UNIVERSITY OF ESSEX

SCHOOL OF LAW

LL.M in Internet Law

2013-2014

Supervisor: Prof. Steve Peers

DISSERTATION

DATA PROTECTION IN THE CONTEXT OF THE INTERNET: THE ADEQUACY OF THE EUROPEAN DATA PROTECTION LAW IN TERMS OF PROBLEMATIC ISSUES POSED BY THE INTERNET

Name: İdil Özcan Cantosun
Registration Number: 1301773
Number of Words: 19.777
Date Submitted: 12 September 2014

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

- **A29WP**: Article 29 Working Party
- **Data Retention Directive**: Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks
- **DPC**: Data Protection Commissioner
- **DPD**: Directive 95/46/EC 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
- **EC**: European Commission
- **ECHR**: European Convention on Human Rights
- **ECJ**: European Court of Justice
- **EEA**: European Economic Area
- **e-Privacy Directive**: Directive 2002/58/EC concerning the processing of privacy in the electronic communications sector
- **EU**: European Union
- **GDPR**: General Data Protection Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- **ICO**: The Information Commissioner
- **ISPs**: Internet Service Providers
- **MNO**s: Mobile Network Operators
- **OECD**: Organization for Economic Cooperation and Development
- **SNS**: Social Networking Sites
- **UDHR**: Universal Declaration of Human Rights

1. INTRODUCTION

Data protection is a system that seeks to protect the privacy and personal information of individuals by introducing certain principles. As being a regulatory protection regime, it governs the time and the way of collecting and processing personal data legitimately. Its regulatory protection involves all kinds of personal data, which includes both general and highly confidential and sensitive personal data [1]. Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive-DPD) is the main legal instrument which came into force in 1998 in order to harmonise the data protection laws within the European Union (EU) and introduce certain rules to protect the fundamental rights and freedoms including privacy with respect to the processing of personal data across the EU[2].

Along with the rapid growth of the Internet, the digitised data has started to flow faster, cheaper and easier. Simultaneously, this development creates the risk of invasion of the individuals' privacy and right to data protection. Given that it has become a daily routine for millions of people to connect to the Internet for several reasons, huge amount of personal data is disclosed and processed in the online environment, especially in the cases where prior registration is necessary in order to access to the websites[3]. As it is explained in depth below, it is a fact that the DPD has established a system of international standard of data protection rules. Nevertheless, when the DPD was first drafted, the Internet was still in its infancy and did not challenge data protection rules with its rapid growth[4]. Therefore, the implementation of the DPD and the key principles of data processing that make it lawful have started to be contested by the Internet[5].

On the other hand, in January 2012, the European Commission (EC) proposed a new Regulation on the protection of individuals with regard to the processing of personal data and on the free

---

[1] Paul Lambert, *A User's Guide to Data Protection*, Bloomsbury, 2013, p.3
[2] Peter Carey, *Data Protection: A Practical Guide to UK and EU Law*, Oxford University Press, 2nd Ed., 2004, p.6-7
[3] Emmanuel Szafran, Tanguy Van Overstraeten, *Data protection and privacy on the Internet: technical considerations and European legal framework*, 2001, *CTLR*, 56, p.1
[4] Rebecca Wong, *Social Networking: Anybody is a Data Controller!*, Nottingham Trent University - Nottingham Law School, Academic Legal Studies, 21 September 2008, p.2
[5] Colette Cuijpers, Nadezhda Purtova, Eleni Kosta, *Data Protection Reform and the Internet: the draft Data Protection Regulation*, Tilburg Law School Legal Studies Research Paper Series No. 03/2014, p.1

movement of such data (General Data Protection Regulation-GDPR). Although there are several reasons triggering this alteration process, the most important driving force for the purpose of this study is the fact that the current EU data protection rules need to be modernized in order to fit them to the digital age[6].

In the light of these above-mentioned facts, the goal of this study is to examine to what extent EU data protection rules are adequate to provide essential rules to cope with the requirements of the Internet. In order to develop an account, there are certain questions that need to be asked, which can be summarized as *"What has changed since the Internet?, What are the problems posed by the Internet in terms of EU data protection rules?, Are the current EU rules sufficient enough to cope with the risks arose from the Internet?, Or are they too protective than they should be?, How does the European Court of Justice (ECJ) apply these rules in the Internet cases?"*. Before attempting the answers, it is necessary to highlight briefly the aims of the data protection law and the EU rules in this regard. Within this context, second chapter seeks to briefly identify the general overview of data protection law, the matter of how the EU regulates this area of law and the alteration process of the EU rules. This chapter also attempts to answer the question of "What has changed since the Internet?".

When data protection rules are considered from the point view of the Internet, there are several significant subjects challenged by the Internet and its methods enabling processing personal data much more easier than it was before. Within this scope, third chapter of this study seeks to map out these significant issues and explain how the Internet has affected them. Additionally, certain leading cases are examined where it is relevant in order to view their explicit implications and how the ECJ approaches to the Internet cases. Finally in the last chapter, some concluding remarks are made in order to decide whether the EU data protection rules are adequate to provide essential rules to cope with the Internet and some suggestions are given.

[6] The Commission's factsheet on "Why do we need an EU data protection reform", http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf, 2011, (Accessed on 10 July 2014)

2. THE IMPACT OF THE INTERNET ON DATA PROTECTION

2.1. General overview of data protection law

Personal data, which is usually the main subject of data protection, can be defined as information regarding to identification of individuals (physical/natural persons) and collective bodies[7]. It should be mentioned from the outset that the objective of data protection law is not about protecting individuals against data processing. In other words, it is impossible to claim that data protection law bans every data processing actions. Its main aim is to provide a regulatory framework for preventing unlawful collection, storage and dissemination of the data. In order to actualize that aim, it focuses on the activities of the processors and regulates their accountability[8]. Therefore, data protection law provides a balance between the benefits and the negative effects of data processing through its procedural and substantive rules[9]. It is also worth noting that the roots of data protection law are relied on the idea that democratic societies should not depend on surveillance, profiling, social sorting, classification and discrimination. Data protection is regarded as a wide personality right aiming to realize individuals' social identity as citizens and consumers[10].

Another important point that has to be discussed is the relationship between 'privacy' and 'data protection'. Even though traditionally, the protection of personal privacy has been regarded as the main objective of data protection laws, according to the EU law, they are two different fundamental rights that complement each other[11]. The word "privacy" is regarded as a physical space around an individual that comprises various rights, including right to make free decisions without outside interference, right to be free from invasive police searches or from wiretapping. As it is a very subjective term whose meaning varies depending on the time and place, it seems almost impossible to make a list of rights that take place under the scope of privacy.

---

[7] Lee A. Bygrave, *Data Protection Law, Approaching Its Rationale, Logic and Limits*, Walters Kluwer Law & Business, 2002, p.2

[8] Maurizio Borghi, Federico Ferretti, Stavroula Karapapa, *Online data processing consent under EU law: a theoretical framework and empirical evidence from the UK,* International Journal of Law and Information Technology, Vol. 21, No:2, 2013, p.116

[9] *Supra* n.5, p.1

[10] *Supra* n.8, p.118

[11] *Supra* n.8, p.114

Nevertheless, "data protection" is a more accurate term than the "privacy" which is designed to regulate the conditions of collection, storage, use and transferring of personal data. Its classic definition is given by Westin, which reads as follows:

> "*the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others*"[12].

The methods used by the states in the 1940s and 1950s to collect and process the personal data were bureaucratic methods which were not supported by digital machines, such as monitoring of internal passports and human surveillance. As it was highly costly to gather, store and process the analogue data, data was protecting inherently. Therefore, it was not necessary to adopt data protection rules at that time[13]. However, a realization emerged in terms of privacy in the era of World War II, Nazism and the rise of Stalinism when widespread automated data processing was becoming common. Since the late 1960s, modern digital computer systems that provide data to be stored and held for unlimited periods provoked the rise to prominence of data protection law. These systems introduced undesirable possibilities enabling reusing the data for different purposes from their original collection purposes. This is because data protection law aims to combat these results by its instructions ordering certain limitations on the period of storage and the purpose of data collection. Subsequent to that fear regarding to individual privacy, in 1970, the world's first data protection law on a local basis was adopted in Hesse, in Germany[14]. This law, which also substantially influenced the world's first national data protection law, Swedish Personal Data Act of 1973, is accepted to be the framework of European data protection laws[15].

2.2. European data protection law

In consequence of the threat felt because of the development of the computer systems, a need for a coordinated legislative reaction that would safeguard citizens' personal information from

---

[12] Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Cornell University Press, 1992, p.13-14
[13] Andrew Murray, *Information Technology Law*, 2nd Ed., Oxford University Press, 2013, p.488
[14] Lilian Edwards, *Privacy and Data Protection Online: The Laws Don't Work?*, Law and the Internet, Edited by Lilian Edwards, Charlotte Waelde, 3nd Ed., Hart Publishing, 2009, p.447-449
[15] *Supra* n.13, p.489

abuses occurred. In this context, several steps were taken in order to satisfy that need[16]. Universal Declaration of Human Rights (UDHR) of 1948 is the first international legal instrument that provides a legal protection for individual's private sphere against invasion from others[17]. The UDHR also had a positive impact on the development of further human rights instruments in the EU. Subsequently in 1950, European Convention on Human Rights (ECHR) was adopted by the Council of Europe, which entered into force in 1953. Under the Article 8 of the ECHR, the right to respect for private and family life, home and correspondence is guaranteed[18]. Despite the fact that protection of personal data is not explicitly mentioned in the ECHR, the case law of the European Court of Human Rights demonstrates that Article 8 also comprises the right to data protection[19]. It can also be inferred from the case law that in addition to the obligation of refraining from actions that could interfere the right, Article 8 also orders the states to actively secure effective respect for private and family life in certain circumstances[20].

On the other hand, there are two significant legal instruments underlying EU data protection framework, namely the Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which was proposed and enacted by Council of Europe and the non-binding 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[21]. Although these two instruments introduced certain rules and the principles in order to provide legitimate personal data processing and emphasized the need to shift from national protection to international protection once again, they are not self-executing and therefore, the purpose to establish a uniform system of data protection laws across Europe could not be realized[22].

---

[16] Donald C. Dowling, Jr., *International Data Protection and Privacy Law*, White & Case, August 2009, p.4
[17] Article 12 of the UDHR, http://www.un.org/en/documents/udhr/index.shtml#a12, (Accessed on 6 July 2014)
[18] Article 8 of the ECHR, http://www.echr.coe.int/Documents/Convention_ENG.pdf, (Accessed on 6 July 2014)
[19] FRA, *Data Protection in the European Union: the role of National Data Protection Authorities*, European Union Agency for Fundamental Rights, 2010, p.11
[20] Council of Europe, European Union Agency for Fundamental Rights, *Handbook on European Data Protection Law*, 2014, p.15, http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf, (Accessed on 6 July 2014)
[21] Kristina Irion, Giacomo Luchetta, *Online Personal Data Processing and EU Data Protection Reform*, Report of the CEPS Digital Forum, Center for European Policy Studies, Brussels, April 2013, p.14
[22] *Supra* n.16, p.4-5

With regards to the EU law, the right to data protection is primarily protected as a fundamental right in the Article 8 of the EU Charter of Fundamental Rights, which recognizes the right as separately distinct from the right to respect of private and family life[23]. Given that according to the Article 6(1) of the Treaty on European Union, the EU Charter of Fundamental Rights has '*the same legal values as the Treaties*', this provision is very significant in terms of protection of the right[24].

The major instrument in this respect is the DPD, which was enacted to prevent the potential obstacles to the free movement of the information across the EU[25]. The main aim of the Directive is to safeguard the right to data protection if there is a situation of processing personal data wholly or partly by automatic means or that data is involved in a manual system. Article 3(2) lays down two situations where the DPD does not apply. Firstly, the activities falling outside the scope of the EU law are excluded from the implementation area of the Directive. Within this context, defence, public safety, state security and the state activities in criminal law are left out of the scope. Secondly, processing of personal data by a natural person in the course of a purely personal or household activity is excluded from the scope[26].

Another significant feature of the DPD is its purpose to tie two conflicting goals together, namely protecting personal data and facilitating free trade within the EU[27]. On the other hand, Article 6 of the DPD introduces eight fundamental data protection principles that Member States are obliged to respect. According to that provision, personal data must be;

"(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

---

[23] EU Charter of Fundamental Rights, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF, (Accessed on 9 July 2014)
[24] *Supra* n.19, p.14
[25] *Supra* n.2, p.6-7
[26] Article 3(2) of the DPD
[27] Michael D. Birnhack, *The EU Data Protection Directive: An engine of a global regime*, Computer Law & Security Report 24, 2008, p.512

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.[28]"

Moreover, legitimate processing conditions (Article 7), the rights of data subjects, security requirements, fair collection and processing rules and restrictions of trans-border data flows or transfers of personal data and sensitive personal data norms are provided under the DPD[29]. It is also worth noting that not only written communications, but also electronic, oral and Internet communications are included in the scope of the DPD[30].

'Personal data' and the 'data subject's consent' are the key concepts of the DPD, which has to be highlighted since they specify the application of the Directive[31]. Firstly, 'personal data' is significant in that it defines whether data protection rules are needed and accordingly triggers the implementation of the obligations[32]. It is described in Article 2 in a way to include *any information relating to an identified or identifiable natural person ('data subject')*, which is a very broad definition excluding only truly depersonalised data. As an illustration, personal data may involve the individual's email address, IP number, information obtained by cookies[33].

As was stated before, there are two categories of personal data, respectively general and sensitive personal data, which are vital for the organizations and individuals while conducting their data processing activities and determining their obligations. The first category, aka general personal

[28] Article 6 of the DPD
[29] *Supra* n.1, p.45
[30] *Supra* n.16, p.4
[31] *Supra* n.21, p.14
[32] *Supra* n.21, p.41
[33] *Supra* n.3, p.5

data, comprises all personal data, if not specified otherwise[34]. On the other hand, sensitive personal data and its coverage are indicated in the Article 8. According to the provision, data relating to racial, ethnic origin, political opinions, religious, philosophical beliefs, trade union membership, health or sex life is in the scope of sensitive personal data and Member States are not allowed to enable processing of such data. More precisely, sensitive personal data is structured as a subset of personal data that needs to be protected distinctively against abusive processing[35].

On the other side, 'data subject's consent' is defined under the Article 2 as "*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*." The DPD stipulates the 'consent' as a general ground for lawful data processing. It is one of the threshold conditions in order to realize the first principle, namely fairly and lawfully data processing[36].

