instead will consent without *spending time effort on reading the privacy statements of related to every service they use.*[197] Koops argues that will further complicate the data protection and will eventually result in neither data minimisation nor preventing unnecessary data processing, as business will instead seek for loopholes or simply relay on mercy of the supervisory authorities. [198]

In similar manner Purtova (2018) argues that GDPR is growing too broad and is becoming the law of everything that will likely result in the system overload in the near future.[199] Purtova argues that GDPR while with good intentions in mind, will inevitably become impossible to comply with and it will therefore be ignored. Putrova warns that the current approach to data protection risks to turn the data protection law applicable: "to nearly anyone processing nearly any information at nearly any time, and the threat of serious sanctions omnipresent.*"*[200] In conclusion author warns, that while GDPR might work in short terms, a new approach to data protection is inevitable in the age of internet: it will require either narrowing the scope and application of data protection laws, or reduce the current intensity of compliance and regime of penalties. [201] Similar future approaches are supported by Levin (2017). When assessing the

[196] Koops B., "The Trouble with European Data Protection Law", International Data Privacy Law, doi: 10.1093/idpl/ipu023 Tilburg Law School Research Paper No. 04/2015 p:3
[197] Ibid. p4
[198] Ibid.p7
[199] Purtova, N., " The law of everything. Broad concept of personal data and future of EU data protection law, Law, Innovation and Technology, 2018 DOI: 10.1080/17579961.2018.1452176 p:2
[200] Ibid. p:38
[201] Ibid. P:39-40

overall future of privacy perception, Levin concludes that while the GDPRs the Right to be forgotten and Privacy by design provisions are pointing in the right directions, future will inevitably require a revolution of data protection laws that would consist of combination of regulatory and legal **"**to directly determine and dictate technological privacy protective measures … and to provide private and public sectors with the right incentives, both positive and punitive that would encourage them, nudge them, and, if necessary, force them to come up with more technological solutions**."**[202]

Having analysed the provisions of the GDPR few patterns are evident: First, the new provision of the GDPR significantly increases burden for data processors and controllers. Second, it is evident throughout the new legislation that the drafters have drastically shifted the focus from free flow of personal data and economic interests prevailing in DPD to new set of rights and empowering the data subjects. It is also clear based on the construction of the new provisions that the GDPR takes into account the growing impact of future technology and innovation as well as the growing value of personal data, this can be seen in the serious limitation to profiling activities, new rules of consent, enforcement of privacy by design and by default and the detailed provision in regards to data breaches. Going back to the discussion in Chapter II and the review importance of the new technologies for socioeconomic developments, under the GDPR it is likely that the innovation intrusion in private lives will be slowed down and implemented only through system of checks and balances in regards to processing of personal data. Another important evident pattern is that GDPR will inevitably increase the overall digital competence levels of the EU citizens, by enforcing provision of more clear information delivered to data subjects.

Chapter 3 elaborated on multiple scenarios in regards to the effect brought in by the GDPR in reality, given the enormous number of affected parties in and outside EU it's likely that all of the scenarios will take place at different stages and different parts of the EU (and the world, hence the new geographical scope) While responsible businesses will invest in privacy by design, security and deploy new tools for transparent and accountable data protection measures, others will either neglect the overcomplicated new provisions or purposely circumvent the obligations.

As demonstrated the emerging criticism of the GDPR is arguing that the regulation is too broad, overcomplicated and at the same time without practical means to monitor and insure compliance. This paper argues that even though the GDPR is already adopted, it is yet too early to pronounce it a failure or a success.

