European (Legal) Studies on-line papers

Queen's University Belfast - School of Law – Jean Monnet ad personam Chair Professor D Schiek

http://go.qub.ac.uk/law-cetls

ADRIEN JAMMET

The Evolution of EU Law on the Protection of Personal Data

Volume 3, Issue 6, 2014

These on-line papers are part of the programme provided under the Jean Monnet ad Personam Chair held by Dagmar Schiek, which was part-funded by the EU Commission from September 2011 to August 2014, when they were published from the Centre of European Law and Legal Studies (CELLS) at the University of Leeds. The support of the EU Commission is acknowledged with gratitude.

The Evolution of EU Law on the Protection of Personal Data

Adrien Jammet

I. Introduction

During the last couple of years, Google and Facebook have entered into a fierce competition to acquire innovative internet social services. Surprisingly, the staggeringly high prices offered for acquisition were incomparable with the revenue of the different services, and especially for the $19 billion that Facebook offered for a small messaging application with 50 employees and 20 million of revenue[1]. Most of these small start-ups were not developing cutting edge technologies, or a revolutionary economic strategy - firstly, because they are essentially communication services and secondly because they were free. Their huge interest resides only in their user's individual worth and attraction capabilities, building an ecosystem linking millions of people that are willing to share and exchange their personal information. That's their true value. Nowadays, "*Personal data is the new oil of the internet and the new currency of the digital world*"[2]. By acquiring such databases, the internet giants are extending their revenue stream that comes from the sale of advertising toward targeted users, and in doing so, they need as much as personal data as possible.

This reciprocal dependency between the users and the service is driven by an economic need that is limited by the respect of the right to privacy. In the digital world, this equation relies on the rights associated with the definition of what personal data is. Currently, the EU legal framework is based upon Directive 95/46/EC on the collection, gathering and treatment of personal data. This set of rights and liberties has given a certain number of protections for the citizens, as well as means to express their prerogatives during the processing of their personal information. Such a definition is built to hold up against the fierce appetite of the economic pressures, and is leaning toward the user's interest for his privacy. However, the recent discussions surrounding the new draft Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data[3] seem to express the idea that this protection is outdated, and must be revaluated. This draft proposal highlights the need to both secure the economic investments and to strengthen the user's protection by redefining associated rights and the place of the user's consent. In doing so, it leans toward a more contractually based relationship where the potential weakening of the respect of the right to privacy have to be assessed.

This paper offers a critical analysis of these attempts to subjugate the human right to privacy to the needs of a technology which is allegedly beyond regulation. This critical analysis is based on a certain conception of law's role, which will be exposed first (II). This will be followed by tracing the evolution of the EU's approach to data protection, starting with analysing the core principle of Directive

1 Taylor Richard, Facebook to buy messaging app WhatsApp for $19bn, BBC news, http://www.bbc.com/news/business-26266689

2 Kuneva Meglena, European Consumer Commissioner, March 2009, quoted by World Economic Forum, *Personal data: The Emergence of a New Asset Class*, January 2011

3 Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25 January 2012, COM(2012) 11 Final. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

95/46/EC (III), and continuing with exposing Europe's two-faced reform of the protection of personal data (IV)

II. Law and the digital world from a socio-legal perspective

When studying an evolution in legal frameworks, "*It is widely and routinely assumed that law reflects/mirror society and operates to maintain social order*"[4]. This socio-legal perspective is of great importance for the analysis contained in this paper. When dealing with new technology, the legal function of maintaining a social order is partially eroded because law has often been described as *'outrun'*[5]. This term implies that this human dimension of the law, partly as a means to regulate social behaviours, cannot be applied to the digital world because "*many types of interactions that have sprung from the Information Age are new in degree and sometimes in kind, and so there is often little or no law to guide those interactions*" [6]. Consequently, one might think that in the digital world, it is only the technologies capabilities and their creators rather than law that are limiting the actions of the users. This can be reflected by the broad scope of the terms of services that services like Google or Facebook have created to regulate their use. Once the common user has accepted these terms, it seems to be the unique piece of regulation that is applied to the service in its relation with its users. The user becomes responsible, and can sometimes have their say about the content of these terms if they appear unacceptable[7]. With that bridgehead established, the internet giants seem to be the better administrators, and the need for the creation of a regulation appears to have lost its interest for the citizen, and turns towards the viability of the services. In this mechanism, by default, the law would no longer originate from a social need, but from a technological and an economic need. Some academics think that

> *"the future of technological development, the future of economic policy, and the future of political relationships among States, rather than the course of legal speculation will be the fundamental factors. It is this which will determine the practical context of the law, pose the problems which it must resolve, and define the range within which a creative approach to legal problems can operate"*[8].

However, such an approach cannot be accepted. It seems reductionist to limit the law to an accessory of technological, economic and political interests. Its dimension goes further than the simple regulation of social behaviour. In reality, the digital world is not only a new social space that has been mostly created and organised by private entities, it also represents a new territory for the expression of human rights and the risks that it implies. Consequently, the argument stating that internet is a legal lacuna, where the better administrators would be the services themselves, is false, despite the absence of specific regulation applicable to each new service. The terms of service cannot be the only rules applying to the relationship between the users and the services because it would be driven by

4 Tamanaha, Brian Z, *A General Jurisprudence of Law and Society*, Oxford University Press, 2001, p51

5 Helft Miguel, Cain Miller Claire, *1986 Privacy Law is Outrun by the Web*, The New York Times, 9 January 2011, http://www.nytimes.com/2011/01/10/technology/10privacy.html?pagewanted=all&_r=0

6 Rashbaum Kenneth, Borden Bennett, Beaumont Theresa, *Outrun the Lions : A practical framework for analysis of legal issues in the evolution of cloud computing*, Ave Maria Law Review, 2014

7 McCullagh Declan, *Instagram apologizes to users: We won't sell your photos,* Cnet, December 18 2012, http://www.cnet.com/news/instagram-apologizes-to-users-we-wont-sell-your-photos/

8 Castberge Frede, *International Law in our time: Changing Values and Priorities*, Martinus Nijhoff Publishers, 1974, p 489.

economic interest. For all these reasons, the rights of the individuals using these services must have the priority over economic interests. These rights remain the expression of higher moral considerations and rights inherent to any human being. Giving in to the temptation to adapt the laws to the necessities of the technologies, without securing fundamental rights is a path that should not be taken. In doing so, the legislator would replace customs and morals with a pledge towards economic pressures. For this reason, the law applicable to new technology must retain its human dimension during its adjustment towards new services, which rely upon fundamental rights.