Another important section of the DPD is Chapter IV, which regulates the transferring of personal data to third countries. Pursuant to those provisions, transferring of personal data to third countries can take place if the concerned third party provides adequate level of protection[37]. Nevertheless, certain exceptions are also stipulated, for instance in the cases where data subject's consent is received or the transfer is essential for public interests[38].

As being a currently leading harmonized instrument in the field of data protection, the DPD is binding for 27 Member States of the EU and 3 members of the European Economic Area (EEA), namely Iceland, Lichtenstein and Norway. Its scope concentrates on the European market via certain extra-territorial mechanisms[39]. However, it is not the only legal text that regulates data protection issues across the EU. There are other certain directives that supplement the DPD either on a sector-specific basis or on the other basis.

---

[34] *Supra* n.1, p.36
[35] *Supra* n.14, p.459
[36] *Supra* n.8, p.110-111
[37] Article 25 of the DPD
[38] *Supra* n.2, p.8
[39] *Supra* n.27, p.512

Directive 2002/58/EC concerning the processing of privacy in the electronic communications sector (the e-Privacy Directive) is one of them. For the purposes of this study, there is no need to discuss the Directive in detail. It suffices to state that the Directive aims to harmonize "*the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community*"[40].

On the other hand, another significant legal text in which data protection issues are regulated is the Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (Data Retention Directive). A fundamental change regarding to data protection and the Internet was brought in the field of Internet Service Providers (ISPs). As from 2001, some laws mandating ISPs to retain communications data about their customers and online actions have been adopted by the states. The Anti-Terrorism, Crime and Security Act of the UK, dated 2001, was one of them which was requiring the ISPs to store customer information. These requirements arising from separate laws were widened across the EU by the Data Retention Directive, which was a result of the political climate affected by Madrid and London bombings of 2004 and 2005[41].

Data Retention Directive introduces a requirement for the providers of publicly available electronic communications services and of public communications networks, which also includes EU based ISPs, to retain traffic and location data for the period of not less than six months and not more than two years from the date of the communication[42]. The Directive indicates the purpose of this retention as investigations, detections and prosecutions of serious crimes[43]. However, its impact on the rights to privacy and data protection guaranteed by the Charter of Fundamental Rights of the European Union had been criticized in several national constitutional

[40] Article 1(1) of the e-Privacy Directive
[41] Ian Brown, *Communications Data Retention in an Evolving Internet*, International Journal of Law and Information Technology, Vol:19, No:2, Oxford University Press 2010, 17 November 2010, p. 95-96
[42] Article 5 and 6 of the e-Privacy Directive
[43] Article 1 of the e-Privacy Directive

court judgments on the ground that there is a probability of misusing of such data[44]. And finally, as a result of the requests from the High Courts of Ireland and Austria to examine the validity of the Directive in terms of two fundamental rights, namely the right to respect for private life and the right to the protection of personal data, the ECJ declared the Directive to be invalid by its judgment dated 8 April 2014 [45]. Significant notes made by the Court can be summarized as follows:

- On the ground that the Directive is ordering the retention of such data, it restricts the fundamental rights to respect for private life and to the protection of personal data.
- The Directive does not make any limitation, differentiation or exception in terms of individuals, means of electronic communication and traffic data.
- The Directive is found insufficient to introduce any objective criterion that would ensure justification when the competent national authorities use the data for the purposes of prevention, detection or criminal prosecutions, which is determined as a contradiction of the principle of proportionality.
- Additionally, the Directive is found insufficient to provide adequate safeguards for the efficient protection of the data against any unlawful use and access.
- The ECJ also criticizes the data retention period imposed by the Directive without making any clarification with regard to the categories of data.
- The ECJ assesses the impact of the provision that enables the retention and use of data without setting any condition for subject's knowledge in the people's mind and states that it is "*likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance*".
- Lastly, the ECJ emphasizes the fact that the Directive does not contain any provision that requires the data be retained within the EU[46].

---

[44] Lukas Feiler, *The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection*, European Journal of Law and Technology, Volume 1, No:3, 2010, p.1

[45] Annulment judgment of the Court regarding Directive 2006/24/EC, dated 8 April 2014, http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN, (Accessed on 6 July 2014)

[46] Press Release regarding the annulment of the Directive 2006/24/EC, Court of Justice of the European Union, No: 54/14, Luxembourg, 8 April 2014, http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf, (Accessed on 6 July 2014)

In light of the grounds relied by the ECJ, it can be inferred that the Court found in the first place that the Directive violated the rights to privacy and data protection. Because of that, the main analysis made by the ECJ is about the justification of such violation. In this sense, amongst the justification conditions, namely public interest, essence of the right and principle of proportionality, proportionality of the interference was the key issue of the Court's ruling[47].

In view of the fact that Article 16 (former Article 286 of the EC Treaty) of the Treaty on the Functioning of the European Union lays down the rules on the protection of the individuals with regard to data processing by the EU institutions and Member States, protection of personal data is a "treaty-given right". Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000, which aims to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data by the EU institutions and bodies, was enacted by relying on the former Article 286 of the EC Treaty[48]. Another significant feature of the Regulation is its role on establishing the European Data Protection Supervisor (EDPS). As an independent supervisory authority, the EDPS audits the personal data processing activities of the EU administrations, gives its comments on the policies and legislations, and deals with the complaints that it receives. It also works in cooperation with other Data Protection Authorities. Article 29 Working Party (A29WP), which is set up in accordance with the Article 29 of the DPD, is the central platform for the cooperation of the EDPS with national supervisory authorities[49].

Eventually, it is worth noting that although data protection is a European innovation in law, it has gained a broad acceptance from all over the world. It can be inferred from the reviews made by the EC that the DPD has affected many countries' legal systems[50].

---

[47] Steve Peers, *The data retention judgment: The CJEU prohibits mass surveillance*, EU Law Analysis, 8 April 2014

[48] Article 1(1) of the Regulation, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:en:PDF, (Accessed on 9 July 2014)

[49] *Supra* n.19, p.15

[50] Jan Philipp Albrecht, *Uniform Protection By The UE – The EU Data Protection Regulation Salvages Informational Self-determination*, Edited by Hielke Hijmans and Herke Kranenborg, Data Protection Anno 2014: How to Restore Trust?, Intersentia, 2014, p.119

2.3. What has changed since the Internet?

As already mentioned, data protection law seeks to balance the risks and gains of personal data processing through its substantive principles and procedural rules. Nevertheless, principles of data protection and the EU legislation on that regard are increasingly challenged by the technological reality. Computing technology and the Internet have developed rapidly since the 1960s and have affected the world in various aspects. The researches reveal that in the EU, 63% of adults and in the US, more than 80% of them use the Internet[51]. More than a billion people around the world use Facebook. Almost all the products of Apple are Internet based and in fact they are regarded as "Internet". Google, as a search engine, ranks among the world's three biggest corporations[52]. These are only few examples amongst the others showing the current situation of the Internet.

Despite the fact that data protection is not a new concept, its importance and the need to improve adequate legislation for the individuals have been understood better in the digital age. As a general rule, principles of data protection are relied on individual autonomy and their ability to control. However, as a result of the technological progress, certain institutions can easily collect, collate, manipulate and use the data[53]. It has become a necessary precondition to submit personal data in order to benefit from online services or facilities. And maybe more importantly, business models of several websites are based on processing of these data for commercial purposes. As was explained earlier, pursuant to the EU data protection law, it is lawful to process data, as long as there are legal grounds for legitimizing the processing. Nevertheless, online environment challenges the key requirements of data processing that make it lawful [54]. Consequently, data breaches have started to occur frequently, which has increased certain concerns related to data protection and privacy[55].

---

[51] Douwe Korff, *The Use of the Internet & Related Services, Private Life & Data Protection: Trends & Technologies, Threats & Implications,* Council of Europe, T-PD(2013)07, 31 March 2013, p.3
[52] Paul Bernal, *Internet Privacy Rights-Rights to Protect Autonomy*, Cambridge University Press, 2014, p.1
[53] Andrew Johnson, *Data protection and E-commerce; The case for new law, in the information age*, 16th BILETA Annual Conference, University of Edinburgh, Scotland, April 9th - 10th, 2001, p.1
[54] *Supra* n.8, p.109
[55] *Supra* n.52, p.1

The online environment has a wide scope, which includes variety of actors and lack of reverence for territorial boundaries. This is not a surprise while taking into account the Internet that contains different web sites established in separate Member States and third party states. On the one hand, with its intercontinental feature, the Internet requires a necessity for data protection to store the trust and confidence. However on the other hand, it creates a challenge to existing European data protection law, since it becomes complicated to implement practiced principles to the complex structure of the Internet[56].

Korff makes the important point that due to the fact that Internet usage has been moving away from fixed to personal and mobile devices, the relationship between the users and the providers has been changing. In other words, the Internet is no longer an area that we can access only through computers. The author makes a useful comparison between traditional ISPs and Mobile Network Operators (MNOs) and states that MNOs providing mobile Internet are disposed to exercise more control both over their services' and networks and are much more interested in the preferences and actions of their subscribers than the traditional ISPs[57]. This approach is insightful in that this change might be regarded as one of the reasons raising the rate of the data breaches.

As already mentioned, according to the basic principle of data protection, legitimate collection of personal information can only be done for specific, explicit and legitimate purposes[58]. Nevertheless, in the area of Internet, "purpose limitation" principle becomes an exception instead of a rule, since all the information created and circulated in the Internet is digital, which threatens the requirements of that principle[59]. There are certain technical means that constitutes a potential invasion of individuals' privacy. These methods being used to collect and process personal information can be illustrated as hardware and software identification, surfing on the Web, cookies, sniffers, e-commerce and chat groups[60]. Additionally, cloud computing, profiling, data mining, nanotechnology, e-commerce and advertising, social networking, e-government, health and social care systems are the other technological key changes that have serious implications

[56] European Commission, *On-line Services and Data Protection and Privacy*, Volume II, Annex to the Annual Report 1998 (XV D/5047/98) of the Working Party established by Article 29 of Directive 95/46/EC, 1998, p.1-3
[57] *Supra* n.51, p.3
[58] Article 6(1)(b) of the DPD
[59] *Supra* n.56, p.5
[60] *Supra* n.3, p.1-3

over data protection and challenge the European data protection law. The concept of "identifiability" on which the data protection law and the concept of personal data are largely relied has been damaged by these changes, since the Internet is about to put an end to the anonymity[61].

In the light of these explanations, it is undoubtedly true that there is an explicit technological change from the date 1990 when the EC first proposed the Data Protection Directive[62]. The Internet provides numerous methods making it possible to analyze, use, gather, store and transfer personal data. It should also be noted that as the Internet becomes indispensable in people's life, it is becoming almost impossible to separate online and offline data. By virtue of the methods created by the Internet, data becomes reachable ubiquitously and flows freely across national boundaries, which causes certain problems in terms of auditing of such data from a data privacy point of view[63]. This is also why data protection has started to occupy a significant place[64].

2.4. The new General Data Protection Regulation

As explained before, the DPD is the main legislative measure that regulates the data protection activities across the EU. Undoubtedly, it has positive impacts on providing an awareness of data protection issues and introducing a uniform legal framework in order to ensure lawful personal data processing. On the other hand, its implementation and certain features have often been criticized, since there is a substantial dissatisfaction. Within this context, there are several concerns whether DPD is sufficient to make data protection principles a reality, and whether its instruments are effective enough to provide free flow of personal data in the EU[65]. Maybe more importantly, the view of the EC is that the current EU data protection legislation is inadequate to ensure the fundamental right to data protection, which is guaranteed by the Article 8 of the Charter of Fundamental Rights. Additionally, there are other specific driving forces behind the

---

[61] *Supra* n.51, p.30
[62] Ian Brown, *Comparative Study on Different Approaches to New Privacy Challenges, in particular in the Light of Technological Developments*, Working Paper No:1, The challenges to European data protection laws and principles, European Commission, Directorate General Justice, Freedom and Security, 20 January 2010, p. 1
[63] *Supra* n.14, p.449
[64] *Supra* n.5, p.1
[65] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri, *Review of the European Data Protection Directive*, RAND Europe, Technical Report, 2009, p.38

need for reform. One of them is about non-EU companies such as Tumblr. The new rules are become applicable for them, when they target EU citizens. The other targets in this respect are the companies established in the EU, such as Google and Facebook (whose European headquarters are in Dublin). It is aimed to enable them to apply to the local supervisory authorities in order to be audited, so that they will have the opportunity to make sure whether they are in compliance with EU law[66]. In its factsheet that clarifies the reasons why reform is needed, the Commission remarks that,

"*The current rules also need to be **modernised** - they were introduced when the Internet was still in its infancy. **Rapid technological developments** and globalisation have brought new challenges for data protection. With **social networking sites, cloud computing**, location-based services and smart cards, we leave digital traces with every move we make. In this "brave new data world" we need a robust set of rules. The EU's data protection reform will make sure our rules are future-proof and fit for the digital age.*[67]"

These concerns, among others, have resulted in an assessment process of the adequacy of the DPD in late 2000s. The main alteration process of the DPD began in 2009. In late 2010, Communication, which was a result of a public consultation was released by the Commission. Afterwards, the views of the major participants, namely the Council, the Parliament, the EDPS and the A29WP, were published[68]. At the end, in January 2012, the EC proposed a new Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data[69].

There are several key changes introduced by the GDPR, which can be summarized as follows:

---

[66] *Supra* n.13, p.517-518

[67] *Supra* n.6, p.1

[68] Paul De Hert, Vagelis Papakonstantinou, *The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals*, Computer Law & Security Review, Volume 28, Issue 2, April 2012, pp. 130–142, p.131

[69] The GDPR, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf, (Accessed on 10 July 2014)

- A new provision that ensures "right to be forgotten" is introduced, which is structured to help people better deal with data protection risks that are possible in the online environment. Such a right will provide the opportunity to delete the data, if people no longer want their data to be processed and there are no legitimate reasons for retaining it.
- A new requirement is created in order to protect the consumers, which requires that the consent has to be given explicitly.
- With another provision, the scope of the implementation of the EU rules are extended to the companies which are not established in the EU, if they offer goods or services in the EU or monitor the online behavior of citizens.
- The right of data portability and easier access are provided for the people to reach their data.
- With regard to the people and companies processing personal data, their responsibilities and accountabilities are increased[70].