There are set of future actions that still can be and should be undertaken in order to maximise the positive impact of the GDPR. First, the focus of the enforcements should be shifted from unclear notion of protection of personal data towards accountability, transparency and responsibility of data processors and controllers. EU and national level authorities must further promote privacy by design and by default, promote cooperate responsibility as well as provide and invest in practical additional technological instruments for safe processing of personal data. Second, administration of data breach fines by the national supervisory authority should be responsibly considered. Penalties to the parties should undergo careful

[202] Levin, A., "Has the Era of Privacy Come to an End?" 2016 Canadian Journal of Law and Technology 15 (1) pp.17-24, p: 15-19

and detailed assessment, by taking into account not only the impact of the data breaches but also the overall impact on the economy. Lastly, this paper would like to rise a point in defence of the GDPR by stating that even though that additional instruments for the personal data protection will be inevitable given the nature of the rapid developments of the digital world, (as example, in 2018 European Parliament have already called for regulation of the Artificial Intelligence technology[203]). The need for new instruments however will not serve as a sign of failure of the GDPR, instead they could be adopted in similar manner as an ePrivacy Directives (now draft Regulations) to compliment the provision of the GDPR and provide for further guidance and sector specific regulation.

CONCLUSIONS

Through the research carried out in this papers, some valuable conclusions are made in regards to the posed question.

First, when exploring the concept of privacy is was shown that: Privacy is need rooted in human nature, therefore it must be preserved and valued as well as balanced with any other aims of society. Therefore privacy must be protected as a right to gain the trust of citizens. What more, the overall approach and conditions of Privacy have its influence on marketplace actors, their behaviour and thus on the economy as a whole, so when approaching the right to privacy other impacts on society are to be taken into account.

This is exactly how development of Data Protection laws emerged in Europe, as policy makers were attempting to balance the needs of trade and economy with the growing national level privacy concerns. The road from adopting the Convention 108 that served as guidance to the directly applicable GDPR took nearly 60 years and should not be viewed as lengthy repetition of failed attempts, but given the differing interests of Members States and changing nature of Europe as a Union – as a final result, that as a process must have undergone the road of different levels of harmonisation. The notion of protection of personal data in EU has always been a limited right, that balances and weights economic needs against the needs of data subjects, today with the adoption of the GDPR a clear shift is visible, as the new law is increasing the burden and responsibilities of economic entities, while giving more rights to the data subjects. This pattern however is emerging from the changes that digitalisation have brought to the society as the overall economic interests and progress become closely interlinked to how effectively the privacy and personal data concerns are addressed. As explored in Chapter II, the development of new technologies like Cloud, Big Data and IoT hold the potential to increase the welfare and quality of life of individuals as well as significantly contribute to the overall growth of economy and role of the EU in the world, but only if correctly addressed and controlled, especially in terms of technological intrusion in the private, previously untouched sphered of lives. The research question of this thesis was: How capable and effective is the newly adopted EU data protection legislation to address the growing future privacy and data protection concerns associated with expansion of the Digital Economy? Having carried out the assessment of both the risks and emerging threats of the

[203] European Parliament News, "MEPs call for EU-wide liability rules" Available at: http://www.europarl.europa.eu/news/en/press-room/20170210IPR61808/robots-and-artificial-intelligence-meps-call-for-eu-wide-liability-rules Last accessed: 20 may 2018

digital economy and the new provision of the GDPR this paper concludes that, GDPR provisions as drafted have profoundly taken into account the challenges of the digital era. New provisions for privacy by design, geographical scope, enlarged, non-exhaustive definition of the personal data together with extensive list of obligations for data controllers and processors and the overall technology neutral stance of the GDPR is a clear attempt to target the rapid, unpredictable expansion and intrusion of the smart technology. However in order for GDPR to be effective not only on paper but also in practice additional measures are to be undertaken by both EU and national policy makers after its adoptions. This paper recommend that future data protection actions are to be focused on promoting cooperate responsibility, rising levels of citizens digital competence and most importantly investing in technological responses to technological challenge.