This question is at the core of the current reform of the personal data framework in Europe. In January 2012, the Commission proposed a reform[9] of Directive 95/46/EC[10], to improve the users' rights, and cut costs for business, which is changing the essence of the text. Viviane Reading (Vice-President of the European Commission) said that:

> *"data is really the currency of this new digital economy […], it is only when the consumers trust that their data will be well protected that they will continue to entrust it to businesses and to the authorities"*[11].

By analyzing such statements, some have raised the concern that the Commission was considering the protection of personal data "*personal data protection as a means to achieve economic growth rather than as a fundamental right"*[12]. This position represents a shift in the very reasoning for the creation of these laws in the first place time, and the core principles of Directive 95/46/EC.

The explosion of new communication and computerised services (which we have experienced since the arrival of computers), has flourished sometimes beyond the legal regime. The law needed to adapt accordingly. This situation is explained by the unforeseeable capabilities of our modern computing technologies, and their international aspects. They are generating new behaviours, new economic models and services which the law could not have predicted, nor ruled efficiently. But it has also given the resources to create new instruments of control and surveillance, highlighting the question of trust that one can put into these new tools. Technological advantages "*are finding their limits in the amplification of the risks for the invasion of privacy*"[13]. Accordingly, in that myriad of numerical innovations, information has become the centre of attention. As early as 1962, the IBM 1311 could store two million characters of information[14], and in 1971, the floppy disk offered the possibility to transport such information easily. The possibilities of exchanges, interconnections and access to databases of citizens' information were made easier and the uncertainty surrounding their use and treatment was accelerated by their possible exploitation by governments for surveillance purposes.

9 Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25 January 2012, COM(2012) 11 Final. *http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf*

10 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995.

11 Committee on Civil Liberties, Justice and Home Affairs, Committee meeting, 9 October 2012, Interparliamentary meeting on data protection, Session III – Data protection and law enforcement challenges. *http://www.europarl.europa.eu/ep-live/en/committees/video?event=20121009-1500-COMMITTEE-LIBE*

12 Association Européenne pour la défense de Droits de l'Homme, commenting on the European Commission's proposal on reform of Directive 94/45 (http://www.aedh.eu/Personal-data-protection-must.html)

13 Féral-Schuhl Christiane, *Cyberdroit : Le droit à l'épreuve de l'internet*, 6eme édition, Praxis Dalloz, 2010, p34

14 IBM 1311 Disk Storage Drive, *http://www-03.ibm.com/ibm/history/exhibits/storage/storage_1311.html*

Also, when they were first made available, the different telecommunication services and their computerised databases raised questions about the processing of their data. Therefore, regarding new technology law, the first legislative efforts not only reflect an opportunist adaptation of old definitions, but more often, the fear evoked by the capabilities of such devices. In the early days of computing technologies, protecting respect for private and family life[15] was one of the first concerns of individuals, motivating the intervention of the national and European legislators. The spectre of the society of surveillance described by Orwell in 1984 was not far away[16]. The logical response, as will be outlined, was completed by translating the right to privacy into the digital world, for securing the privacy of people faced with the fierce appetite for personal information. But then, '*Big Brother*' was still represented by the government in people's minds.

Nowadays, "*Big Brother*" has changed his mask. 1.3 billion people are active per month on Facebook[17] and Google is used for 5,922,000,000 searches per day[18]. 73% of Europeans have internet access[19]. These services represent a tremendous amount of data gathered conveying information on individuals. But if these figures are impressive, it is incomparable with a projected growth in global data generated per year as high as 40%[20]. The data gathered represents so much information, that these databases are now called *big-data*. Despite the fact that this term is often described as "*poor*[21]" in meaning, it has the advantage of representing the gargantuan set of databases that it gathers. This sector has an estimated potential annual value of 250 Billion dollars per year to Europe's public sector administration[22] and this is an economy that the European Union wants to embrace, despite the threat incarnate. Just like Facebook and Google, most of the internet services today are based on an economic model relying on commercials. The price of advertising is linked with its capability to accurately target potential customers. Hence, there is an economic need to build a more precise profile of the different users, which their own right to privacy restricts. That economic pressure is responsible for the current reform. In its Draft Proposal[23], the Commission is leaning towards a more contractual based relationship with users. By accentuating the importance of consent it is suggested that, provided there is sufficient information, the user will be able to have a better understanding of the treatment operated by the services, and will be able to inform their consent more freely. This position has to be analysed with regard to the objective of "*reinforcing legal and practical certainty for economic operators and public authorities*"[24]. It advances the belief that, since

15 Protected under Article 8 of the European Convention on Human Rights

16 Orwell George, *1984*, Gallimard, 1972.

17 Statistic Brain Website, Facebook Statistics, *www.statisticbrain.com/facebook-statistics/*

18 Statistic Brain Website, Google Statistics. *http://www.statisticbrain.com/google-searches/*

19 Internet World Stats, European Union Internet Users, 30 June 2012, *http://www.internetworldstats.com/stats9.htm*

20 McKinsey Global Institute, *Big Data : The next frontier for innovation, competition and productivity*, McKinsey and Company, January 2011, p6

21 Boyd Danah, Crawford Kate, Critical Questions for Big Data: Information, Communication and Society, 15:5, 662-679, 2012, p663

22 McKinsey Global Institute, *Big Data (above note 20)*, p7

23 Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25 January 2012, COM(2012) 11 Final. *http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf*

24 I- Context of the Proposal, p3; Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data (General Data

technology has evolved, the transfer of personal data has been rendered easier, and regarding the colossal investments and services relying on such a legal framework, it has to be redefined. Nevertheless, in the process, we should bear in mind the idea that all this data contains critical and personal information on human beings. Their possible exhibition and exchanges should be firmly tied to fundamental law.