It is also worth noting that the main reform about the new proposal is its way of drafting. Given that it is proposed as a Regulation instead of a Directive, it will be binding for all Member States. Moreover, due to the same reason, it will prevent different interpretations of the legislation between the States[71]. On the other hand, even tough more than two years passed since the first proposal, it still remains unclear when the final draft will be adopted. In this period, almost 4000 modifications were tabled[72]. One of the most recent developments in this respect was on 12 March 2014 when the European Parliament voted overwhelmingly in favour of new data protection laws. Thus, it is revealed that the Parliament supports the architecture and the fundamental principles of the proposal[73]. Subsequently, on 28 May 2014, the Council that consists of Member States' justice ministers has agreed its position on the Chapter V of the proposal dealing with the new EU rules, which will apply to non-EU companies[74]. However, there are still certain steps that have to be taken for the Regulation to become a law.

---

[70] Supra n.6, p.2
[71] *Supra* n.13, p.518
[72] *Supra* n.5, p.2
[73] Press Release regarding the Progress on EU data protection reform now irreversible following European Parliament vote, European Commission, MEMO/14/186, 12/03/2014, http://europa.eu/rapid/press-release_MEMO-14-186_en.htm, (Accessed on 10 July 2014)
[74] Steve Peers, *Reforming EU data protection law: the Council takes its first baby steps*, EU Law Analysis, 13 June 2014

3. SPECIFIC ISSUES RELATED TO THE INTERNET

As was mentioned earlier, the DPD is regarded as the most important legislative measure in terms of data protection issues, which harmonizes the data protection laws within the EU. During this process since its first adoption, most of the Member States have succeeded to implement the DPD by preparing new laws or modifying their data protection laws. However, as a result of the irrepressible development of the Internet, the application of the DPD and the interpretation of its certain concepts have started to be questioned before the national courts, beginning with the landmark case of *Lindqvist*[75]. Within this context, in this chapter, the most important subjects of the data protection law that seem to have been affected by the Internet will be examined.

Before attempting to highlight these sub-sections below, it will be useful to give brief summary of the landmark cases that have far-reaching implications in terms of application of the DPD in the Internet cases and will be reviewed in detail in the relevant sections. The first case is *Lindqvist*, which especially revealed the problem of publishing sensitive data on the Internet. In this case, Mrs. Lindqvist, who was working as a catechist in the parish of Alseda (Sweden), set up a home page on the Internet in her personal computer, in order to enable parishioners to obtain information. These pages included information about her self, her husband, and her 18 colleagues in the parish, including names, jobs, hobbies, family circumstances, telephone numbers and other information. In addition to that information, she also included information about one of her colleagues who had injured her foot and was on half time on medical grounds. It should be mentioned that concerned information were obtained and published without colleagues' consent and she also did not notify Swedish data protection authority on that regard. Once she received certain complaints from her colleagues, she removed the pages[76]. However, she was convicted and fined by the Swedish Courts. Subsequently, she appealed the decision on the claim that there was no violation of the DPD. Thereupon, Swedish Courts referred certain questions to the ECJ

[75] Rebecca Wong, *The Data Protection Directive 95/46/ EC: Idealisms and realisms*, International Review of Law, Computers & Technology, 26:2-3, 229-244, 2012, p.229-230

[76] CJEU, C-101/01, *Bodil Lindqvist*, 6 November 2003, para. 12-14, http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=9409, (Accessed on 17 July 2014)

and the ECJ ruled that although she was not guilty of a transfer, processing of such personal data constituted data processing and concerned data were in the scope of sensitive personal data[77].

Another significant case in this regard is *Google Spain*, in which search engines' situation under the DPD was examined for the first time. In this case, Mr. Costeja González (data subject) realized that his name was seen as a debtor on Google references because of a debt occurred 11 years ago. Thereupon, he firstly requested from the Spanish newspaper, which published his social security debt in the electronic version of the newspaper, to remove that financial history. After the newspaper rejected his request, he contacted to Google Spain and asked stop referencing the link in its search results. At the same time, he complained to Spain's Data Protection Authority. By its decision, the Authority rejected it against newspaper, however required Google Spain and Google Inc. to remove certain links. Nevertheless, Google Spain and Google Inc. brought separate actions against that decision and subsequently, the national court of Spain referred several questions to the ECJ for a preliminary ruling. The concerned questions and ruling of the ECJ will be reviewed in detail below[78].

3.1. Territorial application of the DPD in the Internet

Determining applicable law in data protection cases is important in that it defines the territorial lines in which concerned applicable law would be valid and taken into account. Nevertheless, since increased globalization and new technologies allow the companies to operate in different jurisdictions, determining applicable law has started to become complicated[79]. In this respect, Article 4 of the DPD is the provision that governs the rules determining the application of the DPD. According to the provision, the primary factor among others that enables the application is the processing of personal data carried out "*in the context of the activities of an establishment of the controller on the territory of the Member State*"[80].

---

[77] Briana N. Godbey, *Data Protection in the European Union:Current Status and Future Implications*, I/S: A Journal of Law and Policy, Vol.2:3, 2006, p.809-811

[78] CJEU, C-131/12, *Google Spain,* 13 May 2014, para.14-20, http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=243691, (Accessed on 22 July 2014)

[79] The A29WP Opinion 8/2010 on applicable law, 0836-02/10/EN WP 179, 16 December 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf, (Accessed on 11 July 2014), p.6

[80] Article 4(1) of the DPD

Within this context, the A29WP introduced an opinion in 2010 trying to clarify certain questions related to applicable law and websites. As is explained by the A29WP, "*location of the establishment*[81] *of the controller*", "*public international law"* and "*location of the means or equipment being used when the controller is established outside the EEA"* are the main measures that specify the applicable law[82]. Article 4(1)(c) stipulates the third measure, in which data controllers that are not established within the EU, but use the equipment for the processing of personal data within the EU are included to the scope. However, the implementation of this provision raises several questions in terms of data processing performed on the Internet. As an illustration, one might question whether Article 4(1)(c) can apply to non-EU data controllers, who collect personal data through the computers of the users in the case of cookies, on the ground that it amounts to the use of equipment on a national territory[83]. In respect thereof, the A29WP emphasizes the possibility that cookies or Javascript banners might trigger the application of Article 4(1)(c)[84].

Although Article 4(1)(c) is targeting the controllers that are not established within the EU in order to prevent them to abrogate their responsibilities by moving outside the EU, it does not seem sufficient, especially when taking into account the nature of the Internet. As a matter of fact, the GDPR desists from the test of "use of equipment" and extends the scope of the implementation of the EU rules to the companies, which are not established in the EU, but offer goods or services in the EU or monitor the online behavior of citizens[85]. In other words, EU rules would apply regardless of foothold, legal or physical presence in the EU, which would bring general application of the EU rules. When it comes to "general application", it is also worth mentioning that in the *Lindqvist* case, the ECJ stated that every personal data uploaded onto an Internet page would not trigger the application of the Article 25, since there are still technical actions that should be performed to access to that websites. Therefore, the ECJ warned that special regime of the DPD should not become a general application with regard to the operations

[81] The term of "establishment" is not defined under the DPD. Nevertheless, in the Recital 19, it is stated that the term can be regarded as effective and real exercise of the activity through stable arrangements. Rebecca Wong, *Data Protection in the Online Age*, Sheffield University, 2006, p. 105
[82] *Supra* n.79, p.8
[83] Supra n.74
[84] *Supra* n.79, p.21
[85] Article 3 of the GDPR

on the Internet[86].

Given that A29WP warns about the undesirable consequences of the "use of equipment" test, such as a possible universal application of EU law[87], this problem is far more likely to arise under the GDPR which provides a more broad application[88]. Moreover, Schwartz argues that in order to limit the scope of the application of the GDPR, the meaning of "monitoring" should be explained restrictively so as to include only the situations where individual's privacy is at risk[89].

In relation to the territorial application of the DPD rules, it should also be noted that the meaning of the concepts "establishment" and "use of equipment" were examined under the case *Google Spain*. In this regard, Google's arguments relied on the claim that Google Spain was a commercial representative acting as only for its advertising purposes, which is something separate from its search engine services[90]. Nevertheless, in the Advocate General's opinion submitted before the ECJ's judgment, the A29WP's opinion on data protection issues relating to search engines was recalled. As in the opinion of the Working Party, which examines search engines' business model, based on advertising, Advocate General considered the business model of search engine service providers that relies on keyword advertising. Subsequently, he made the important point that since the entity had to be presence on different countries in order to realize keyword advertising, Google had found subsidiaries in certain Member States, which could be accepted as "establishments" under Article 4(1)(a)[91].

As a matter of fact, the ECJ ruled in the same direction as Advocate General's opinion by stating that,

---

[86] *Lindqvist*, para. 69
[87] *Supra* n.79, p.31
[88] Omer Tene, Christopher Wolf, *Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation*, Future of Privacy Forum, January 2013, p.2-3
[89] *Supra* n.5, p.3
[90] Press Release, No 77/13 Luxembourg, Advocate General's Opinion in Case C-131/12, 25 June 2013, p.1, http://curia.europa.eu/jcms/upload/docs/application/pdf/2013-06/cp130077en.pdf, (Accessed on 13 July 2014)
[91] Opinion of Advocate General Jääskinen in the Case C-131/12 *Google Spain SL Google Inc. v Agencia Española de Protección de Datos (AEPD) Mario Costeja González*, para.64, http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=38131, (Accessed on 13 July 2014)

"*Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State.*[92]"

In its judgment, the ECJ emphasized the fact that since the advertising activities rendered by Google Spain constituted economic profit to the search engine and the search engine, at the same time, enabled those activities to be performed, the activities of the both Google Spain and Google Inc. were inextricably linked[93].

It is undoubtedly true that this judgment will have certain consequences and will raise several questions in practice. As an illustration, one might question whether a search engine, which does not have an "establishment" within the EU, can be regarded as being in the territorial scope of the DPD. Nevertheless, implications of the judgment suggests that if a non-EU company has a subsidiary which performs advertising activities regarding its Internet services in an EU Member State, this company would be considered to fall into the scope of the DPD[94].

Lastly, given that the GDPR still includes the "establishment" clause, this clause would be interpreted the same way as the ECJ interpreted in *Google Spain,* at least in the cases where there is a link between subsidiary's activity and the non-EU parent company's business model. Nevertheless, in view of the fact that it is impossible to find any clarification in the case law with regard to the meaning of "use of equipment", it is not easy to evaluate what kind of results will arise because of the removal of this clause in the GDPR in practice[95].

[92] *Google Spain,* para.60
[93] *Google Spain,* para.56
[94] Steve Peers, *Further Comments on Google Spain*, University of Essex, Human Rights Centre, Blogs, 13 May 2014
[95] *Supra* n.74

3.2. Data processing in the Internet

The DPD defines the concept "processing" very widely in a way to include "*collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction*"[96]. It is a significant provision for the processing performed in the Internet. In order to adequately assess how processing is assessed in the Internet cases, it is pertinent to analyze *Lindqvist*. In this case, one of the questions referred to the ECJ was whether an Internet page on which Mrs. Lindqvist posted her colleagues' pictures and information established processing of personal data wholly or partly by automatic means within the meaning of Article 3(1) of the DPD. With respect to this question, although Mrs. Lindqvist claimed that only mentioning by name of a person or of personal data in a document would not be acknowledged as automatic processing of data[97], the ECJ found that this activity constituted processing of personal data according to the Article 3(1)[98].

Another issue evaluated by the ECJ was whether Mrs. Lindqvist's home page could possibly fall under the exceptions in Article 3(2) of the DPD. According to the provision, the DPD shall not apply to two situations where processing of personal data is conducted *"in the course of an activity which falls outside the scope of Community law"* and "*by a natural person in the course of a purely personal or household activity"*. With regard to that question, Mrs. Lindqvist raised the issue of freedom of expression and argued that establishing an Internet page as a non-profit-making activity was not subject to Community law. Even though the Court accepted Mrs. Lindqvist's actions as "*charitable and religious*", it adopted a literal approach in the interpretation of first indent of Article 3(2)[99] and decided that first exception could not apply to charitable and religious activities[100]. With respect to the second exception, the ECJ found that Mrs. Lindqvist's activity also could not be placed under the scope of personal or household

[96] Article 2 of the DPD
[97] *Lindqvist*, para.20
[98] *Lindqvist*, para.27
[99] Flora Garcia, *Bodil Lindqvist: A Swedish Churchgoer's Violation of the European Union's Data Protection Directive Should Be a Warning to U.S. Legislators,* Fordham Intellectual Property, Media and Entertainment Law Journal, Volume 15, Issue 4, Article 10, Volume XV, Book 4, 2005, p.1223
[100] *Lindqvist*, para.45

activity, on the ground that publication on the Internet made data accessible to an indefinite number of people[101].

It is also worth noting that despite the fact that Mrs. Lindqvist raised the issue of freedom of expression, the Court rejected this argument by stating that a defense of personal use and the freedom of expression could not cause disregarding the right of privacy. To put it another way, the Court emphasized that even though we were in the age of communication technologies, Mrs. Lindqvist's colleagues still had an expectation of privacy and the right to be consulted, and therefore the public interest in preserving privacy should be protected[102].

This decision and the reasoning of the ECJ are described as "high water mark" of data protection maximalism and have been much criticized, as it triggers the concerns on whether setting up a family photo page, Facebook or MySpace accounts displaying friend's information and photos would be under the scope of processing on the Internet[103]. Given that the reason relied by the ECJ was that data made accessible to an indefinite number of people, one might question whether an Internet page, which is restricted or limited to a number of people, could be regarded as an exception. In this sense, Wong maintains that the meaning of the Article 3(2) can be extended[104]. Similarly, Edwards argues cogently that if password protection or friends-locked are used by the individuals on their website, then the data would not be publicly accessible and therefore these websites would constitute "*purely personal or household activity*"[105]. All the same, even if a website, which is only accessible by family members will constitute an exception, it still remains unclear where the line is drawn for individuals whose web pages can only be accessed by his family members and friends. The reason is that according to the implications obtained from *Lindqvist* ruling, the burden would be on the individual to demonstrate that the Webpage was established for private purposes, which would be a very difficult thing to achieve[106].

---

[101] *Lindqvist*, para.47
[102] Rebecca Wong, Joseph Savirimuthu, *All or Nothing: This is the Question? The Application of Article 3(2) Data Protection Directive 95/46/EC to the Internet*, The John Marshall Journal of Information Technology & Privacy Law, Volume 25, Issue 2, Spring 2008, p.245
[103] *Supra* n.14, p.461
[104] *Supra* n.81, p. 104
[105] *Supra* n.14, p.461
[106] *Supra* n.102, p.246

Lastly, it is argued that these implications might restrict enjoying the right to freedom of expression and penalize individuals for their "harmless activity", which would not be expected to harm data subjects. Hence, it is suggested that this issue needs to be discussed in detail by data protection authorities, legislators and the EC[107].