BIBLIOGRAPHY/SOURCES

Primary sources

- 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)
- Treaty on the Functioning of the European Union
- CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION (2000/C 364/01)
- 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
- Sweden Data Protection Act (No. 289 of 1973), unofficial English translation available atwww.skolverket.se
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,

Secondary sources

European institution's official publication

- European Comission, "A Digital Single Market for Europe: Commission sets out 16 initiatives to make it happen" May 2015 Availbe at: http://europa.eu/rapid/press-release_IP-15-4919_en.htm Last accessed: 15 May 2018
- European Comission, "Digital Single Market" Available at: https://ec.europa.eu/commission/priorities/digital-single-market_en Last accessed: 20 May 2018
- European Comission, "European Union explained: Digital agenda for Europe" Luxembourg: Publications Office of the European Union, 2014 Availbale at: http://eige.europa.eu/resources/digital_agenda_en.pdf
- European Comission, Comission Staff working Document "Mid-Term Review on the implementation of the Digital Single Market Strategy A Connected Digital Single Market for All" May 2017 {COM(2017) 228 final}
- European Commission "Europe 2020 Strategy" Availble at: https://ec.europa.eu/info/business-economy-euro/economic-and-fiscal-policy-coordination/eu-economic-governance-monitoring-prevention-correction/european-semester/framework/europe-2020-strategy_en
- European Commission, "The EU explained: Digital agenda for Europe"
- European parliament technology assesment, "ICT and Privacy in Europe", Final report October 16 2006, p:72 available at: https://teknologiradet.no/wp-content/uploads/sites/19/2013/08/Rapport-ICT-and-Privacy-in-Europe.pdf last accessed: 14 May 2018 Luxembourg: Publication Office of the European Union, 2014
- Proposal for a regulation of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
- Reading, V., "Speech of Vice president of European Commission" Innovation Conference Digital, Life, Design, Munich: 22 January 2012 available at: https://ec.europa.eu/commission/commissioners/2014-2019/katainen/announcements/vice-president-katainens-speech-sustainability-and-innovation-conference-brussels-12-october-2017_en last accessed: 20 May 2018
- Report from the European Commission "First Report on the implementation of the Data Protection Directive (95/46/EC)" /COM/2003/0265 final
- Wauters P., Van Der Peijl S. et al. "Measuring the economic impact of cloud computing in Europe" Deloitte for European Commission, 2014 DOI:10,2759/75071

Books and E-books:

- Bassi, A et al "Enabling Things to Talk", Springer, Berlin 2013, https://doi.org/10.1007/978-3-642-40403-0
- Centre for Buiness Research, "The Internt of things Shaping our future" , University of Cambridge:2-
- De Hert, P., "The Right to Protection of Personal Data. Incapable of Autonomous Standing in the Basic EU Constituting Documents?" Utrecht Journal of International and European Law .31 (80), 2015 pp .1–4 . DOI: http://doi.org/10.5334/ujiel.cz
- European Union Agency for Fundamental Rights, "Handbook on data protection", 2014
- Jay, R., "Data protection law and practice" 4th edition, Thomson Reuters, 2012
- Karegar, F., Pulls, t., Fischer-Hübner S. "Visualizing Exports of Personal Data by Exercising the Right of Data Portability in the Data Track - Are People Ready for This? IFIP Advances in Information and Communication Technology, 2017 DOI: 10.1007/978-3-319-55783-0_12
- Kuschewsky, M., "Data Protection & Privacy", European Lawyer, 2016
- Madsen W, "Handbook of Personal Data Protection", Palgrave Macmillan,1992

- Parent, W., A., "Privacy, morality, and the law." In Privacy, pp. 105-124. Routledge, 2017.
- Solove D.J., "Nothing to Hide: the False Tradeoff between Privacy and Security" New Haven & London: Yale University Press, 2011
- Sundmaeker,et al "Vision and Challnges for Realising the Internet of Things" Luxembourg: Publications Office of the European Union, 2010 doi:10.2759/26127 p:23-25
- Trepte, S., Reinecke, L., "Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web" Springer Science & Business Media, 2011,
- Tzanou, M., "The Fundamental Right to Data Protection Normative Value in the Context of Counter-Terrorism Surveillance" Bloomsbury Publishing, 2017.
- Vermesan, O., Bacquet J. "Cognitive Hyperconnected Digital Transformation: Internet of things Intelligence Evloution" River Publishers, June 2017
- Vittet-Philippe, P., "EU POLICY FOR THE E-ECONOMY EUROPE IN THE E-ECONOMY: CHALLENGES FOR EU ENTERPRISES AND POLICIES" Computer Law & Security Report Vol. 18 no. 1 2002
- Zekos, Georgios, Risk Management and Corporate Governance in 21st Century Digital Economy. (New York: Nova Science Publishers, 2014)