The potential of these services for tracking people should not be underestimated. When it comes to creating a new framework for personal data, the relative similarities of the first concerns surrounding computers with our current situation with the Snowden affair[25] and the creation of the *'big data'* justifies an historical approach. In this period of modernisation of the data protection Directive, it is particularly important to remember the very core of its values and principles of the Directive (I), and the reasons for its existence, before analysing its next two-faced evolution (II).

III. The core principles of Directive 95/43/ EC

The Directive appeared after a long process of legal and social investigation, its genesis has been built around a firm reference towards the right to privacy (A), before setting up its broad set of rights and liberties (B).

A) A Genesis Built Upon the Right to Privacy

In 1974 in France an attempt to interconnect the files of different administrations[26] lead to a general outcry from the citizens. The public debate exposed the anxiety of a society towards such possibilities. This situation helped the creation of the first laws on the processing of data with computers, creating rights for the person concerned, and obligations for the responsible of the treatments, based upon the right of privacy[27]. This right to privacy is one of the fundamental rights protected by Article 12 of the Universal Declaration of Human Rights 1948[28]. It is also protected under Article 8 of the European Convention on Human Rights[29], where the right to respect for private and family life is

---

Protection Regulation), Brussels, 25 January 2012, COM(2012) 11 Final. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

25 Name of an NSA's consultant that has revealed critical information on global internet services surveillance. See Gellmann Barton, Edward Snowden, After months of NSA revelations, says his mission's accomplished, The Washington Post, 24 December 2013, http://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html

26 Boucher Philippe, *Safari ou la chasse aux Français*, Le Monde, 21 Mars 1974, http://www.delis.sgdg.org/menu/25avril/PresseLeMonde19740321.pdf

27 After Hesse Lander in Germany in 1970, Sweden in 1974 and The US in 1974, See Perray Romain, *Jurisclasseur Administratif, Fasc. 274 : Informatique. – Traitements de données à caractère personnel*, 31 Janvier 2008, Mise à jour le 15 Novembre 2012, et Castets-Renard, *Droit de l'internet : Droit Français et Européen*, Montchrestien, LMD Edition 2012, p10

28 United Nations Universal Declaration of Human Rights, 1948, article 12: *No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks*. http://watchlist.org/wordpress/wp-content/uploads/Universal-declaration-of-human-rights.pdf

29 "*Right to respect for private and family life : 1 – Everyone has the right to respect for his privacy and family life, his home and his correspondence. 2 – There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*", Article 8, European Convention on Human Rights, Rome 1950, http://www.echr.coe.int/Documents/Convention_ENG.pdf

protected[30], and Article 17 of the International Covenant on Civil and Political Rights[31]. Its existence is confirmed in Article 16 TFEU. According to the European Court of Human Rights (ECtHR):

> *"the protection of personal data, particularly medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by article 8 of the Convention"[32].*

But the ECtHR has gone further, by saying that even:

> *"the storing by a public authority of information relating to an individual's private life amounts to an interference within the meaning of Article 8. […]The subsequent use of the stored information has no bearing on that finding"[33].*

Therefore, it is not only the processing of the data that would be subject to Article 8 ECHR, but the mere fact of possessing personal data. This statement is easily explained by the importance of privacy for citizenship. Without entering greatly into a philosophical or a sociological debate, one can understand that it directly affects our inner-self.

Consequently:

> *"privacy, after all, encompasses much more than just control over a data trail, or even a set of data. It encompasses ideas of bodily and social autonomy, of self-determination, and of the ability to create zones of intimacy and inclusion that define and shape our relationships with each other"[34].*

First, privacy is linked with our liberty. By directly affecting our ability to think by ourselves, and to develop our own social network that will allow further political actions, it is touching the essence of a democratic society[35]. That concern is of particular importance in the context of surveillance, where "*freedom and security have always stood in a certain tension with one another. They must constantly be held in balance by rights and laws*[36]". Nonetheless, the overall concept is larger. It is also tied to intimacy, which can be understood as a "*personal action, done in an activity sphere that a person recognizes as inviolable*"[37]. Privacy has been defined as the right to be left alone[38]. But again, this

30 Article 8-1: *Everyone has the right to respect for his private and family life, his home and his correspondence*.

Article 8-2: *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*.

31 "*1 – No one shall be subjected to arbitrary of unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2 – Everyone has the right to the protection of the law against such interference or attacks*", Article 17 of the International Covenant on Civil and Political Rights, adopted and opened for signature, ratification and accession by General Assembly Resolution 2200A(XXI) of 16 December 1966, Entry into force 23 March 1976, in accordance with article 49. http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

32 European court of human rights, Case of M.S V. Sweden, 27 August 1997, Case Number 74/1996/693/885, point 41.

33 See European Court of Human Rights, Case of Kopp v. Switzerland, 25 March 1998, Case Number 13/1997/797/1000, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58144#{%22itemid%22:[%22001-58144%22]}

34 Froomkin A. Michael, *The Death of Privacy ?,* Stanford Law Review, 2000, Vol. 52: 1461, p1466

35 See Strate Lance, *The Deprivation of Privacy*, 3 December 2012, Hanna Harendt Center, http://www.hannaharendtcenter.org/?p=8466

36 Speech by German Chancellor Angela Merkel to the German Parliament on January 29, 2014, Translated from the German by Michael Shae, http://www.nybooks.com/articles/archives/2014/mar/20/freedom-and-security/?insrc=hpma

37 Author's translation from the original text at Saint-Pau Jean-Christophe, Jurisclasseur, Fascicule numéro 10 : *Jouissance*

cannot encompass the whole notion. Privacy comes along with a certain control given to the person on its own individuality and who can oppose a disclosure of his name, face or biometric information, which has to do with confidentiality and identity[39]. Liberty, intimacy, identity and confidentiality are all present in the broad conception of privacy. Consequently, privacy is a legal tenet that is very difficult to cease, firstly because its definition varies from one country to another and secondly because it's very nature is subject to a certain number of discussions. Some think that it could be propriety right[40], others thinks that it could be a right attached to the person[41]. The reasoning is that this concept appeared not so long ago[42], and "*technology has played a large role in the story of the emergence of information privacy law*"[43]. Furthermore, our own definition of our private information and space is different from one person to another. That argument is regularly used by partisans of a deconstruction of the notion, "*seeing it not as a right, but rather as an exchange between people and organizations, bound by the same trust that facilitate effective social and business relationship*" [44].