3.3. Personal data in the Internet

The definitions of the "personal data" and "sensitive personal data" have been stated before and therefore will not be dealt here. However, it is necessary to emphasize again that the notion of "personal data" is extremely broad, which covers both the information relating to "**identified**" or "**identifiable**" natural person. It still remains debated among the data protection practitioners and policymakers whether to embrace a broad or limited approach of "personal data" [108]. It is significant to mention that the debate particularly centers on the question which data could be accepted as personal data relating to an **"identifiable"** natural person. On the question of "identifiable", Recital 26 states that "*to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person*" [109]. Subsequently, it is explicitly mentioned that "*the principles of protection shall not apply to data rendered **anonymous** in such a way that the data subject is no longer identifiable*"[110].

Additionally, a clarification on determining personal data was provided by the A29WP, which recommended four elements, namely "relate", "content", "purpose" and "result" that are necessary for personal data. Pursuant to this definition, data can be personal data, if it relates to an individual, if its content covers information about a particular person, if it is used or likely to be used for the purpose to identify a particular person or if its result is likely to have an impact on a particular person[111]. Despite the fact that A29WP suggests a more relative interpretation, four-criterion method is criticized for being still very broad, as it is not taken into account the

---

[107] Supra n.81, p.104
[108] *Supra* n.75, p.231
[109] *Supra* n.81, p.39
[110] Recital 26 of the DPD
[111] The A29WP Opinion 4/2007 on the concept of personal data, p.10, http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/opinion_04-2007_personal_data_/Opinion_04-2007_personal_data_en.pdf, (Accessed on 15 July 2014)

possibility of privacy risk[112]. Nevertheless, it is a fact that the main issue attached importance by the DPD is the *capability* or *potentiality* of identification. More precisely, actual achievement of identification is not required, which is why data can be accepted as personal data even though the data controller refrains from making a connection between that data and a particular person[113].

3.3.1. Anonymous data

In the light of the explanations, terms and concepts mentioned above, there are certain issues in the context of the Internet that needs to be explained. The first issue is about anonymisation on the Internet, which is significant since it has a role in triggering the application of the DPD. "**Anonymous data**" is defined by the A29WP in a way to include any information of a natural person who cannot be identified by that information[114]. This is why anonymous data does not fall under the scope of the DPD[115]. Therefore, the concern is that anonymisation enables companies to collect data of the individuals without having responsibilities required by the DPD[116]. However, the determination of the issue whether the DPD rules would operate depends on the interpretation of the data protection authorities. In the cases where the authorities adopt a narrow interpretation, then the privacy would only amount to protection of the identity of the data subject. But, in broad interpretations, the privacy would not be limited with the identity and also comprises data subjects' physical, psychological and moral integrity. Therefore, it is argued that broad approach should be adopted in order to extend the meaning of the Recital 26[117].

It should also be noted that although anonymous data is not regarded as personal data because of its characteristic containing no personal identifiers, the act of anonymising is still data processing within the meaning of Article 2(b) of the DPD; therefore, the application of the DPD is possible to that activities[118]. Anonymisation on the Internet was addressed by the A29WP in which in principle it is emphasized that Internet users should be properly identified and all their activities

[112] *Supra* n.65, p.27-28
[113] *Supra* n.7, p.44
[114] *Supra* n.111, p.21
[115] Recital 26 of the DPD
[116] White & Black Corporate & Technology Lawyers, *Anonymising personal data: new EU guidance published,* http://www.wablegal.com/e-bulletins/anonymising-personal-data-new-eu-guidance-published, (Accessed on 16 July 2014)
[117] *Supra* n.81, p.81-82
[118] *Supra* n.81, p.79

in the Internet should be traceable. However, apart from certain exceptions, such as public policy, fight against illegal and harmful content, financial fraud or copyright infringements, the possibility of remaining anonymous on the Internet is acknowledged by the A29WP[119]. Additionally, as a recent development on that regard, A29WP introduced a new Opinion on 10 April 2014 with respect to Anonymisation Techniques. In the new Opinion, Working Party provided three criteria that should be assessed in the each case in order to determine the robustness of each technique of anonymisation. These are;

> *"(a) is it still possible to single out an individual? (b) is it still possible to link records relating to an individual? (c) can information be inferred concerning an individual?[120]"*

3.3.2. Clickstream data

Another issue that needs to be highlighted is whether clickstream data is personal data within the meaning of the DPD. It has to be mentioned from the outset that although it is impossible to find a legal definition of the concept, clickstream data can be defined as data regarding to an activity of a user on the Internet, which contains information about every visited Web site, for instance the time spent by the user on that site and the e-mail addresses that the user sends and receives[121]. Clickstream data is collected from cookie-based technology, which has been used by the websites since mid-1990s. With respect to the question posed before, there are different views on that regard. On the one hand, Reidenberg and Schwartz argue that, *"[for] online services, the determination of whether particular information relates to an 'identifiable person' is unlikely to be straightforward."*. However, the A29WP states that clickstream data usually amount to personal data under the DPD, since it includes certain links that the user follows and logs in the Internet[122]. In fact, in the cases where clickstream data enables the direct or indirect identification

---

[119] The A29WP Recommendation 3/97 on Anonymity on the Internet, 3 December 1997, p.3, 5, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp6_en.pdf, (Accessed on 15 July 2014)

[120] The A29WP Opinion 05/2014 on Anonymisation Techniques, p.3, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf, (Accessed on 16 July 2014)

[121] *Supra* n.81, p.89-90

[122] The A29WP Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware, 23 February 1999, p.4, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp17_en.pdf, (Accessed on 16 July 2014)

of the individual, the DPD rules would apply. In particular, given that the technologies have become so sophisticated, clickstream data can easily identify individuals[123].

3.3.3. IP addresses

Another significant issue in the context of Internet is whether IP addresses can be regarded as personal data under the EU rules. Firstly, it should be noted that IP address is defined as "*a device's (typically a computer's) numerical address as expressed in the format specified in the Internet Protocol*"[124]. There are several guidelines attempting to clarify the notion. For instance, The Information Commissioner (ICO) dealing with the Data Protection Act across the UK has provided particular guidance on this matter, which suggests that an IP address could be regarded as personal data only if it relates to a PC or other device that is used by a single user[125]. On the contrary, there are some other views arguing that IP addresses are personal data, even though the data processor does not have the possibility of linking these IP addresses to a given individual[126]. Moreover, A29WP has introduced several opinions in which IP addresses have been touched. For instance, in its working document dated 2000, it is stressed that IP addresses are personal data by considering that Internet access providers, ISPs and managers of local area networks have the opportunity to identify Internet users to whom they have attributed IP addresses[127].

Bygrave in this regard makes another important explanation in which he refers to the Article 2(a) of the DPD that indicates "identification number" as personal data. The author argues cogently that since the DPD does not restrict identification number only to natural person, a computer's IP address could be acknowledged as identification number[128].

---

[123] Daniel B. Garrie, Rebecca Wong, *Demystifying Clickstream data: A European and U.S. Perspective*, Emory International Law Review, Vol.20, 2006, p.580

[124] Eneken Tikk, *IP Addresses Subject to Personal Data Regulation*, p.27

[125] ICO, Personal Information Online – Code of Practice, p.9, http://ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/personal_information_online_cop.pdf, (Accessed on 14 July 2014)

[126] *Supra* n.65, p.27

[127] The A29WP Working Document on Privacy on the Internet - An integrated EU Approach to On-line Data Protection, 21 November 2000, p.21, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp37en.pdf, (Accessed on 16 July 2014)

[128] *Supra* n.7, p.316

There are two ways with regard to the assignment of the IP addresses. If they are assigned temporarily, it means that they change every time when a user logs in (dynamic). In the other way, they are assigned permanently to a user's computer (static), which is usually acknowledged as personal data. Nevertheless, it is impossible to argue that IP addresses always relate to a specific individual. The reason is that in some circumstances more than one person might share the same IP address on one computer, especially in the cases where a home computer is in question. In such a case, if it is possible to link that IP address to an individual through passwords operated by the ISP, there is a chance that IP address would form personal data. However, in the other possibility where passwords are not included, it would seem unlikely to be considered as personal data[129].

Lastly, it is also significant to mention that with the development of mobile telecommunications that enables devices with an IP address to be used by another entity, determining the scope of personal data has become difficult. Moreover, this difficulty is expected to increase while IPv6 is taken into account, as IP addresses will be allocated to objects, such as cars and home appliances[130].

3.3.4. Sensitive data

As was mentioned earlier, DPD regulates sensitive personal data as a subset of personal data, which needs to be protected distinctively against abusive processing. It is worth noting from the outset that the DPD is not the only legal measurement stipulating special categories of personal data. Apart from the DPD, Council of Europe Convention No. 108 also requires high level of protection for sensitive personal data, which states that sensitive data *"may not be processed automatically unless domestic law provides appropriate safeguards".* However, in comparison with the Convention, the DPD seems more restrictive[131]. According to the Article 8(2), processing of sensitive personal data is only allowed if,

---

[129] *Supra* n.81, p.96-97
[130] *Supra* n.65, p.27
[131] Julie Ringelheim, *Processing Data on Racial or Ethnic Origin for Antidiscrimination Policies: How to Reconcile the Promotion of Equality with the Right to Privacy?,* Center for Human Rights and Global Justice Working Papers, Number 13, 2006, NYU School of Law, p.28

- explicit consent of the data subject is obtained; or,
- this processing is necessary,
  - because of the obligations of the data controller by virtue of law in the field of employment law; or,
  - in order to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or
- processing is conducted by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or,
- the data is made public clearly by the data subject or processing is necessary for the establishment, exercise or defence of legal claims[132].

As can be inferred from the Article 8(1), the scope of the sensitive data is extremely broad, which has both positive and negative outcomes in terms of data protection. On the one hand, it is an affirmative provision that requires assessing certain data whether they "reveal" sensitive characteristics of individuals. Thus, for such data, which do not appear immediately, they will be treated as sensitive. But on the other hand, only considering revealing certain characteristics might result in assuming enormous quantity of data as sensitive data, although they were not processed for the purpose of revealing sensitive data. Therefore, the provision is criticized for its danger that could make the purpose of the sensitive data meaningless in practice[133].

Another questionable part of the provision is its implementation in the Internet cases. In this sense, there are certain concerns focusing on whether the enumeration in the Article 8(1) is exhaustive and whether such a categorization falls short of the dangers generated in recent online

[132] Article 8(2) of the DPD

[133] Jean-Marc Dinant, Cécile de Terwangne, Jean-Philippe Moiny, *Report on the lacunae of the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No 108) resulting from technological developments,* The Bureau of the Consultative Committee of the Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, T-PD-BUR(2010)09 EN, p.31-32.

age. These concerns has began to rise especially after the judgment of the case *Lindqvist,* in which the ECJ was referred the question whether information naming a colleague who injured her foot and was on half-time on medical grounds would amount to sensitive data under the scope of Article 8(1)[134]. In reply to the question, the ECJ ruled that *"(i)n the light of the purpose of the directive, the expression data concerning health used in Article 8(1) thereof must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the health of an individual."*[135].

On the basis of the above reasoning, Wong argues cogently that current approach of the Court seems impractical and debatably antiquated. The author also claims that Article 8 providing a blanket provision cannot make it possible to consider whether data is published intentionally or unwittingly, which would lead to many Internet users in breach of Article 8(1) of the DPD[136]. Also, Garcia makes a useful comparison between *Lindqvist* decision and similar US cases in which potential damage to the financial security of those individuals are involved, and in the end the author acknowledges the former as abusive and draconian[137].

Besides, as can be inferred from the reasoning, the EJC adopted a wide interpretation method while applying Article 8(1). Therefore, it is pertinent to argue that interpretation constitutes a great impact in practice. Within this regard, instead of adopting a literal approach, there are several methods recommended by the scholars and relevant organisations. The first one is "**purpose-based**" approach that is originally suggested by Council of Europe Report entitled "Informational self-determination in the Internet era". The Report recommends that literal approach, which is based on the definitions required by data protection laws, should be abandoned in favour of a purpose-based approach. The main advantage of the purpose-based approach is that since it attempts to find out whether processing intended to reveal sensitive data,

[134] With regard to questions referred to the ECJ, it is also worth noting that Swedish authorities did not request an explanation on whether naming peoples' name as Church volunteers reveal "religious or philosophical beliefs" of data subjects. *Supra* n.99, p.1224-1225
[135] *Lindqvist*, para.50
[136] *Supra* n.81, p.112-113
[137] *Supra* n.99, p.1233

it targets the persons who deliberately reveal of such data. Thus, such an approach could also have an impact on decreasing the number of trivial cases[138].

The other alternative method is "**contextualised-approach**", which suggests evaluating the data by considering the background of the context that determines the usage of data. In this sense, there are several issues that could be taken into account in order to determine the degree of sensitivity, such as the conditions of the processing, its possible results, specific interests of the controller, possible receivers of the data[139]. It is a flexible method as it is based on the idea that sensitivity should not be limited to the categories stipulated under the Article 8(1). This is also why; this approach could easily apply in the Internet cases, since data does not have to fall into the scope of Article 8(1)[140].

In light of the explanations with regard to interpretation approaches, it can be argued that in *Lindqvist*, the ECJ adopted a literal approach and therefore considered the actual definition of the term, which is believed to be a danger for Internet cases. For instance, Wong makes the important point that broad application of Article 8(1) constitutes risk, since anything published on the Internet would be included directly or indirectly to the scope. In fact, Wong questioned the main reasons why the original legislators of the DPD preferred such a category[141]. Furthermore, Edwards argues convincingly that given that there is a possibility to extend the scope of the Article 8(1) to every picture published on the Internet, a more flexible classification is needed[142]. All these critics have one thing in common that they recommend an amendment of the provision. Nevertheless, contrary to the expectations, GDPR maintains both the distinction between personal and sensitive personal data, and broad categorization of sensitive data under the Article 9[143]. It is also worth noting that in its paper analyzing GDPR, ICO indicated its reservations about proposed sensitive data provision that again categorises data as sensitive by default. The ICO emphasized that the new provision's wording should be narrower in order to ensure that data is

[138] Rebecca Wong, *Data Protection Online: Alternative Approaches to Sensitive Data?*, Journal of International Commercial Law and Technology Vol. 2, Issue 1, 2007, p.10-12
[139] Spiros Simitis, *Revisiting Sensitive Data*, Review of the answers to the Questionnaire of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1999, p.5
[140] *Supra* n.81, p.115-116
[141] *Supra* n.138, p.9, 11
[142] *Supra* n.14, p.460
[143] Article 9 of the GDPR

accepted as sensitive data only if the purpose of the processing is to reveal individuals' sensitive data[144]. Needless to say, if the GDPR will finalize as it stands, the concerns seem to continue, particularly the ones emerged after *Lindqvist* decision, which is about shortsighted EU rules and heavy-handed centralized legislation would damage the businesses that are supposed to be encouraged[145].