Journal articles:

- Acquisti A., Brandimarte L., Leowenstein, G., "Privacy and human behaviour in the age of information" Science Mag, Vol 347:Issue: 6221
- Acquisty A., College, C. "The Economics of Personal Data and the Economics of Privacy" OECD Conference Background paper, Centre 1 December 2010
- Aprimo, S., " The Right to be Forgotten, determining the liability of ISP as media platforms and paving the way to a regulated future", law and Policy of the Media in a Comparative Prespectve: Law and Media Working Paper Series
- Bélanger, F.,R. "Privacy in the digital age: a review of information privacy research in information systems." MIS quarterly 35, no. 4 (2011): 1017-1042. p:1020
- Bing, J., "The Council of Europe Convention of the OECD Guidelines on Data Protection", MICH. J. INT'L L. 271 (1984). Available at: https://repository.law.umich.edu/mjil/vol5/iss1/13 Last accesed: 20 May 2018
- Clarke, R., What's privacy? In *Australian law reform commission workshop* (Vol. 28) July 2016 p:3 available at: http://www.cse.unsw.edu.au/~cs4920/resources/Roger-Clarke-Privacy.pdf last accessed: 20 May 2018
- De Hert, P., "The Right to Protection of Personal Data. Incapable of Autonomous Standing in the Basic EU Constituting Documents?" Utrecht Journal of International and European Law .31 (80), 2015 pp .1–4 . DOI: http://doi.org/10.5334/ujiel.cz
- Finn, Rachel L., Wright, and Michael Friedewald. "Seven types of privacy." In *European data protection: coming of age*, pp. 3-32. Springer, Dordrecht, 2013.
- Gryz, J., "Privacy as informational commodity." Proc IACAP, philpapers. org (2013).
- Yousefi, A., "The impact of information and communication technology on economic growth: evidence from developed and developing countries", Economics of Innovation and New Technology, 20:6, 2011 581-596, DOI: 10.1080/10438599.2010.544470
- Karegar, F., Pulls, t., Fischer-Hübner S. "Visualizing Exports of Personal Data by Exercising the Right of Data Portability in the Data Track - Are People Ready for This? IFIP Advances in Information and Communication Technology, 2017 DOI: 10.1007/978-3-319-55783-0_12
- Kemp, R. "Legal Aspects of the Internet of Things", Kemp IT Law, London, June 2017
- Koops B., "The Trouble with European Data Protection Law", International Data Privacy Law, doi: 10.1093/idpl/ipu023 Tilburg Law School Research Paper No. 04/2015
- Kuschewsky, M., "Data Protection & Privacy", European Lawyer, 2016
- Laverty et al. "Micro and Macro economic analysis of Cloud Computing" Issues in Information Systems, Volume 15, issue II
- Levin, A., "Has the Era of Privacy Come to an End?" 2016 Canadian Journal of Law and Technology 15 (1)
- Moore, A. D. "Privacy: Its Meaning and Value." American Philosophical Quarterly, vol. 40, no. 3, 2003, pp. 215–227. JSTOR, www.jstor.org/stable/20010117 last accessed 20 May 2018