Therefore, for the purpose of this paper, we will not elaborate on that question further, since it would require an entire book to focus on a simple definition that regroups the ideas of liberty, intimacy and identity. The right to the respect of the private life is

> *"permitting everyone to ask the state or individuals to respect the actions and the secrecy linked to identity and intimacy. It is a power of action and control over certain information […] and the power to authorize or oppose to an investigation or the disclosure of information tied to identity or intimacy"*[45].

This definition has the advantage of representing a concrete approach of the concept of privacy, which can be applied negatively to a certain number of practices in the digital world. However, it does not allow half of the internet services to exist in their current form. Their economic model itself represents an infringement to the secrecy of the personal information, which could be extremely complicated to console with the respect of privacy. There is a necessary equilibrium to take into account, to dodge an "*informational seclusion, which prohibits the state or private organizations from collecting or applying certain kinds of personal data*"[46].

---

des Droits Civils – Droit au respect de la vie privée – Définition conceptuelle du droit subjectif, 20 Avril 2010, point 94. [''*Lorsqu'une personne invoque une ingérence dans la liberté de la vie privée, c'est-à-dire une liberté civile ou publique, la vie privée s'entend d'une action personnelle, d'une sphère d'activité dont le titulaire invoque l'inviolabilité''].*

38 Warren D. Samuel, Brandeis D. Louis, *The Right to Privacy*, Harvard Law Review 193, 1890.

39 Saint-Pau Jean-Christophe, Jurisclasseur, (as note 37).

40 Lessig Lawrence, *Privacy as Property – Party V: Democratic Process and Nonpublic Politics*, Social Research, Spring, 2002. http://www.englishdiscourse.org/lessig.html

41 Kayser P, *La Protection de la Vie Privée par le Droit*, Economica 3eme édition, 1995.

42 Sociologists are linking its appearance with some social phenomenon arising in the XVIII' century, see Pardailhé-Galabrun V. A., *La naissance de l'intime,* PUF 1988.

43 Solove J. Daniel, *A brief History of Information Privacy Law*, George Washington Faculty Publications , 2006, p I-3

44 Leroux Yves, *Privacy Concerns in the Digital World*, Computer Weekly, October 2013, http://www.computerweekly.com/opinion/Privacy-concerns-in-the-digital-world

45 Author's translation from the original text at 'Saint-Pau Jean-Christophe, Jurisclasseur, point 26, (as note 37) [''*Le droit au respect de la vie privée, permet à chacun d'exiger de l'État comme des particuliers, le respect de la liberté d'action et du secret des informations relatives à l'identité et à l'intimité. Le droit manifeste ainsi un pouvoir d'action et un pouvoir de contrôle de certaines informations, c'est-à-dire en dernière analyse le pouvoir d'autoriser ou de s'opposer à une investigation ou une divulgation d'informations relatives à l'identité ou l'intimité''*. .

46 Schwartz M. Paul, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*,

The law needed to come with a concept that would be a material representation of the individuals' privacy in these numerical worlds, creating a nest for them to develop, and the concept of "*personal data*" [47] was the answer. In the same spirit that is expressed behind the current reform, Europe was trying to find the right approach that "*can strengthen people's rights practically and concretely, without cutting them off from new economic and social benefits*"[48]. Following this though, in a time when no regulations had been set, the European Council stated that it was necessary to take into account the increasing flow across frontiers of personal data undergoing automatic processing, without interfering with "*the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy*" [49]. In 1981, the Council of Europe built the first ever regional European regulation with regard to automatic processing of personal data[50]. The aim was to "*reconcile the fundamental values of the respect for privacy and the free flow of information between peoples*"[51]. This text, created basic principles for data protection, especially concerning the fair and lawful process of obtaining and processing of the information, the scope and purpose, the storage, the accuracy and the preservation of the data[52]. These will generally interact with the first works on Directive 95/46/ EC.

B) The Set of Rights and Liberties of Directive 95/46/ EC

The gestation of Directive 94/45/ EC has lasted almost 10 years, starting as soon as Convention 108 entered into force on the 1st October 1985[53]. Convention 108 was considered incomplete, by letting open "*a large number of options for the implementation of the basic principles it contains, and it has been ratified by only seven Member States, of which one still has no domestic legislation*"[54]. It was important that a "*minimum level of uniformity* [exists] *between the member states*"[55]. During this period, tides of proposals trying to fade the fundamental rights had come and gone, leaving the European citizens' rights intact. The respect of the fundamental rights was considered as prominent, and it is related to the objective of that text. In a time where no harmonization had been made "*the scale*

Berkeley Law Scholarship Repository, 1-1-1994, p555.

47 Contion for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg 28 January 1981, *Article 2 – Definition : Personal data means any information relating to an identified of identifiable individual (data subject).*

48 Kroes Neelie, *Data Protection Day Statement*, 28 January 2014, https://ec.europa.eu/commission_2010-2014/kroes/en/content/data-protection-day

49 Preamble of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, Strasbourg, 28 January 1981. http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

50 Ibid. Preamble.

51 Ibid. Preamble.

52 Op. Cit. Convention of European Council, Article 5 – Quality of data of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

53 Entered into force with the first 5 signatures, see the complete list of signatures, Conseil de l'Europe Website, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=FRE

54 Introduction, Point 3 of the Communication of the Commission of the European Communities, COM (90) 314 Final – Syn 287 and 288, Brussels, 13 September 1990.

55 Point 1.5.4, Economic and Social Committee, Opinion on the proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, the proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks and the proposal for a Council Decision in the field of Information security, 91/C 157/14, 17 June 1991, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:1991:159:0038:0048:EN:PDF

of divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States[56]" urges the Commission to take a step towards a common acceptance of fundamental principles. Back then, the first Directive was trying to achieve a functioning internal market:

> *"in which the free movement of goods, persons, services and capital is ensured [And] require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded."*[57]

The preamble says that:

> *"data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals*[58]*".*

Consequently, the Directive has extended the definitions and rights contained in Convention 108. A personal data:

> *"shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."*[59]

This reference to a direct or indirect identification is particularly important in the digital economy. Most of the time the identity can be distinguished from an identification number, and this could have represented a loop hole for the Directive[60]. But furthermore, this broad concept encompasses the new data that can be found in the extension of the numerical technologies of video and audio recording[61].