3.4. Transferring data to third countries

Trans border data flows, which can be described as transferring of personal data outside of the EU/EEA, is a significant issue that needs to be highlighted within the context of the Internet. It has to be mentioned from the outset that transferring personal data is restricted by the EU data protection legislation, unless certain conditions are met. There are several underlying reasons behind the fact why data controllers/processors prefer to transfer personal data outside the EU. These reasons can be summarized as reducing costs, outsourcing to countries outside of the EU, rapid growth of the Internet that provide data flow and store easily[146].

EU data protection rules are the most advanced and restrictive rules in terms of transferring data. The specific objective of the legislators is to protect the rights of the EU citizens, if data is transferred to the third countries where adequate data protection regime is not provided[147]. Therefore, Article 25(1) of the DPD stipulates that "*transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer*" may take place only if the third country in question ensures an adequate level of protection[148]. Article 25(6) of the DPD empowered the EC to produce a list of countries ensuring such adequate protection. So far, the EC declared certain countries as safe countries, such as Andorra, Faeroe Islands, Argentina, Israel, Canada, Switzerland, Guernsey, Isle of Man and Jersey[149]. It is also worth mentioning that a special agreement was negotiated with the US that enables personal data to be

[144] Sensitivity of personal data should be determined by processing purpose and context not through categorisation, says ICO, http://www.out-law.com/articles/2013/february/sensitivity-of-personal-data-should-be-determined-by-processing-purpose-and-context-not-through-categorisation-says-ico/, (Accessed on 18 July 2014)
[145] *Supra* n.99, p.1239
[146] *Supra* n.1, p.395
[147] *Supra* n.2, p.103
[148] Article 25(1) of the DPD
[149] W Kuan Hon, Christopher Millard, *Data Export in Cloud Computing: How can Personal Data be Transferred outside the EEA?, The Cloud of Unknowing,* Part 4, Queen Mary University of London, 2012, p.5

transferred to companies in the US if they agree to fulfill the requirements of the "Safe Harbour"[150] privacy principles[151].

Although the DPD does not define "transfer", it can be deduced from the throughout the body of the DPD that the concept is used to describe moving data to third countries[152]. According to the A29WP, transferring data outside the EU also includes the transfer of personal data to a server outside the EU[153]. In fact, the meaning of "transfer" within the context of the Internet was examined under the case *Lindqvist*, in which the ECJ was asked to determine "*whether there is any transfer [of data] to a third country within the meaning of Article 25*" in the case where Mrs. Lindqvist uploaded personal data onto an internet page which made those data accessible to people in the third countries and "*whether the reply to that question would be the same if no one from the third country had in fact accessed the data or if the server where the page was stored was physically in a third country*.[154]".

On the question of transferring, the Commission and the Swedish Government had the opinion that loading personal data onto an Internet page established transfer of data to third countries on the ground that nationals of them can access the pages, even if no one from these countries in fact accessed to such data[155]. Nevertheless, the ECJ held against. One of the grounds relied by the ECJ was the fact that deciding otherwise would lead to impracticable and unrealistic results[156]. The ECJ emphasized that if every personal data uploaded onto an Internet page would be treated as transferring to third countries, then the special regime of the DPD would become general application[157]. The ECJ also stressed that as Mrs. Lindqvist's Internet pages did not send the data automatically to people, Internet users had to connect to the Internet and conduct some other actions in order to access that data[158]. Then, it was concluded that since "*there is no 'transfer [of*

---

[150] The Commission Decision on this regard dated 26 July 2000, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:EN:PDF, (Accessed on 22 July 2014)
[151] Richard Jones, Dalal Tahri, *An overview of EU data protection rules on use of data collected online*, Computer law & security review, 27, 2011, pp. 630-636, p.635
[152] *Supra* n.99, p.1225
[153] The A29WP Opinion 2/2010 on online behavioural advertising, 22 June 2010, p.21, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf, (Accessed on 21 July 2014)
[154] *Lindqvist*, para.52
[155] *Lindqvist*, para.53
[156] Supra n.149, p.9
[157] *Lindqvist*, para.69
[158] *Lindqvist*, para.60

data] to a third country' within the meaning of Article 25 of Directive 95/46" where the site was hosted by an ISP located within the EU, it was not necessary to examine whether third country citizens accessed to those pages or whether the server of that hosting service was physically in a third country[159].

Another significant case in this regard is a very recent example: *Europe v. Facebook* case. In this case, Mr. Schrems applied to the Irish Data Protection Commissioner (Commissioner) to investigate Facebook's international headquarters in Ireland. His complaint was focused on the Facebook's activity to transfer his personal data as a Facebook user to the US. He cited Snowden disclosures[160] as evidence and claimed that given that those disclosures proved that US data protection system was not sufficient, the Commissioner must suspend transferring of personal data from Facebook Ireland to its parent company in the US. Nevertheless, the Commissioner rejected the request on the ground that it was bound by the terms of the Commission's decision dated July 2000, which presents Safe Harbour system. Then, Mr. Schrems challenged this decision before the Irish High Court, which referred some questions to the ECJ in its ruling dated 18 June 2014[161]. The questions can be summarized as whether the Commissioner is bound by the Commission's decision (regarding Safe Harbour) and whether the Commissioner can conduct its own examination on that matter[162].

In his claims, Mr. Schrems relied on the *Digital Rights* judgment of the ECJ in which Data Retention Directive was announced invalid and the ECJ found that mass surveillance violated the fundamental right to privacy. Based upon this judgment, he argued that "*It is obvious that Facebook Ireland can't be allowed to aid the US government when violating our rights, if not even our own governments would be allowed to take such measures*.[163]". Irish High Court also

---

[159] *Lindqvist*, para.70

[160] After Mr. Snowden disclosed thousands of highly classified US National Security Agency (NSA) files, it was revealed that NSA was realizing interception and surveillance of Internet and telecommunications systems, not only limited in the US. Additionally, this incident has triggered the concerns whether the US data protection regime provides an adequate protection. Judgment of Mr. Justice Hogan in the case *Europe v. Facebook*, 18 June 2014, para.1, http://courts.ie/Judgments.nsf/09859e7a3f34669680256ef3004a27de/481f4670d038f43380257cfb004bb125?OpenDocument, (Accessed on 22 July 2014)

[161] Judgment, para.2-3

[162] Judgment, para.71

[163] Irish High Court: European Court of Justice will decide over Facebook/PRISM, p.1, http://www.europe-v-facebook.org/PRISM_pa_en.pdf, (Accessed on 22 July 2014)

paid great attention to the Digital Rights judgment and it can be inferred from its judgment that it believes that as the US data protection regime cannot provide adequate protection to the EU citizens, it is a violation of EU data protection law. Nevertheless, Peers questioned this analysis by presenting several issues that were not taken into account by the national court. According to Peers, the Court should have considered whether subject matter of the dispute was under the scope of the DPD or derogations stipulated in the DPD. He also emphasizes the fact that even it is doubtful whether external transfer would apply to that case, the Court did not asses this issue. At this point, he recalls the *Google Spain* judgment, in which it was ruled that standard rules should apply to Google that has establishment in Spain. Therefore, he states that contrary to the national court's assumption that external transfer rules apply; this issue should be evaluated by the ECJ[164].

Yet, *Europe v. Facebook* case is pending before the ECJ. Nevertheless, there is no doubt that the judgment of the ECJ would have a great impact on both Facebook users in the EU and on other companies, such as Yahoo and Apple that have the same company structure in Ireland like Facebook[165]. With regard to transferring data on the Internet, it is a fact that *Lindqvist* decision, in which the ECJ ruled that uploading a personal data to the Internet should not be regarded as transferring personal data, is a significant precedent. However, it is suggested that more research should be conducted in order to determine whether a distinction between passive and active transfers should be made under the Article 25[166].

3.5. Search engines and their role as data controller

As indicated in the previous chapters, the Internet has growth rapidly over the last two decades. Within this period, search engines have become an indispensable tool enabling access to requested information on the Internet. Although they are one of the most important developments in the Internet, search engines have raised several problems arising because of the tension

[164] Steve Peers, *Europe v Facebook: the beginning of the end for NSA spying on EU citizens?* , EU Law Analysis, 18 June 2014
[165] *Supra* n.163, p.2
[166] *Supra* n.81, p.111

between data protection and the nature of the Internet[167]. The reason behind these problems is the easiness of obtaining any information on any topic. Therefore, people have become concerned about the information that search engines might refer to[168]. In this sense, the place of search engines and their role within the meaning of DPD will be examined in this sub-section.

There are some technical operations that search engines use to provide information to their users. For instance, the operations currently used by Google are: 1) crawling, 2) indexing, 3) algorithmic analysis, 4) retrieval, 5) ranking and 6) fighting spam[169]. These concepts are significant, since according to the A29WP, when they are '*crawling, analyzing and indexing the World Wide Web and other sources they make searchable and thereby easily accessible through these services*', search engine providers process personal data in the context of Article 2(b) of the DPD[170].

"Processing" was one of the questions referred to the ECJ in the *Google Spain* case. The argument of the Google Spain focused on "intention". They claimed that activity of search engines couldn't be regarded as processing personal data due to the fact that concerned data appear on third parties' websites, and Google crawls and indexes these websites without deliberate intent to process personal data[171]. However, the ECJ ruled against by stating that even if data originated from third parties, this did not change the result. The Court referred to the case *Satamedia,* in which the ECJ decided that it was processing personal data, although material had already been published in unaltered form in the media[172]. Additionally, Article 2(b) does not set forth any necessity that data should be altered[173].

Having established that the activities conducted by the search engines fall within the scope of processing personal data, the next issue to consider is whether search engine providers can be

---

[167] *Supra* 52, p.117, 124
[168] B. Van Alsenoy, A. Kuczerawy, J. Ausloos, ICRI Working Paper Series, *Search engines after Google Spain: internet@liberty or privacy@peril?,* 6 September 2013, p.7
[169] *Supra* n.168, p.11
[170] The A29WP, Opinion 1/2008 on data protection issues related to search engines', WP 148, 4 April 2008, p. 13, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf, (Accessed on 23 July 2014)
[171] *Supra* n.168, p.12
[172] *Supra* n.94, p.1
[173] Steve Peers, *The CJEU's Google Spain judgment: failing to balance privacy and freedom of expression*, EU Law Analysis,13 May 2014, p.2

regarded as data controller. "Data controller" is defined under the DPD as a *"natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data"*[174]. According to the A29WP, a search engine provider should be treated as controller where it processes user data involving IP addresses and/or persistent cookies covering a unique identifier, as it has an effective role on determining the purposes and means of the processing[175]. At this point, one might question who would be responsible for data processing in the cases where large multinational search engine providers are concerned and several branches and some third parties are involved in the processing. With regard to this question, Burgstaller refers to the definition under the DPD, which describes the controller as a person "*which alone or jointly with others determines the purposes and means of the processing of personal data*". Therefore, the author states that a search engine provider is the data controller of such data, regardless of the question about the jurisdiction[176].

In fact, from a literal approach, it is worth observing that given that they determine the purposes and means of the processing activities, and automated processing of personal data is occurred during these activities, search engines meet the conditions stipulated under the Article 2(d)[177]. However, to what extent is it legitimate to adopt a literal approach? There are certain views regarding these concerns arguing that "intent" and "awareness" should be taken into account while determining data controller. This was the position of the Advocate General in *Google Spain*. He was in the view that Google Spain was not a data controller. He adopted a maximalist approach and continued that in order to be a controller, data controllers should be aware of a defined category of information and processing and there should be some degree of intent about concerned data[178]. According to him, Google Spain could not meet this condition.

Nevertheless, In ICRI's Working Paper, Google's own words that describes their purpose '*to*

[174] Article 2(d) of the DPD
[175] *Supra* n.170, p.9
[176] Peter Burgstaller, *Search engines and the extra-territorial dimension of the EC data protection law*, Computer and Telecommunications Law Review, 2009, (Westlaw sources), p.6. This is also the same result reached by the A29WP in its opinion 1/2008.
[177] *Supra* n.168, p.16
[178] Lorna Woods, *Google v Spain, Background to the forthcoming decision of the European Court of Justice*, 12 May 2014

organize the world's information make it universally accessible and usable' are recalled. They interpret these words as evidence that arguing Google not to 'purposefully' process personal data seems difficult[179]. As a matter of fact, contrary to the Advocate General's opinion, the ECJ held that Google Spain was a data controller within the meaning of the DPD. The Court emphasized that it was possible to distinguish the activities, namely original publication of the data and its processing by a search engine. According to the Court, among these two different activities, search engines' activities are significant since they play a decisive role in the dissemination of data. Lastly, the ECJ stated that even if publishers of websites choose the option to publish certain information only on their site, this would not change the position of the search engines, since Article 2(d) of the DPD provided that determination might be made jointly with others[180]. Despite the fact that search engines does not play a role on controlling the original publication of the data, they undoubtedly play an additional role on processing that arise from the use of a search engine. Therefore, it is pertinent to argue that decision of the ECJ seems convincing[181].

Another significant issue assessed by the ECJ in *Google Spain* was whether Google Spain was obliged to remove the requested links from the results list although concerned name or information was not erased from those web pages before, and publication of the name or information on those pages was lawful[182]. One of the rights given to the data subjects by the DPD is the right to request rectification, erasure or blocking of data under certain circumstances[183]. Examining the question, the ECJ mainly focused on the fact that the activities carried out by the search engines had great impact on the rights to privacy, especially while considering that search engines enabled any internet users to attain search results probably containing information regarding the people's private life. As a result, the ECJ stated that it was impossible to justify these activities of the search engine by merely relying on the economic interest[184]. Additionally, the ECJ took into account the possibilities that would prevent effective and complete protection, where the original publisher of the information was not subject to EU legislation and where the

[179] *Supra* n.168, p.16
[180] *Google Spain*, para.35-40
[181] *Supra* n.94, p.2
[182] *Google Spain*, para.62
[183] Article 12(b) of the DPD
[184] *Google Spain*, para.80-81

publisher was carrying out 'solely for journalistic purposes' and thus fall into the scope of the derogations from the requirements[185]. In light of these reasons, the ECJ ruled that "*the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.*" This decision regarding erasure of the information can be justified by Google Spain's responsibilities as data controller. However, it should be noted that in this case, the concerned personal data is not inaccurate or libellous, but only embarrassing[186].