- Moore, A. D., "Privacy: its meaning and value." American Philosophical Quarterly 40, no. 3 (2003): 215-227
- Parent, W., A., "Privacy, morality, and the law." In Privacy, pp. 105-124. Routledge, 2017. P:106
- Pomykalski J., "Discovering Privacy—or the Lack Thereof" Information Systems Education Journals, January 2017 p:4 availble at: https://files.eric.ed.gov/fulltext/EJ1135734.pdf: Last accessed: 16 May 2018
- Purtova, N., " The law of everything. Broad concept of personal data and future of EU data protection law, Law, Innovation and Technology, 2018 DOI: 10.1080/17579961.2018.1452176
- Rubinstein, I. "Big data: the end of privacy or a new beginning?." (2012) International Data Privacy Law, 2013, Vol. 3, No. 2
- S.Warren and L.Brandeis "The Right to privacy", Harwards Law Review, 1890 p:194-201
- Schoeman, F., " Privacy: Philosophical Dimensions" American Philosophical Quarterly Vol 21. No 3, 1984
- Schubert L., " the future of Cloud Computing" By the Commission of the European Communities, Information Society & Media Directorate-General, Software & Service Architectures, Infrastructures and Engineering Unit. P:5
- Sololve J.,S., "Conceptualizing Privacy", California Law Review, Volume 90, Isssu 4. P: 1091
- Solove, J.S., "Understanding Privacy", Harvard University Press, May 2008 GGWU Law School Public Law Research Paper No. 420 availble at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1127888 last accessed: 20 May 2018
- Vittet-Philippe, P., "EU policy for the e-economy Europe in the e-economy: challenges for EU enterprises and policies" Computer Law & Security Report Vol. 18 no. 1 2002 p 24-26
- Ziegeldorf et al. "Privacy in the Internet of Things: threats and challnages" SECURITY AND COMMUNICATION NETWORKS Security Comm. Networks 2014; 7:2728–2742 p: 2728-2738 Published online 10 June 2013 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.795

Institutional reports and studies:

- Acquisty A., College, C. "The Economics of Personal Data and the Economics of Privacy" OECD Conference Background paper, Centre 1 December 2010,
- Body of European Regulators for Electroncs Communcation Market, " Enabling the Internet of Things" Availble at: https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-the-internet-of-things p:4-6
- Deloitte for European Commission : Measuring the economic impact of cloud computing in Europe" 2016 p:1-9
- EDPS "Data Protection" https://edps.europa.eu/data-protection/data-protection_en last accessed: 15 May 2018
- Ernst and Young, "Global Forensic Data Analytics Survey 2018" Availble at: http://www.ey.com/gl/en/services/assurance/ey-global-forensic-data-analytics-survey-2018
- European Commission "The EU explained: Digital agenda for Europe" Luxembourgh: Publication Office of the European Union, 2014,
- European Commission, "Special Eurobarometer 460:Summary" March 2017 Availble at: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2160 Last accessed: May 20, 2018
- European Commission, "The GDPR New opportunities, new obligations" Luxembourg: Publications Office of the European Union, 2018
- European Commission, EU Science Hub "Digital Economy" availble at: https://ec.europa.eu/jrc/en/research-topic/digital-economy Last accessed: 18 May 2018
- European Commission DG Communications Networks, Content & Technology "Definition of a Research and Innovation Policy Levaraging Cloud Computing and IoT Combination"
- European Data Protection Supervisor (EDPS) presentation "EU data protection view on IoT: The EDPS experience" Enisa, 17 Septmber 2009
- European parliament technology assesment, "ICT and Privacy in Europe", Final report October 16 2006, p:72 available at: https://teknologiradet.no/wp-content/uploads/sites/19/2013/08/Rapport-ICT-and-Privacy-in-Europe.pdf last accessed: 14 May 2018
- EUROSTAT, "E-Commerce statistics" Available at: http://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce_statistics Last accesed: 21 May 2018
- Hijmans, H. "The European Union as a constitutional guardian of internet privacy and data protection." 2016,Digital Academic Repository; 2016 p:55