In fact, the Directive is functioning around three layers of protection that directly concerns the different actors implicated. Firstly, a set a rules concerning the gathering and treatment of the personal data that the responsible of treatment will have to follow, then it gives rights to data subject, and finally a means to control that protection system with national independent supervisory authorities

Concerning the set of rules for the gathering, the Directive contains an important add on with respect to the processing of personal data. Here, the definition tries to predict and ring fence any use that could be made of a data, by applying the Directive to a broad list of operations in Article 2[62]. The

---

56 Point 8 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995 P. 0031 – 0050, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

57 Ibid. Point 3.

58 Ibid. Point 2 of the Preamble

59 Ibid. Article 2 - Definitions

60 An extended look at that distinction could be found with the IP address case in CJCE 29 January 2008, Aff. C-275/06, *Promusicae c/Télefonica de Espana*, conlu. J. Kokott, 18 Jully 2007

61 Ponthoreau Marie-Claire, La Directive 95/46 CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, RFDA 1997. 125

62 Op. Cit. Article 2 of the Directive 95/46/ EC, (b) "*processing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording,*

novelty remains in the combination of manual and automatic processing, which was not considered in the Convention 108. For the protection itself, the Directive is not particularly innovative in relation to the previous principles. It extends the necessary rules regarding the quality of data[63], and it establishes the concrete rule for the gathering of the personal data, as seen in Article 6[64]. Along these principles, the Directive is implementing additional safeguards for the data subject, by including a certain number of new criteria for making data processing legitimate in Article 7[65].

As regards to rights for the citizen, they are prescribed in the continuation of Convention 108. The data subject has a right to be informed of the processing happening to his personal data. According to Article 10, he must be provided with a certain amount of information relating to the controller and the destination of the processing[66]. But moreover, there is a right to access the data, were the citizen can have the confirmation that there is data relating to him that is being processed and specifically what the processing entails. However, the idea that a company retains some personal information is only relevant if the citizen is entitled to know exactly what the concealed data is. For that purpose, the Directive has given the citizen an action to request *"in an intelligible form [of] the data undergoing processing and of any available information as to their source".* Once provided with this information, these rules give the right to rectify any data stored, and to have it erased when it infringes the Directive under certain conditions detailed in Article 6. Consequently, the citizen can have access to a primitive right to be forgotten thanks to Article 6.e, where the deletion of data that is no longer needed can be requested. This position has been very recently confirmed by the CJEU in the case of a Spanish citizen against Google[67]. At last, according to Article 14, the European citizens have a right to object "*at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation*[68]*".*

Finally, the Directive has established national and independent supervisory authorities in Article 28. It will have a power to investigate, to intervene and to engage in legal proceedings where violations have been committed on its national soil. It will hear the different claims lodged, and will report on its activities. Still, the supervisory authority, unless provided by the Member State, won't be able to edict regulation or to pre-authorise the different processing of personal data. These dispositions are easily explained by the fact that the Commission has chosen an *ex-post* control system: "*in this context, ex post facto verification by the competent authorities must in general be considered a sufficient measure"*[69]. To balance the possible threat, the Directive places great pressure on those responsible

---

organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction"

63 Op. Cit. Article 5 of the Convention 108.

64 Op. Cit. Article 6 of Directive 95/46/ EC, Section I, Principles relating to data quality : Article 6

65 Ibid. Article 7 of Directive 95/46/ EC, Article 7

66 Op. Cit. Article 10 of Directive 95/46/ EC

67 Cour de Justice de l'Union Européenne, Communiqué de Presse numéro 70/14, Luxembourg, le 13 Mai 2014, Affaire C-131/12, Google Spain SL / Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez, http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070fr.pdf

68 Op. Cit. Article 14 of Directive 95/46/ EC, "*Where there is a justified objection, the processing instigated by the controller may no longer involve those data; (b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses*".

69 Ibid. Point 52 of Directive 95/46/ EC

of the treatment, by implementing a new obligation toward security and the confidentiality of data treated. Subsequently, if certain academics have raised doubts about Article 7-f[70], which authorises the processing if it is "*necessary for the purpose of the legitimate interest*", this remains as a certain protection for the citizen. Also the opportunities offered by Article 18 of the Directive leaves the possibility for the Member States to create a notification system for each database creation. Yet, this provision is not mandatory, and there was a need for greater protection from a structural approach. This does however generate the first discussion about a possible modernisation of the Directive's principles.

IV. Europe's Two-Faced Reform of the Protection of Personal Data

In an attempt to modernize the Directive, the Commission will introduce a series of new rights for the European citizen (A), but will ultimately weaken the overall protection in establishing a reduction of the enforcement possibilities (B).

A) An Extension of the Citizen's Rights

In fact, most of these principles will be conserved inside the new Regulation, which will even try to strengthen these principles[71]. It is presented as a modernisation of the old Directive. It includes the possible use of online identifiers or genetic identification techniques inside the data subject definition, as well as the definition of biometric and genetic data (Article 4). However, the real interest resides inside the enlargement of the data subject protection. Firstly, concerning the treatments, we can observe that the overall emphasis is put on the transparency and clarification of information given to the data subject. It can be found throughout the entire Proposal, particularly in Articles 5 and 11. But the procedure also needed simplification. According to this Proposal, the controller of the file should establish a clear mechanism for providing the information to the data subject and the electronic means to request that data (Article 12). Participating in that movement towards better accountability for the different actors, the draft Regulation seeks to introduce Data protection by design and by default in Article 23. The first one represents the idea that "*the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures and procedures*" is sufficient to ensure the protection of the right of the data subject. The second one is related to the implementation of:

> *"mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage".*

This step, in spite of the potential legal criticism that it may invoke, describes an attempt to implement technical obligations that will directly impact the liability of those responsible for the treatment. Consequently, the Commission reserves the right to implement technical regulation in order to these new mechanisms.