Lastly, it should be mentioned that Peers criticizes *Google Spain* decision in terms of balancing of interests between data controller, data subject and other Internet users. In this criticism, *ASNEF* judgment of the ECJ, in which the Court decided that Spanish law could not balance the rights of data subjects and direct marketing companies and company's right to carry on a business was not taken into account sufficiently, is recalled. By relying on this judgment, Peers maintains that in *Google Spain*, despite the fact that Google's advertising activity is related to direct marketing, the Court did not even mention Google's right to carry on a business in its judgment. Peers also makes the important point that even though the rights of third parties *to whom the data are disclosed* should be considered while balancing of interests in accordance with the Article 7(f), the Court did not give enough weight to the interests of other Internet users[187].

3.6. Right to be forgotten and to erasure in the Internet

In the era of Internet, it has become almost impossible for the people to abandon their history. Mailboxes, search engines and social networks are some of the tools enabling information not to

[185] *Google Spain*, para.84-85
[186] *Supra* n.94, p.3
[187] *Supra* n.173, p.4

lost and remain arguably forever[188]. As this issue is related to the Internet, it is significant to examine the right to be forgotten and erasure with its features. In this sense, this sub-section looks at how the right to be forgotten is set out in the GDPR and will conclude with a look at how this issue was questioned in *Google Spain*.

Right to be forgotten has been a debated issue recently, since Commissioner Viviane Reding announced the intention that this right would be included in the GDPR[189]. It is defined by the EC as a "*right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes.*"[190]. It has to be mentioned from the outset that the DPD and existing consent regime seem insufficient to provide such a right[191]. Although in its 'Opinion on Consent', the A29WP suggests that individuals should be given the opportunity to withdraw their consent, this will only have an impact on the future processing, therefore will not be effective for the data processed before[192].

Article 17 of the GDPR is the provision introducing the right to be forgotten and to erasure. Although in the Commission's proposal, the title of the article was **'Right to be forgotten and to erasure'**, in the Parliament voting the title was changed to **'Right to erasure'**. According to the provision voted by the Parliament, this right can be applied where,

"(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;

(c) the data subject objects to the processing of personal data pursuant to Article 19;

---

[188] Hans Graux, Jef Ausloos, Peggy Valcke, *The Right to be Forgotten in the Internet Era*, ICRI Working Paper Series, ICRI Working Paper, 11/2012, 12 November 2012, p.3

[189] Paul Bernal, *The EU, the US and Right to be Forgotten*, Reloading Data Protection, Edited by Serge Gutwirth, Ronald Leenes, Paul De Hert, Springer, 2014, p.61

[190] European Commission, COM (2010) 609 final: *A comprehensive approach on personal data protection in the European Union*, 4.11.2010, p.8, http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf, (Accessed on 31 July 2014)

[191] Axel Spies, *Reform of the EU Data Protection Directive: 'Right to Be Forgotten'—What Should Be Forgotten and How?*, Privacy and Security Law Report, ISSN 1538-3423, 2011, p.1

[192] *Supra* n.188, p.11

(ca) a court or regulatory authority based in the Union has ruled as final and absolute that the data concerned must be erased;

(d) the data has been unlawfully processed.[193]"

It is argued that the GDPR is only extending the existing data protection principles stipulated under the Article 12(b) by providing a new idea that already given consent may be withdrawn[194]. With this provision, the right to erasure, which has been already provided under the Article 12(b) of the DPD, was aimed to be clarified and strengthened in order to give individuals more control over their data[195]. This is also emphasized by the EC in its Factsheet on *Google Spain* ruling. According to the EC, since the DPD has already included principles forming basis for right to be forgotten, it will be wrong to claim that the Article 17 of the GDPR is presenting fundamentally new provisions[196].

Another change stipulated by the GDPR is that it requires the data controller who made the personal data public to take all the steps, including to inform third parties processing such data about the data subject's request to erase any links to, or copies or replications of that personal data[197].

Right to be forgotten is believed to contain two distinct features at the same time. On the one side, in the cases where processing or retention of the data is no longer authorized or are illegal for other reasons, this right enables individuals to have their data deleted. On the other side, it provides a different kind of right ensuring that *"outdated negative information should not be used against people."*. It can be argued that the first leg of the right has been applied in accordance with the Article 12(b) in the form of the right to erasure and blocking of data and with the Article 14(a) in the form of right to object[198].

---

[193] Press Release regarding the Progress on EU data protection reform now irreversible following European Parliament vote, European Commission, MEMO/14/186, 12/03/2014, http://europa.eu/rapid/press-release_MEMO-14-186_en.htm, (Accessed on 10 July 2014)
[194] *Supra* n.189, p.62
[195] *Supra* n.168, p.42
[196] European Commission, *Factsheet on the "Right to be Forgotten" ruling*, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf, p.2,
[197] *Supra* n.5, p.10
[198] *Supra* n.5, p.10

Nevertheless, this right raises several doubts as to whether it will be effective and technically feasible, particularly in this era of Big Data. Needless to say, enforcement of the provision is a very significant issue, since it determines the viability of the right. The particular question raised in this regard is whether data subjects can enjoy the right to be forgotten in the cases where data controllers are social networks, video-hosting platforms or search engines operating independently from the content providers. With regard to intermediaries, Rosen makes the important point that there is a threat that right to be forgotten will result in value judgments made by the intermediaries in order to decide whether to delete the requested data[199]. The reason behind this concern is that data controllers should not be in a position to balance right to privacy and right to freedom of expression that are conflicting which may possibly cause "*in a chilling effect on use of the Internet*"[200].

There is no doubt that, the requirement for the data controllers to "*take all reasonable steps*" is a positive provision attempting to ensure the enforcement of the Article. However, the Article cannot guarantee that all third parties will be informed about the data subject's request or these people will respect the request[201]. Another concern is the possibility that social network sites can be problematic to exercise this right, as in the example of Facebook where it is almost impossible to delete an account[202].

Probably the biggest concern about the implementation of this Article is related to freedom of expression. The main objection made by the freedom of expression advocates is that right to be forgotten will pose a threat to free speech in the Internet which will prevent other people exercising their freedom of expression. This concern is also mentioned by the ICO by stating that a general right to be forgotten should not be provided which would be probably impossible to enforce and have adverse impacts on freedom of expression[203]. However, on the question of freedom of expression, it should be stated that certain exceptions are listed in the third paragraph

---

[199] *Supra* n.168, p.42-43
[200] *Supra* n.21, p.2, 68
[201] *Supra* n.5, p.11
[202] *Supra* n.189, p.64
[203] ICO, *The future of data protection in the EU Briefing from the UK Information Commissioner's office*, September 2011, http://ico.org.uk/~/media/documents/library/Data_Protection/Research_and_reports/ico_stakeholder_briefing_-_the_future_of_dp_in_the_eu.ashx, (Accessed on 3 August 2014)

of Article 17 in order to prevent exercising the right to erasure in the cases where further processing is *"necessary for exercising the right of freedom of expression"*[204].

As was mentioned before, another question referred to the ECJ in *Google Spain* was about right to be forgotten. The National Court asked whether the rights to erasure and blocking of data and the right to object could be interpreted in a broad manner in order to include the data subject's right to be forgotten, even though the information in question has been lawfully published by third parties[205]. Examining the question, the ECJ accepted the fact that data processed lawfully could become incompatible in the course of time and individuals had the right to request from the search engines to remove these links about their data, especially in the cases where processing of these data would be inadequate, irrelevant, excessive or no longer relevant[206]. Moreover, the ECJ stated that processing personal data by the search engines might result in serious interference of right to privacy of the individuals and the economic interest of the search engine does not seem to justify this interference, as it cannot in this particular case. In this sense, it is important to observe that although the Court accepted that in certain circumstances, right to be forgotten can be deduced from the requirements under the DPD stipulating that data should be retained for limited periods, it never mentioned that such a right existed as such[207]. Nevertheless, it was emphasized that since the right to be forgotten is not an absolute right, every case should be assessed in terms of balancing against other fundamental rights in order to determine sensitivity of the data for the data subject's private life and the interest of the other people accessing to that information[208].

On the other hand, according to a new system that has established for the deletion requests, if applicant's request is refused by Google, he/she can apply to Data Protection Commissioner (DPC). However, DPC clarified that they had not yet received any application that rejected by Google. Official figures show that more than 70.000 applications requesting to delete certain links were submitted to the Google[209]. Nevertheless, it is undoubtedly true that the decision of the ECJ in this aspect will have significant implications. First of all, it raises certain questions on

[204] *Supra* n.168, p.43-44
[205] *Google Spain*, para.20
[206] *Google Spain*, para.93
[207] *Supra* n.173, p.3
[208] *Supra* n.196, p.2
[209] Ruadhan Mac Cormaic, *EU data protection authorities to agree approach to 'right to be forgotten' appeals*, 8 July 2014

how to determine the public figure and the time that should be passed for the personal data to be irrelevant[210]. Another aspect of the judgment is its possible impacts on online publishers. It has started to be questioned after the decision whether right to be forgotten will be compatible with journalism and a balance between privacy and freedom of expression can be achieved[211].

3.7. The role of "consent" in the Internet

As indicated in the previous chapters, the DPD acknowledges the consent as a general condition for legitimizing data processing. According to the Article 7 of the DPD, unambiguous consent of the data subject should be obtained for lawful processing. There are also three other requirements referred by the DPD while defining data subject's consent. These requirements are "freely given", "specific" and "informed". Similarly, pursuant to the Article 8 of the Charter of Fundamental Rights of the EU, one can enjoy his right to protection of personal data if consent is given. However, online world raises certain questions as to how unambiguous consent should be given. Because of the rapidly growth technology and its various methods enabling individuals to express their indication of wish, sometimes it might be not clear whether informed and freely consent is obtained[212]. In this sense, this section of the study investigates the consent given in the Internet and its validity under the DPD.

The first thing to note is that there are two different consent types stipulated by the DPD. First one is "unambiguous consent" set forth under the Article 7, which is provided as a condition for lawful processing of personal data. This type of consent requires that there must be no doubt about the intention of the data subject's. In principle, given that non-response or being silence is ambiguous, they do not constitute a valid consent. This is a very common issue on the Internet where websites prefer to use default settings requiring data subjects to change their browser settings or the pre-ticked boxes in order to prevent data processing[213]. On the other hand, the second type is "explicit consent" that is stated by the Article 8 as a condition for processing sensitive personal data. In a comparison between these two types of consent made by the EC, it is

[210] *Supra* n.94, p.4
[211] Roy Greenslade, *Data Protection: What should be public and what should be private*, 1 July 2014
[212] *Supra* n.8, p.110, 111, 118
[213] *Supra* n.151, p.632

specified that "unambiguous consent" needs further clarification and more uniform interpretation than the "explicit consent", in particular in the online practices[214]. At this point, it is worth noting that the GDPR is found to be helpful since it moves away from the distinction between these two types of consent. However, it is criticized for enhancing the consent requirements since the definition of the consent involves explicit consent[215].

What needs to be stressed here is a current phenomenon about opt-in and opt-out boxes, which are frequently used by data controllers while gathering the data in the online environment[216]. On the question of opt-in boxes, in its opinion issued on the application of the e-Privacy Directive, the A29WP acknowledges that data subject might give his consent by ticking of a box[217]. Similarly, in another opinion, the A29WP suggests that data subject can give his explicit and unambiguous consent in the online environment, as in the offline domain. According to the opinion, the difference between these two environments is that the former includes much more risk that necessities special attention[218]. However, when it comes to opt-out boxes that enables data controller to process the data automatically, unless data subject objects, the A29WP finds them not compatible in terms of direct marketing through emails. It is emphasized that *"(I)mplied consent to receive such mails is not compatible with the definition of consent of Directive 95/46/EC…"*[219]. Nevertheless, according to Murray, given that this opinion of the A29WP is about direct marketing through emails and Working Party opinions are advisory, such an opinion does not have a direct impact on the validity of the opt-out boxes[220].

---

[214] Report from the Commission, *First report on the implementation of the Data Protection Directive (95/46/EC)*, Brussels, 15.5.2003 COM(2003) 265 final, p.17, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0265:FIN:EN:PDF, (Accessed on 4 August 2014)

[215] Gabriela Zanfir, *Forgetting About Consent. Why The Focus Should Be On "Suitable Safeguards" in Data Protection Law,* Reloading Data Protection, Edited by Serge Gutwirth, Ronald Leenes, Paul De Hert, Springer, 2014, p.240-241

[216] Supra n.8, p.121

[217] The A29WP, Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC, 11601/EN, WP 90, 27 February 2004, p.5, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp90_en.pdf, (Accessed on 15 August 2014)

[218] The A29WP, Opinion 15/2011 on the definition of consent, 01197/11/EN WP187, 13 July 2011, p.23, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf, (Accessed on 15 August 2014)

[219] *Supra* n.8, p.121

[220] *Supra* n.13, p.505

It is also worth noting that, as in the case *Lindqvist*, the Internet might cause certain difficulties in the cases where Internet users upload other individuals' personal data. Despite the fact that some operators usually require the visitors to obtain consent of their contacts by putting a provision in their terms and conditions, it is impossible to claim that visitors always fulfill these requirements in practice[221]. In this sense, it is suggested by the A29WP that the Social Networking Site providers should offer their users default-setting systems in order to prevent unlawful data processing by the people who are not from the selected contacts and who access to the users' profile[222].

Another significant point made by the A29WP with regard to consent is about 'browse-wrap' consent, which is usually used by the search engines. In this type of consent, it is considered that since de facto contractual relationship has started for the users, they have given their consent to the terms and conditions. However, it is stated by the A29WP that this assumption cannot be accepted, as strict limitation of necessity stipulated under the Article 7(b) of the DPD is not met[223]. There are even further examples in which many Internet providers compel the consent requirements. In these examples, terms and conditions are set in a way to ensure that once a user has signed in to one service of this provider, it is deemed that this user had given his consent to having his data gathered for other services provided by the same provider[224].