- IDC and Open Evidence, Study prepared for the EC "European Data Market SMART 2013/0063", February 1, 2017
- Kemp, R. "Legal Aspects of the Internet of Things", Kemp IT Law, London, June 2017 p:1
- Lewis, J.A. " Managing Risk for the Internet of Things" – A Report of the CSIS Strategic Technologies Progam February
- McKinsey & Company "the internet of things: mapping the value beyond the hype", June 2015 "Executive Summary"
- OECD, "30 Years After: the Impact of the OECD Privacy Guidelines" Conference held at the OECD Conference center Paris, France, 10 March 2010.
- Ponemon Institue "2017 Cost of Data breach Study" Research Report, IBM Security June 2017
- Report from the European Commission "First Report on the implementation of the Data Protection Directive (95/46/EC)" /COM/2003/0265 final
- Stewart, B., The Economics of Data Privacy: Should we place a dollar value on personal autonomy and dignity? The 26th International Conference on Privacy and Personal Data Protection, Poland, Worclaw. Vol. 14. 2004.
- Wauters P., Van Der Peijl S. et al. "Measuring the economic impact of cloud computing in Europe" Deloitte for European Comission, 2014 DOI:10,2759/75071 p:5
- Wolfie C.,Winter, R.,Schweinzer B. " Collecting, Collating and Selling Personal Data: Background Information and Research" Vienna, Austria May 6 2013

Non scholarly Works:

- Reading, V., Speech of Vice president of European Commission, Innovation Conference Digital, Life, Design, Munich: 22 January 2012 available at: https://ec.europa.eu/commission/commissioners/2014-2019/katainen/announcements/vice-president-katainens-speech-sustainability-and-innovation-conference-brussels-12-october-2017_en last accessed: 20 May 2018
- CENTRAL EUROPEAN FinancialObserver.eu, Recent news, Baltic SME optimism wobbly, available on: http://www.financialobserver.eu/recent-news/baltic-sme-optimism-wobbly/, accessed on May 18, 2017.
- Cellarius, M., "The right to informational self-determination: Keep it simple!" https://www.europeanfiles.eu/digital/right-informational-self-determination-keep-simple
- IBM Corporation 2018 "Internet of threats Securing the Internet of Things for industrial and utility companies" March 2018 p:2
- EDPS "Data Protection" https://edps.europa.eu/data-protection/data-protection_en last accessed: 15 May 2018
- Radick R for Forbes, "A Heart-To-Heart From The Hackers: Cyber-Vulnerabilities In Cardiac Devices" availble at: https://www.forbes.com/sites/insider/2017/04/26/a-heart-to-heart-from-the-hackers-cyber-vulnerabilities-in-cardiac-devices/#4e7eaab827b0 Last accessed: 20 May, 2018
- Samsun Privacy Policy, Smart TV Supplement. Availble at: http://www.samsung.com/hk_en/info/privacy/smarttv/
- Cohen, J.E "Examined lives: Informational privacy and the subject as object." Stanford Law Rev. 52, 1373–1438 (2000)
- Wolfie C.,Winter, R.,Schweinzer B. " Collecting, Collating and Selling Personal Data: Background Information and Research" Vienna, Austria May 6 2013
- Cellarius, M., "The right to informational self-determination: Keep it simple!" available at: https://www.europeanfiles.eu/digital/right-informational-self-determination-keep-simple Last accessed: 20 May 2018
- Libelium.com " 50 Sensor Application for a Smart Home" Available at: http://www.libelium.com/resources/top_50_iot_sensor_applications_ranking/ Last accessed: 20 May 2018
- BBC news, " Cheating Frenchman sues Uber for tipping off wife about affair" February 2017, Availble at: http://www.bbc.com/news/world-europe-38948281 Last accessed: 20 May 2018
- BBC News, " NHS cyber-attack: GPs and hospitals hit by ransomware" Available at: http://www.bbc.com/news/health-39899646 Last accessed: 15 May 2018
- European Parliament News, "MEPs call for EU-wide liability rules" Available at: http://www.europarl.europa.eu/news/en/press-room/20170210IPR61808/robots-and-artificial-intelligence-meps-call-for-eu-wide-liability-rules Last accessed: 20 may 2018