---

70 See Ponthoreau Marie-Claire, *La Directive 95/46 CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* RFDA 1997. p125

71 European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), SEC (2012) 72 Final.

This idea participates in the data security obligations which the controller and the processor should implement regarding Article 30. According to the draft Regulation, the technical and organizational measures necessary to ensure a security level appropriate to the risks represented by the processing will become mandatory. The goal is to protect:

> *"personal data against accidental or unlawful destruction, or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorized disclosure, dissemination or access, or alteration of personal data".*

In case of breach of security, the controller will have to inform the supervisory authority of the data breach, "*not later than 24 hours after having become aware of it*". But furthermore, if the data breach is "*likely to adversely affect the protection of the personal data or privacy of the data subject*", which we can assume that it will be the case almost each time, the controller shall communicate the data breach to the data subject without undue delay, in accordance with Article 32. All of these measures amplify the information obligations, and seem to empower the citizens.

Within the same perspective, concerning the data subject's rights, the draft Regulation seeks to extend the right to rectify and to erase personal data. Here, it is establishing for the first time the right to be forgotten, alongside the right to erasure and the right to rectify. The right to be forgotten is the right for a person to erase certain personal information on the internet despite the fact that he has already given its consent for the treatment. It is a "*safeguard [that can be used] if there is no legitimate reason for an organization to keep it*"[72]. It is different from the simple right to erase in its very goal. This gives a right "*to silence on past events in life that are no longer occurring*[73]" and to offer citizen a possibility to obliterate some recording of their past behaviour. The idea is that this right applies both to past court records and other publications. This has to do with our identity that can be misrepresented by previous claims online[74]. If the internet never forgets, it is important that citizens can delete their "*digital skeletons*"[75]. However, the exact territorial scope of this notion is yet uncertain. Article 12-b of the Directive explicitly only expressed a right to erase and rectify, which seemed to allow an interpretation towards a right to be forgotten. However, the Court of Justice of the European Union recently accepted the right to be forgotten[76], allowing to use the Directive to remove certain information "*Unless there are particular reasons, such as the role played by the data subject in public life, justifying a preponderant interest of the public in having access to the information when such a search is made*"[77]. Here, the Court has to balance between the right for a person to erase certain information relating to him, and the right of information. Yet, much opposition has been raised against such decision, especially from Google where it's Global Privacy Counsel said that "*Search engines serve an important function online, and the right to be forgotten should not interfere with their*

72 Reading Vivianne, Speech : EU Data protection reform and social media : Encouraging citizen's trust and creating new opportunity" presented at the Economist Conference "*New frontiers for Social Media Marketing*", Speech/11/827, Paris, 29 November 2011

73 Pino Giorgio, *The right to Personal Identity in Italian Private Law : Constitutional Interpretation and Judge-Made Rights*, Edited by M. Van Hoecke and F. Ost, Hart Publishing, Oxford, 2000, p14

74 Gutwirth Serge, *Computers, Privacy and Data Protection: An element of Choice*, Springer, 26 Fevrier 2011, p91

75 Alexander Kurtis, Ho Vivian, *New law lets teens delete digital skeletons*, San Francisco Chronicle, 24 September 2013, Franhttp://www.sfgate.com/news/article/New-law-lets-teens-delete-digital-skeletons-4837309.php

76 CJEU C-131/ 12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [ECLI:EU:C:2014:317]

77 Ibid.

ability to point consumers to information published elsewhere"[78]. Therefore, the definition of that right is crucial.

In the draft Regulation, Article 17 specifies that "*The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child",* under certain conditions relating to the real purpose of the conservation or the consent of the data source. If no solid objection can be made, the controller will be forced to take "*all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible*". But if this seems like a small step toward data protection, the new Article extends this right to the third parties. Those responsible of the treatment will have to inform the third party that he has been requested to erase the information. Not to mention that he will be liable for the third parties' publication if he has authorised them to publish the personal data before.

This possibility will help the European Citizens by simplifying their demands. Instead of asking the erasure to each controller, they will make that demand to the entity they gave their personal data in the first place. Yet, the right to be forgotten is not the only right added. Article 18 of the draft Regulation introduces the right to data portability, where the ancient right to be informed "*in an intelligible form of the data undergoing processing"* from the Directive is extended. The data subject will have the possibility to request a copy of the data undergoing processing. Be as it may, this right is authorises the citizen to transmit this information to another service in this electronic form. This entitles people to easily change their service operators, reducing considerably the technical difficulties that may arise. For the services, this represents a huge possibility to acquire new customer, and new materials to sell.

Following this statement, the Commission is addressing this issue of advertisement and the use of such data inside the right to object. Article 19 provides additional safeguards to the possibilities of using personal data for marketing purposes. Yet, in the Directive, the right to object was not directly mentioning profiling. Nowadays, the better the profile of a customer is built, the more its worth. The different internet services are directly relying on such economy. Accordingly, in the draft Proposal, Article 20 limits the use of profiling to a certain number of criteria, like the consent of the data subject, or the necessity of its existence for the performance of a contract. Enlightening this matter, one can observe that the notions of contract and consent are now central in every one of these previous rights. According to Article 17, the right to be forgotten is valid if "*no other legal ground for the processing of the data*" is present. For that reason, the definition of the consent has been modified. Instead of an "unambiguous consent" in the Directive, the draft proposes a free, specific, informed and explicit indication of wish. The controller will then bear the burden of proof for that consent, and it should be given in the context of a written declaration which must be distinguishable from other matters. That consent has the ability to be removed at any time by the data subject, plus the fact that this consent cannot become a legal basis if there is a significant imbalance between the position of the data subject and the controller. At this point, one might think that this new Regulation is giving too many rights to the citizen that will be allowed to have a perfect control over their data, and to be

78 Fleischer Peter, Global Privacy Counsel at Google, Our thoughts on the right to be forgotten, 16 February 2012, *http://googlepolicyeurope.blogspot.fr/2012/02/our-thoughts-on-right-to-be-forgotten.html*

informed fairly about the processing used in the different services they use. Nevertheless, a second reading suggests another reality.