3.8. Social networking sites (SNS) and data protection

It is undoubtedly true that SNS are one of the main components of the communication performed in the Internet. Nevertheless, they raise certain concerns on whether effective guarantee of the right to data protection could be achieved[225]. In this context, this sub-section of the study will focus on the problems in applying the DPD rules to the SNS.

The first issue that needs to be highlighted is determining data controller in SNS cases. When the

---

[221] *Supra* n.151, p.632
[222] The A29WP, Opinion 5/2009 on online social networking, 01189/09/EN, WP 163, 12 June 2009, p.7, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf, (Accessed on 6 August 2013)
[223] *Supra* n.170, p.17
[224] *Supra* n.52, p.37
[225] Artemi Rallo, Ricard Martines, *Data Protection, Social Networks and Online Mass Media*, European Data Protection: Coming of Age, Edited by Serge Gutwirth, Ronald Leenes, Paul De Hert, Springer, 2013, p.409-411

definition of the "data controller" stipulated under the DPD is taken into account, there is no doubt that the organisations such as Facebook, MySpace and Twitter are considered as data controller, since they "*determines the purposes and means of the processing of personal data.*" Nevertheless, the definition gives rise to a concern that individuals who post information about their friends as the users of the SNS would also be considered as data controllers, therefore the requirements of the DPD would apply on them, unless the exceptions of the DPD would be applicable[226]. However, this result is criticized for being highly impracticable. As pointed out by the scholars, while certain requirements applied for the data controllers, such as processing the data lawfully and fairly and supplying data subjects certain information, are applicable for the organisations, it seems unrealistic to apply these obligations to the SNS users. Therefore, it is argued cogently that the EU should focus on the remain unanswered questions as to whether it is realistic to consider the SNS users as data controller and whether it is fair for individuals and organisations to have the same obligations as data controllers[227].

With regard to this concern, what needs to be stressed here is that whether the SNS users would benefit from the exemptions stipulated under the DPD. The first exemption to consider is the Article 3(2) of the DPD, which was examined before as household exemption. Although it seems likely to be applied for the individuals who only post photo of their friends, *Lindqvist* judgment supports the opposite view. As was mentioned before, in *Lindqvist*, the ECJ held that posting personal data of friends in a web site that is accessible to anyone was not fall into the scope of the household exemption[228]. It should also be noted that the Opinion of the A29WP is in accordance with the *Lindqvist* judgment. According to the Opinion, in the cases where the SNS users use the platform for advancing commercial, political or charitable goals, it is not possible to benefit from household exemption. Similarly, if the information posted by the individuals could be accessed by a high number of third party contacts, this would be an indication that the exception would not apply[229].

---

[226] *Supra n.4*, p.1
[227] Daniel B. Garrie, Maureen Duffy-Lewis, Rebecca Wong, Richard L. Gillespie, *Data Protection: The Challenges Facing Social Networking*, Brigham Young University International Law and Management Review, Volume 6, Issue 2, Article 6, 2010, p.132-134
[228] *Supra* n.225, p.415-417
[229] *Supra* n.222, p.6

On the question of other exemptions, although the A29WP mainly focuses on the implementation of the private purpose provision to the SNS users, it is stated that exemption for journalistic purposes, artistic or literary expression might also be applied to the SNS users[230]. Nevertheless, given that it is impossible to find any clarification neither in the Opinion of the A29WP nor in the DPD in relation to the application of the other exemptions to the SNS users, it still remains unclear whether the individuals would benefit from them. Wong gives a significant hypothetical example in which a journalist has a Facebook profile. It is likely that journalistic exemption may apply for the references made by the journalist to certain individuals. However, it is undoubtedly true that it would be difficult to determine whether this Facebook profile is used for a journalistic purpose[231].

Another significant problem arising from the SNS is about obtaining consent. As was mentioned earlier, the SNS operators are regarded as data controller. Therefore, they are under the obligation of gaining "consent" (or "explicit consent" in the case of sensitive personal data) of the users in accordance with the DPD. However, it is common in the SNS that, the consent is obtained in the registration step as a privacy policy or terms and conditions by ticking a box without any chance to negotiate. Thus, it is argued that these kinds of consents are unlikely to be accepted as free and informed[232]. In this regard, the only suggestion made by the A29WP is that privacy-friendly default settings should be provided by the SNS operators in order to ensure that users could give their consent freely and specifically to any access by their self-selected contacts[233].

---

[230] *Supra* n.222, p.6
[231] Rebecca Wong, *Social Networking: A Conceptual Analysis of a Data Controller*, Nottingham Trent University, Nottingham Law School, Academic Legal Studies, Communications Law, Vol. 14, No. 5, pp. 142-149, 30 December 2009, p.8
[232] *Supra* n.14, p.479
[233] *Supra* n.222, p.7

4. CONCLUSION

Along with the increasing development of the Internet and SNS, applying the current DPD rules have started to be contested, especially after the judgments of some leading cases that have significant implications in terms of the Internet. As indicated in the previous chapters, Article 4 stipulating the territorial application of the DPD is a problematic provision for online processing, since its complex wording gives rise to some difficulties for the implementation of the Article, as in *Google Spain*. It is a fact that "use of equipment" test brings some advantages, since it aims to prevent non-EU data controllers to circumvent their responsibilities; therefore, it offers a wide data protection for the EU citizens. On the other hand, if it would be applied to the non-EU web servers, which set cookies and are regarded as triggering the application of the Article 4(1)(c) by the A29WP, it would cause a general application of the DPD, which is something that the ECJ avoided in *Lindqvist*. Given that Article 3 of the GDPR provides new provisions that would have more overreaching results than the current rules, these concerns seem to continue.

Lindqvist ruling has significant implications in terms of the interpretation of "processing" and application of the Article 3(2). Considering these implications and concerns with regard to freedom of expression and potential non-proportional decision that might be held in the future, it is pertinent to propose that data protection authorities, legislators and the EC should assess these terms by taking into account the realities of the Internet in order to draw a fair line between protecting right to data protection and other fundamental rights, such as freedom of expression. Otherwise, possible judgments that will be held in the same direction as *Lindqvist*, might have "chilling effect" on the exercising the right to freedom of expression.

Another problematic provision of the DPD is Article 8(1), which can be defined as a blanket provision posing some risks for the Internet users. In fact, the risk is that every Internet user uploading photo or any information of his friends might be accused of being in breach of the Article 8(1), since these information would be regarded as sensitive data, as in *Lindqvist*. Therefore, it can be suggested that the provision should be amended so as to enable the sensitivity not to limited to the categories. Such an amendment would also promote the courts to

assess whether data controller intends to reveal sensitive data of the data subject in each case. Nevertheless, it seems that this categorization remains in the GDPR.

In the digital age, it is necessary to provide certain protections, in view of the fact that the global character of the Internet enables data to flow without frontiers. As was stated before, the DPD presents a restrictive system on this regard. Then, to what extent the DPD is sufficient to provide data transferring rules within the context of Internet? The answer is ambiguous and depends on how the courts approach to the provisions. In *Lindqvist*, even though the DPD does not offer any explicit provision stipulating data transferring issues performed in the Internet, ECJ took a wide approach by ruling that uploading personal data onto a webpage did not amount to transferring personal data, so that the Court avoided holding an impracticable decision. Besides, the future decision of the ECJ in *Europe v. Facebook* case will provide some guidance in this regard.

With the above mentioned considerations related to the right to be forgotten and erasure in mind, it can be argued that the GDPR seems to provide certain benefits by giving individuals stronger data subject rights, particularly in the Internet era. However, the critics made about the proposal have shown that it raises some questions in a number of ways, including enforcement of the Article in the cases where search engines and social networks are concerned. Given that it is important for a provision to be enforceable, legislators should provide necessary conditions for the implementation. Therefore, these concerns need to be addressed and assessed in more detailed in order to find a solution about how data controllers will comply with these requirements. However, despite these concerns and questions raised after the Commission Proposal, the text of the Article 17 was become stronger by the Parliament.

Due to the fact that the Internet enables various ways to process personal data over the Internet, it has become harder for the individuals to give a valid consent for data processing[234]. Although A29WP states that opt-out mechanism is not suitable for obtaining a valid consent within the meaning of the DPD, concerns remain whether ongoing opt-out boxes can be considered as valid. Therefore, it is pertinent to argue that current DPD rules do not seem to provide sufficient provisions to clarify this issue.

[234] *Supra* n.51, p.30

On the question of whether SNS users would be regarded as data controller, it does not seem practicable to apply "strict" and "excessive" DPD rules to the SNS users. Despite the fact that Opinion of the A29WP has provided certain clarification in terms of household exemption, there are still grey areas to what extend journalistic exemption would apply to the users[235]. Therefore, it is necessary to draw a fair line between freedom of expression and right to data protection in order to determine whether users are data controllers in an SNS platform.

To sum up, it is a fact that since the Internet has challenged the current EU data protection rules, the EC has a new responsibility to restore the trust and confidence of the EU citizens with the updated rules. When the guidance provided by the ECJ in the leading cases are taken into account, existing rules and principles seem to be insufficient for the complex structure of the Internet and its methods.

[235] Daniel B. Garrie, Rebecca Wong, *Social networking: opening the floodgates to "personal data"*, C.T.L.R., Issue 6, Thomson Reuters (Legal) Limited and Contributors, 2010, p.174

BIBLIOGRAPHY

I. Books

- Albrecht, J. P., *Uniform Protection By The UE – The EU Data Protection Regulation Salvages Informational Self-determination*, Edited by Hijmans, H., Kranenborg, H., Data Protection Anno 2014: How to Restore Trust?, Intersentia, 2014

- Bennett, C. J., *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Cornell University Press, 1992

- Bernal, P., *Internet Privacy Rights: Rights to Protect Autonomy*, Cambridge University Press, 2014

- Bernal, P., *The EU, the US and Right to be Forgotten*, Reloading Data Protection, Edited by Gutwirth, S., Leenes, R., De Hert, P., Springer, 2014

- Bygrave, L. A., *Data Protection Law: Approaching Its Rationale, Logic and Limits*, Walters Kluwer Law & Business, 2002

- Carey, P., *Data Protection: A Practical Guide to UK and EU Law*, Oxford University Press, 2nd Ed., 2004

- Edwards, L., *Privacy and Data Protection Online: The Laws Don't Work?*, Law and the Internet, Edited by Edwards, L., Waelde, C., 3nd Ed., Hart Publishing, 2009

- Lambert, P., *A User's Guide to Data Protection*, Bloomsbury, 2013

- Murray, A., *Information Technology Law*, 2nd Ed., Oxford University Press, 2013

- Rallo, A., Martines, R., *Data Protection, Social Networks and Online Mass Media*, European Data Protection: Coming of Age, Edited by Gutwirth, S., Leenes, R., De Hert, P., Springer, 2013

- Zanfir, G., *Forgetting About Consent. Why The Focus Should Be On "Suitable Safeguards" in Data Protection Law,* Reloading Data Protection, Edited by Gutwirth, S., Leenes, R., De Hert, P., Springer, 2014

II. Articles and Reports

- Alsenoy, B. V., Kuczerawy, A., Ausloos, J., *Search engines after Google Spain: internet@liberty or privacy@peril?,* ICRI Working Paper Series, 6 September 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2321494, (Acessed on 23 July 2014)

- Birnhack, M. D., *The EU Data Protection Directive: An engine of a global regime*, Computer Law & Security Report 24, 2008, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1268744, (Accessed on 7 July 2014)

- Borghi, M., Ferretti, F., Karapapa, S., *Online data processing consent under EU law: a theoretical framework and empirical evidence from the UK,* International Journal of Law and Information Technology, Vol. 21, No:2, 2013

- Brown, I., *Communications Data Retention in an Evolving Internet*, International Journal of Law and Information Technology, Vol:19, No:2, Oxford University Press 2010, 17 November 2010

- Burgstaller, P., *Search engines and the extra-territorial dimension of the EC data protection law*, Computer and Telecommunications Law Review, 2009, (Westlaw sources)

- Cuijpers, C., Purtova, N., Kosta, E., *Data Protection Reform and the Internet: the draft Data Protection Regulation*, Tilburg Law School Legal Studies Research Paper Series No. 03/2014, http://ssrn.com/abstract=2373683, (Accessed on 3 July 2014)

- De Hert, P., Papakonstantinou, V., *The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals*, Computer Law & Security Review, Volume 28, Issue 2, April 2012, pp. 130−142

- Dowling, Jr, D. C., *International Data Protection and Privacy Law*, White & Case, August 2009, http://www.whitecase.com/files/publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/presentation/publicationattachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_intldataprotectionandprivacylaw_v5.pdf, (Accessed on 7 July 2014)

- European Commission, *On-line Services and Data Protection and Privacy*, Volume II, Annex to the Annual Report 1998 (XV D/5047/98) of the Working Party established by Article 29 of Directive 95/46/EC, 1998

- Feiler, L., *The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection*, European Journal of Law and Technology, Volume 1, No:3, 2010

- FRA, *Data Protection in the European Union: the role of National Data Protection Authorities*, European Union Agency for Fundamental Rights, 2010

- Garcia, F. J., *Bodil Lindqvist: A Swedish Churchgoer's Violation of the European Union's Data Protection Directive Should Be a Warning to U.S. Legislators,* Fordham Intellectual Property, Media and Entertainment Law Journal, Volume 15, Issue 4, Article 10, Volume XV, Book 4, 2005, http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1335&context=iplj, (Accessed on 18 July 2014)

- Garrie, D. B., Duffy-Lewis, M., Wong, R., Gillespie, R. L., *Data Protection: The Challenges Facing Social Networking*, Brigham Young University International Law and Management Review, Volume 6, Issue 2, Article 6, 2010, http://digitalcommons.law.byu.edu/cgi/viewcontent.cgi?article=1079&context=ilmr, (Accessed on 18 August 2014)

- Garrie, D.B., Wong, R., *Demystifying Clickstream data: A European and U.S. Perspective*, Emory International Law Review, Vol.20, 2006, http://www.law.emory.edu/fileadmin/journals/eilr/20/20.2/Garrie_Wong.pdf, (Accessed on 16 July 2014)

- Garrie, D. B., Wong, R., *Social networking: opening the floodgates to "personal data"*, C.T.L.R., Issue 6, Thomson Reuters (Legal) Limited and Contributors, 2010, http://gallery.mailchimp.com/b67555cbd61d2c649329cc05a/files/2010_CTLR_Issue_6_Garrie_Wong_Final.pdf, (Accessed on 19 August 2014)