B) A Reduction of the Enforcement Capabilities

As we have seen, the protection inside the draft Regulation relies on the fact that the "consent" of data subject is necessary for most of the data processing. The burden of proof is put on the service to bring the existence of such a free, informed and explicit consent. As such, this provision is supposed to be "*empowering the citizen*[79]" and this statement would be true if it were inside a classic negotiation protocol. Though registering to an internet service, such as Google or Facebook is not equivalent to a negotiation, the customer cannot choose to refuse certain conditions that would be threatening his vision of privacy. In reality, this is a binary choice, between a full registration and abandoning the service. And this concerns the vast majority of internet services[80].

As a matter of fact the emphasis put on the consent and its consequences is weakening the rights that it was supposed to enhance. Nowadays, it is very difficult to use any service or software without accepting fully and explicitly the terms of service and conditions of use. A recent study suggests that it would take 76 work days to read the privacy policies that a normal person encounters in a year[81]. These documents frequently authorise the controller to sell and use any information that the customer is going to enter into the service. Hence, once a customer, the European citizen has explicitly consented to the further use of their own personal data. Perceived in its civil law tradition, this consent gives legitimacy to almost any processing, participating the growing contractualisation movement that is surrounding personal data and privacy rights. Yet, one might think that a citizen can withdraw his consent at "*any time*" according to the draft Regulation. Unfortunately, this would only apply if they are leaving the service. Most of the time, the option to withdraw consent is tied with the erasure of the account[82]. In this context, the choice of the draft Regulation to extend the rights of the European citizen appears to be in vain. Instead of being inspired by the initial work on the concept of personal data and the translation of privacy within the digital world, the Commission gives legitimacy to a commercial approach of the personal data, to the detriment of customers.

Fortunately, the draft Regulation has conserved the supervisory authority. It will be responsible for the protection of privacy, be able to punish any infringement, and will act as a safeguard to any misuse of personal data in the name of the European citizens. This authority shall hear any claims from the national citizens, or any legal person, and act accordingly. In fact, the Regulation proposal even confirms the importance of the supervisory authority by increasing the administrative sanctions that can be applied to data protection infringement. The idea was to "*strengthen*" [83] independent national data protection authorities, by giving it the power to impose penalties of up to €1 million or up to 2%

79 European Commission communication Paper, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf

80 Rogosch Patricia, Hohl Erik, *Data Protection and Facebook: An empirical Analysis on the role of Consent in social networks*, LIT Verlag Munster, 2012, p28

81 Madrigal Alexis, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, The Atlantic Website, 1 March 2012, http://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/

82 Rogosch Patricia, Hohl Erik, *Data Protection and Facebook: An empirical Analysis on the role of Consent in social networks*, LIT Verlag Munster, 2012, p28

83 European Commission, Communication IP/12/46, 25 January 2012 http://europa.eu/rapid/press-release_IP-12-46_en.htm

of the global annual turnover, depending on the size of the company and the infringement. This statement associated with the obligation to notify any breach of data privacy "*can attract a high level of attention from all stakeholders and supervising authorities*[84]*"* which was one of the objectives of the measure. Also, the supervisory authority will be responsible for the application of the draft Regulation on a territorial scope that will include every activity on the European soil, and to data subjects residing in EU. This means that even foreign based services, if dealing with European consumers, will have to comply. However, Article 51-2 reduces considerably the competence of the national entity by changing the territorial scope of national independent authorities.

It establishes that:

> *"where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States".*

This shift in the purpose of national supervisory authority complicates the action of the citizen. Also, the "*proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established*" according to Article 74-3. This is creating a situation of dependence towards an external national entity that is weakening the rights of the European citizens. Today, most of the internet services are established in Ireland. We can hardly believe that the Irish authority will have the means to protect every citizen from Europe and monitor the process of every major internet service. That proposition is tempered by the fact that "*Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has its habitual residence*", but the doubt subsists for the real power of the national court towards proceedings happening in another member states. First of all, this disposition will only be delaying a procedure that was previously enquired about by the national authority of the origin of the claim. Secondly, despite the cooperation mechanisms that exist, the coordination of the different entity will be virtually denied by the fact that only the one present in the country of the main establishment will be entitled of the procedure. Finally, the idea of the one-stop-shop opens the possibility of forum shopping for the private companies. By choosing the place of its main establishment, the company is partially choosing its legal compliance policy. This notion itself tends to nullify the effort of the Commission in recent years, to harmonise the different regime of data protection across the European Union. As we can see, it is not simply the fact of having a right that is important. According to Motulsky[85], it is only the gathering of some very precise elements that make the essence of the effectiveness of the legal action. Namely: the fact of being a legal entity, the existence of an action and its possible use in justice, and finally, the appreciation of the validity of the demand. Today, it is the possibility of exercising that action, and the condition of its assessment for the European citizen that is threatened by the Regulation. In simplifying the system

84 Dekker Tonny, Lynch Lindsey, Boukadid Nora, Kits Peter, EU Data Protections's Pradigm Shift: From Directive to Regulation, Ernst and Young; 2013, *http://www.ey.com/Publication/vwLUAssets/EU_Data_Protections_Paradigm_Shift_From_Directive_to_Regulation/$FILE/EU%20Data%20Protections%20Paradigm%20Shift%20From%20Directive%20to%20Regulation.pdf*

85 Guinchard Serge, Ferrand Fredérique, Chainais Cécile, *Procédure Civile*, Dalloz Hypercours, 3eme Edition

for the big internet operators, the Commission is taking away the possibility for the citizen to have the infringements regarding their data punished.

Finally, the requirement related to the privacy by design is considering technical measures as part of the necessary protection regarding personal data. Despite the necessary effort towards the creation of more secure platforms, and way to store personal data, one can hardly see the legal implications of such provision. According to Article 77 "*The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage".* In this context, if the controller has respect for the minimum security level expected by the Commission, he won't be liable in the case of a data breach, even if the impact of the attack for citizen's privacy is important. Besides, the creation of the technical level of security will require the participation of many actors from the tech sphere. In this scheme, we have to question the legitimacy of such a group that has not been defined in the draft Regulation.

At the time of publishing, most of these measures have been approved in first reading by the European Parliament[86], and await the Council's approval. Despite the 207 amendments, the conflict between the economic aspects and the interest of the citizen's protection still appears. On one hand, amendment 99 concerning Article 5 has added the importance of the effectiveness of the exercise of the right of the data subject[87] and the modification of Article 7 strengthens these rights by ensuring that "*provisions on the data subject's consent which are partly in violation of this regulation are fully void*[88]". Also, in relation to the Snowden revelations[89][90], the transfer or disclosure of personal data ordered by a court, a tribunal or an administrative authority from a third country shall not be recognized or enforceable in any manner without prior authorisation by the supervisory authority[91]. On the other hand, disclosure of information has been rendered easier by including a clause according to which data can be lawfully processed if: "*the third party to whom the data is disclosed, and which meet the reasonable expectation of the data subject based on his or her relation with the controller.*[92]" Furthermore, a service provider shall be allowed to withdraw its services if the customer withdraws consent to data processing. [93] Any consent to data processing will thus be based on a significant imbalance between the customer as data subject and the service provider as the controller . Consequently, customers will find it difficult to object to profiling, which shall be newly defined in Article 4 as "*any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability or behav-*

86 Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (*COM(2012)0011* – C7-0025/2012 – *2012/0011(COD)*).

87 Ibid, Amendment 99, "*A personal data shall be: […] (ea) processed in a way that effectively allows the data subject to exercise his or her rights (effectiveness)".*

88 Ibid, Amendment 101.

89 See Greenwald Glenn, *No Place to Hide: Edward Snowden, the NAS and the U.S. Surveillance State*, Henry Holt and Co, Metropolitan Books, May 2014.

90 "*Following the U.S. data spying scandals, data protection is more than ever a competitive advantage*". Viviane Reding, EU's Justice Commissioner*, European Commission, Progress on EU data protection reform now irreversible following European Parliament vote*, MEMO/14/186, 12 March 2014.

91 Ibid, Amendment 140, inserting a new Article 43a.

92 Ibid, Amendment 100, addition to Article 6, paragraph 1 f)

93 Ibid, Amendment 101, addition to Article 6 paragraph 4.

iour[94]". Such an approach nullifies the gains in favour of the citizens' rights, and this point would be critical in the next Council decision on this Regulation.

The final text of the directive is highly unpredictable, although the outgoing EU Commission had viewed the European Parliament's position as irrevocable[95]. The new Justice Commissioner Martine Reicherts has already met Kent Walker, Vice President and General Counsel of Google "*after the commitment given last week from Italy's Justice Minister Andrea Orlando to treat the EU data protection reform as a political priority under the Italian Presidency, and ahead of the Justice and Home Affairs Council in October at which Ministers are expected to agree on further key aspects of the reform*"[96]. As a matter of fact, the respective positions of the Member States expressed in the next Home Affairs Council will shape the future of this Regulation.

V. Conclusion

The process of updating the legal framework surrounding the processing of personal data in the digital world has led to a structural opposition between the economic models of the internet giants and the right to privacy. The principal objective of Directive 95/46/EC was to enhance the protection of the citizen's rights in a numerical area where their personal information could be easily used against their interest. That protection was based on the wide notion of privacy (partially transferred into the definition of personal data) to become a concrete legal object in the information and communication technologies. This was meant to "*reconcile the fundamental values of the respect for privacy and the free flow of information between peoples*"[97] in the idea of dogging an informational seclusion. Based on such consideration, the Directive established a set of rights and liberties that were made to apply at three different levels. Firstly, by surrounding the possibilities for the collection and processing of personal data by the different services. Secondly, by giving rights to the users that allow them to have a certain control over their own data and finally, by permitting the subject of the treatment to claim their rights in front of an independent national supervisory authority. However, in 2012, the Commission issued a draft Regulation proposal to modernize such legal construction in response to the fact that "*technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities*"[98]. In the search for an equilibrium between the economic and public interests, its analysis shows that this reform is leaning toward a contractualisation movement of the relationship between the user and the service.

Consequently, the action of the Commission inside the draft Regulation can be summarised as a slide of the formalities surrounding the treatment, to the benefit of accountability borne by the control-

94 Ibid, Amendment 98, new paragraph 3a to Article 4

95 European Commission, *Progress on EU data protection reform now irreversible following European Parliament vote*, MEMO/14/186, 12 March 2014.

96 European Commission website, *Commissioner Martine Reicherts meets Senior Vice-President and General Counsel of Google, Kent Walker*, 9 September 2014. http://ec.europa.eu/commission_2010-2014/reicherts/multimedia/news/2014/09/20140909_en.htm

97 Preamble of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, Strasbourg, 28 January 1981. http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

98 Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25 January 2012, COM(2012) 11 Final. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

lers and processors of the files. This slide is accompanied by a tightening of the protection's requirements and rights of the data subject. But, by emphasizing the necessity of the consent, and facilitating the legal procedure for the private entities, the draft Regulation is in fact greatly in favour of the contractualisation movement that will ultimately arm the citizen. The change present in the territorial scope of the independent national authorities is a possible threat toward the possibility of enquiry on infringements. Such an approach is partially ignoring the very nature of the personal data, which comes from the fundamental right to privacy. In this scheme, the Commission is leaning towards the American conception of the protection of privacy, more in favour of a property nature of personal data[99]. In its role of balancing the fundamental rights and the free flow of personal data, the Commission has chosen. Under the current draft, the exchanges of personal data are greatly facilitated despite the attempt to settle the data to the European soil. Here, the same issue arises, since the consent is a possible derogation for any transfer of personal data, as seen in Article 44. The power of consent of the citizen, will lead him into selling his privacy, in exchange for a service.

Be as it may, this discussion around the protection of privacy for the European citizen is not limited to our vision of personal data, but directly concerns the idea of internet services itself, relying on an economic model based on advertisement. Considering this point of view, the Commission, with this draft Regulation, has not only failed its object of greater protection for the citizen, but ultimately, it has failed in creating a more secure legal environment for the internet industries by giving rights to the customers that has not been defined precisely enough.

99 For example, Schwartz Paul, *Property, Privacy and Personal Data*, University of California, Berkeley, Harvard Law Review, Vol. 117, Vol. 7, p2055, May 2004.