- Godbey, B. N., *Data Protection in the European Union:Current Status and Future Implications*, I/S: A Journal of Law and Policy, Vol.2:3, 2006, http://heinonline.org/HOL/Page?handle=hein.journals/isjlpsoc2&div=38&g_sent=1&collection=journals#841, (Accessed on 17 July 2014)

- Graux, H., Ausloos, J., Valcke, P., *The Right to be Forgotten in the Internet Era*, ICRI Working Paper Series, ICRI Working Paper, 11/2012, 12 November 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2174896, (Accessed on 1 August 2014)

- Hon, W. K., Christopher Millard, *Data Export in Cloud Computing: How can Personal Data be Transferred outside the EEA?, The Cloud of Unknowing,* Part 4, Queen Mary University of London, 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925066, (Accessed on 21 July 2014)

- Irion, K., Luchetta, G., *Online Personal Data Processing and EU Data Protection Reform*, Report of the CEPS Digital Forum, Center for European Policy Studies, Brussels, April 2013, http://www.ceps.eu/book/online-personal-data-processing-and-eu-data-protection-reform, (Accessed on 7 July 2014)

- Johnson, A., *Data protection and E-commerce; The case for new law, in the information age*, 16th BILETA Annual Conference, University of Edinburgh, Scotland, April 9th - 10th, 2001, http://www.bileta.ac.uk/content/files/conference%20papers/2001/Data%20Protection%20and%20E-commerce%20-%20The%20Case%20for%20New%20Law,%20in%20the%20Information%20Age.pdf, (Accessed on 1 July 2014)

- Jones, R., Tahri, D., *An overview of EU data protection rules on use of data collected online*, Computer law & security review, 27, 2011, pp. 630-636, http://www.sciencedirect.com/science/article/pii/S0267364911001488, (Accessed on 22 July 2014)

- Ringelheim, J., *Processing Data on Racial or Ethnic Origin for Antidiscrimination Policies: How to Reconcile the Promotion of Equality with the Right to Privacy?,* Center for Human Rights and Global Justice Working Papers, Number 13, NYU School of Law, 2006, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=983685, (Accessed on 17 July 2014)

- Robinson, N., Graux, H., Botterman, M., Valeri, L., *Review of the European Data Protection Directive*, RAND Europe, Technical Report, 2009, http://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR710.pdf, (Accessed on 10 July 2014)

- Simitis, S., *Revisiting Sensitive Data*, Review of the answers to the Questionnaire of the

Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1999, http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Report_Simitis_1999.pdf, (Accessed on 18 July 2014)

- Spies, A., *Reform of the EU Data Protection Directive: 'Right to Be Forgotten'—What Should Be Forgotten and How?*, Privacy and Security Law Report, ISSN 1538-3423, 2011, http://www.bingham.com/Publications/Files/2011/12/Reform-of-the-EU-Data-Protection-Directive-Right-to-Be-Forgotten--What-Should-Be-Forgotten-and-How, (Accessed on 31 July 2014)

- Szafran, E., Van Overstraeten, T., *Data protection and privacy on the Internet: technical considerations and European legal framework,* 2001, CTLR, 56

- Tene, O., Wolf, C., *Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation*, Future of Privacy Forum, January 2013, http://www.futureofprivacy.org/wp-content/uploads/FINAL-Future-of-Privacy-Forum-White-Paper-on-Jurisdiction-and-Applicable-Law-January-20134.pdf, (Accessed on 13 July 2014)

- Tikk, E., *IP Addresses Subject to Personal Data Regulation*, http://www.ccdcoe.org/publications/legalproceedings/Tikk_IPAddressesSubjecttoPersonalDataRegulation.pdf, (Accessed on 16 July 2014)

- Wong, R., *Data Protection in the Online Age*, Sheffield University, 2006, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2220754, (Accessed on 12 July 2014)

- Wong, R., *Data Protection Online: Alternative Approaches to Sensitive Data?*, Journal of International Commercial Law and Technology Vol. 2, Issue 1, 2007, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=936391, (Accessed on 18 July 2014)

- Wong, R., *Social Networking: Anybody is a Data Controller!*, Nottingham Trent University - Nottingham Law School, Academic Legal Studies, 21 September 2008, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1271668, (Accessed on 18 August 2014)

- Wong, R., *Social Networking: A Conceptual Analysis of a Data Controller*, Nottingham Trent University, Nottingham Law School, Academic Legal Studies, Communications Law, Vol. 14, No. 5, pp. 142-149, 30 December 2009, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1529738, (Accessed on 19 August 2014)

- Wong, R., *The Data Protection Directive 95/46/ EC: Idealisms and realisms*, International Review of Law, Computers & Technology, 26:2-3, 229-244, 2012, http://www.tandfonline.com/doi/abs/10.1080/13600869.2012.698453, (Accessed on 11 July 2014)

- Wong, R., Joseph Savirimuthu, *All or Nothing: This is the Question? The Application of Article 3(2) Data Protection Directive 95/46/EC to the Internet*, The John Marshall Journal of Information Technology & Privacy Law, Volume 25, Issue 2, Spring 2008, http://repository.jmls.edu/cgi/viewcontent.cgi?article=1007&context=jitpl, (Accessed on 20 July 2014)

III. Official Sources

- Annulment judgment of the Court regarding Directive 2006/24/EC, dated 8 April 2014, http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN, (Accessed on 6 July 2014)

- Brown, I., *Comparative Study on Different Approaches to New Privacy Challenges, in particular in the Light of Technological Developments*, Working Paper No:1, The

challenges to European data protection laws and principles, European Commission, Directorate General Justice, Freedom and Security, 20 January 2010

- CJEU, C-101/01, *Bodil Lindqvist*, 6 November 2003, http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=en&mod e=lst&dir=&occ=first&part=1&cid=9409, (Accessed on 17 July 2014)

- CJEU, C-131/12, *Google Spain,* 13 May 2014, http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=243691, (Accessed on 22 July 2014)

- Council of Europe, European Union Agency for Fundamental Rights, *Handbook on European Data Protection Law*, 2014, http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf, (Accessed on 6 July 2014)

- Dinant, J., Terwangne, C., Moiny, J., *Report on the lacunae of the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No 108) resulting from technological developments,* The Bureau of the Consultative Committee of the Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, T-PD-BUR(2010)09 EN, http://www.coe.int/t/dghl/standardsetting/dataprotection/tpd_documents/T-PD-BUR_2010_09_en.pdf, (Accessed on 17 July)

- European Commission, COM (2010) 609 final: *A comprehensive approach on personal data protection in the European Union*, 4.11.2010, http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf, (Accessed on 31 July 2014)

- European Commission, *Factsheet on the "Right to be Forgotten" ruling*,

http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf, (Accessed on 2 August 2014)

- Korff, D., *The Use of the Internet & Related Services, Private Life & Data Protection: Trends & Technologies, Threats & Implications,* Council of Europe, T-PD(2013)07, 31 March 2013

- Judgment of Mr. Justice Hogan in the case *Europe v. Facebook*, 18 June 2014, http://courts.ie/Judgments.nsf/09859e7a3f34669680256ef3004a27de/481f4670d038f43380257cfb004bb125?OpenDocument, (Accessed on 22 July 2014)

- Opinion of Advocate General Jääskinen in the Case C-131/12 *Google Spain SL Google Inc. v Agencia Española de Protección de Datos (AEPD) Mario Costeja González, http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=38131*, (Accessed on 13 July 2014)

- Press Release regarding the annulment of the Directive 2006/24/EC, Court of Justice of the European Union, No: 54/14, Luxembourg, 8 April 2014, http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf, (Accessed on 6 July 2014)

- Press Release regarding the Progress on EU data protection reform now irreversible following European Parliament vote, European Commission, MEMO/14/186, 12/03/2014, http://europa.eu/rapid/press-release_MEMO-14-186_en.htm, (Accessed on 10 July 2014)

- Press Release, No 77/13 Luxembourg, Advocate General's Opinion in Case C-131/12, 25 June 2013, p.1, http://curia.europa.eu/jcms/upload/docs/application/pdf/2013-06/cp130077en.pdf, (Accessed on 13 July 2014)

- Report from the Commission, *First report on the implementation of the Data Protection*

Directive (95/46/EC), Brussels, 15.5.2003 COM(2003) 265 final, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0265:FIN:EN:PDF, (Accessed on 4 August 2014)

- The Commission's decision on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, 26 July 2000, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:EN:PDF, (Accessed on 22 July 2014)

- The Commission's factsheet on "Why do we need an EU data protection reform", http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf, 2011, (Accessed on 10 July 2014)

IV. The A29WP Documents

- The A29WP, Recommendation 3/97 on Anonymity on the Internet, 3 December 1997, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp6_en.pdf, (Accessed on 15 July 2014)

- The A29WP, Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware, 23 February 1999, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp17_en.pdf, (Accessed on 16 July 2014)

- The A29WP, Working Document on Privacy on the Internet - An integrated EU Approach to On-line Data Protection, 21 November 2000, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp37en.pdf, (Accessed on 16 July 2014)

- The A29WP, Opinion 5/2004 on unsolicited communications for marketing purposes

under Article 13 of Directive 2002/58/EC, 11601/EN, WP 90, 27 February 2004, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp90_en.pdf, (Accessed on 15 August 2014)

- The A29WP, Opinion 4/2007 on the concept of personal data, http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/opinion_04-2007_personal_data_/Opinion_04-2007_personal_data_en.pdf, (Accessed on 15 July 2014)

- The A29WP, Opinion 1/2008 on data protection issues related to search engines', WP 148, 4 April 2008, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf, (Accessed on 23 July 2014)

- The A29WP, Opinion 5/2009 on online social networking, 01189/09/EN, WP 163, 12 June 2009, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf, (Accessed on 6 August 2013)

- The A29WP Opinion 2/2010 on online behavioural advertising, 22 June 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf, (Accessed on 21 July 2014)

- The A29WP, Opinion 8/2010 on applicable law, 0836-02/10/EN WP 179, 16 December 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf, (Accessed on 11 July 2014)

- The A29WP, Opinion 15/2011 on the definition of consent, 01197/11/EN WP187, 13 July 2011, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf, (Accessed on 15 August 2014)

- The A29WP, Opinion 05/2014 on Anonymisation Techniques,

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf, (Accessed on 16 July 2014)

V. Other Sources

- White & Black Corporate & Technology Lawyers, *Anonymising personal data: new EU guidance published*, http://www.wablegal.com/e-bulletins/anonymising-personal-data-new-eu-guidance-published, (Accessed on 16 July 2014)

- Cormaic, R., M., *EU data protection authorities to agree approach to 'right to be forgotten' appeals*, 8 July 2014, http://www.irishtimes.com/news/crime-and-law/eu-data-protection-authorities-to-agree-approach-to-right-to-be-forgotten-appeals-1.1858574?utm_content=buffer57d30&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer, (Accessed on 3 August 2014)

- Greenslade, R., *Data Protection: What should be public and what should be private*, 1 July 2014, http://www.theguardian.com/media/greenslade/2014/jul/01/itn-media-events-conferences?utm_content=bufferdeada&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer, (Accessed on 3 August 2014)

- ICO, Personal Information Online – Code of Practice, http://ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/personal_information_online_cop.pdf, (Accessed on 14 July 2014)

- Irish High Court: European Court of Justice will decide over Facebook/PRISM, http://www.europe-v-facebook.org/PRISM_pa_en.pdf, (Accessed on 22 July 2014)

- Peers, S., *Europe v Facebook: the beginning of the end for NSA spying on EU citizens?*, EU Law Analysis, 18 June 2014, http://eulawanalysis.blogspot.co.uk/2014/06/europe-v-facebook-beginning-of-end-for.html, (Accessed on 22 July 2014)

- Peers, S., *Further Comments on Google Spain*, University of Essex, Human Rights Centre, Blogs, 13 May 2014, http://blogs.essex.ac.uk/hrc/2014/05/13/further-comments-on-google-spain/, (Accessed on 22 July 2014)

- Peers, S., *Reforming EU data protection law: the Council takes its first baby steps*, EU Law Analysis, 13 June 2014, http://eulawanalysis.blogspot.co.uk/2014/06/reforming-eu-data-protection-law.html, (Accessed on 14 July 2014)

- Peers, S., *The CJEU's Google Spain judgment: failing to balance privacy and freedom of expression*, EU Law Analysis,13 May 2014, p.2, http://eulawanalysis.blogspot.co.uk/2014/05/the-cjeus-google-spain-judgment-failing.html, (Accessed on 30 July 2014)

- Peers, S., *The data retention judgment: The CJEU prohibits mass surveillance*, EU Law Analysis, 8 April 2014, http://eulawanalysis.blogspot.co.uk/2014/04/the-data-retention-judgment-cjeu.html, (Accessed on 8 July 2014)

- Sensitivity of personal data should be determined by processing purpose and context not through categorisation, says ICO, http://www.out-law.com/articles/2013/february/sensitivity-of-personal-data-should-be-determined-by-processing-purpose-and-context-not-through-categorisation-says-ico/, (Accessed on 18 July 2014)

- Woods, L., *Google v Spain, Background to the forthcoming decision of the European Court of Justice*, 12 May 2014, http://inforrm.wordpress.com/2014/05/12/google-v-spain-background-to-the-forthcoming-decision-of-the-european-court-of-justice-lorna-woods/, (Accessed on 24 July 2014)

VI. Legislation

- Data Retention Directive, http://eur-lex.europa.eu/legal-

content/EN/TXT/PDF/?uri=CELEX:32006L0024&from=en, (Accessed on 9 July 2014)

- ECHR, http://www.echr.coe.int/Documents/Convention_ENG.pdf, (Accessed on 6 July 2014)

- EU Charter of Fundamental Rights, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF, (Accessed on 9 July 2014)

- General Data Protection Regulation, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf, (Accessed on 10 July 2014)

- ICO, *The future of data protection in the EU Briefing from the UK Information Commissioner's office*, September 2011, http://ico.org.uk/~/media/documents/library/Data_Protection/Research_and_reports/ico_stakeholder_briefing_-_the_future_of_dp_in_the_eu.ashx, (Accessed on 3 August 2014)

- The DPD, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML, (Accessed on 6 July 2014)

- Treaty on the Functioning of the European Union, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN, (Accessed on 9 July 2014)

- UDHR, http://www.un.org/en/documents/udhr/index.shtml#a12, (Accessed on 6 July 2014)