Competitive value of data protection: the impact of data protection regulation on online behaviour

COMPETITIVE VALUE OF DATA PROTECTION: THE IMPACT OF DATA PROTECTION REGULATION ON ON-LINE BEHAVIOUR

Alessandro Mantelero[*]

This is an electronic pre-print version (un-refereed author version) of an article published in ***International Data Privacy Law (2013)*** *doi: 10.1093/idpl/ipt016* First published online: July 14, 2013.

ABSTRACT

- The increasing demand from individuals to have their privacy respected or to take decisions about the management of their information assumes a significant role in business activities and it becomes an important element for building public trust in service providers.
- In this scenario, keeping the focus of data protection only on the individual and its decisions is no longer adequate. If legislators consider data protection as a fundamental right, it is necessary to reinforce its protection in order to make it effective and not conditioned by the asymmetries which characterise the relationship between data subject and data controllers.
- This aim is implemented by the EU proposal by means of three different instruments: data protection impact assessment, privacy by design/by default solutions and the data minimization principle.
- The competitive value of data protection can be assured and enhanced only if the user's self-determination over personal data is guaranteed. From this point of view, countering the phenomena of data lock-in and "social" lock-in is fundamental in order to offer privacy-oriented and trustworthy services, which increase user propensity to share data and stimulate the digital economy and fair competition.

* Alessandro Mantelero, faculty fellow at the Nexa Center for Internet & Society, Polytechnic University of Turin and visiting fellow at the Oxford Internet Institute, University of Oxford. E-mail: alessandro.mantelero@polito.it.

1. The competitive value of data protection

For many years data protection has been considered an undue burden for the private sector, as it limits business opportunities, reduces innovation in the area of customized services and increases operating costs. These arguments have been used by lobbies in order to criticize the EU Directive 95/46/EC[1] and to suggest a limited implementation of its principles. This attitude has now re-emerged with regard to the new EU Proposal for a General Data Protection Regulation.[2]

Firstly, these arguments represent a limited and incorrect representation of the impact of data protection regulations. They consider the costs due to legal compliance without analysing the related benefits and the external effects on other areas (such as security, corporate reputation, value of informational assets) that should also be included in a correct and global estimation of the costs.

Secondly, they underestimate the demand for data protection coming from the society at large. The increasing technological power of data collection and data mining have generated a reaction in terms of rising concern about privacy and social control.

In a society where many voices outline the risks of massive data collection,[3] profiling and

1 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 [1995] OJ L281/31. All the following references and footnotes concerning the Directive 95/46/EC are indicated simply as Directive 95/46/EC.

2 See 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)', COM(2012) 11 final, Brussels, January 25, 2012 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF> accessed 15 march 2013. See also Council of the European Union, '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)', Brussels, June 22, 2012. All the following references and footnotes concerning the Proposal refer to the document of the Council of the European Union and are indicated simply as Proposal. See also Julie E. Cohen, 'What Privacy Is For' (2013) 126 Harv.L.Rev. 1904-1933.

3 See Daniel J. Solove, 'Privacy and Power: Computer Databases and Metaphors for Information Privacy' (2001) 53

concentration of power over information, attention has become focused mainly on privacy policies adopted by private companies and governments. This concern is not contradicted by the theories, which claim that the right to privacy no longer exists as people willingly share information in return for economic benefits or free services. Even if the economic exploitation of personal information is an accepted (or desirable) consequence of the information age and of the pervasive use of ICT services, these are not sufficient elements to consider the protection of personal data as outdated.

As demonstrated in recent studies on young people, a more intense activity of data sharing is linked with the consciousness of the value of personal information and of the consequences of sharing it, and this consciousness is higher among digital natives than in the older generations.[4] It seems that the more the data are exploited, the more people seem to acquire a consciousness of informational self-determination. Furthermore, information about risks related to data protection or news on data breaches increase the awareness of the implications and relevance of privacy policies.

In this context, the increasing demand from individuals to have their privacy respected[5] or to take decisions about the management of their information assumes a significant role in business activities and it becomes an important element for building public trust in service providers.[6] Moreover, a lack of data protection increases the risks of illegitimate access to information or misuse of personal data, with a potential chilling effect on individual willingness to share and

Stan.L.Rev. 1393, 1403–1413.

4 See Danah Boyd and Alice Marwick, 'Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies' (Oxford Internet Institute Decade, Internet Time Symposium, 22 September 2011) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128> accessed 4 February 2013.

5 See The Boston Consulting Group, 'The value of our digital identity', November 2012, 12, 14, 26, 43, 44 <http://www.lgi.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf> accessed 7 March 2013. For a more comprehensive analysis, see European Commission, 'Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union', June 2011 <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf> accessed 7 March 2013.

6 According to The Boston Consulting Group, "two-thirds of the potential digital identity value – or about €440 billion in 2020 alone – is at risk if stakeholders fail to establish a trusted flow of personal data". See The Boston Consulting Group (n 5) 111.

communicate personal information.[7]

From this perspective, data protection and a compliance to regulations that protect personal information have generated a new demand for and supply of privacy-oriented services, which is increasing competition and innovation.

These needs become more relevant and observable in the context of social networks, where service providers are collecting large amounts of data (Big Data) in order to extract predictive information about individuals and social groups. Although there is a "social" lock-in effect[8] due to the dimension of the dominant players (e.g. Facebook), the relevance of privacy policies has emerged in different cases. These have induced companies to change their policies and business plans (see e.g. Google Buzz[9] and Facebook facial recognition[10] cases). This result is not only the consequence of individual actions or protests of many users, but has also been made possible by the existing legal framework and by the presence of data protection authorities. In the presence of sophisticated

7 Unfortunately many companies still underestimate the relevance of data protection issues, as emerged in The Edelman Privacy Risk Index, which reveals that 57% of respondents think their organization does not consider privacy and the protection of personal information to be a corporate priority, see Edelman and Ponemon, 'Edelman Privacy Risk Index Powered By Ponemon', 13 November 2012 <http://www.edelman.com/insights/intellectual-property/privacy-risk-index/> accessed 23 January 2013.

8 See below paragraph on Reinforcing user self-determination. The social lock-in excludes or restricts effective competition and limits the opportunities to create alternative services.

9 See *In re Google Buzz Privacy Litigation*, No. C 10-00672 JW (N.D. Cal. May 31, 2011) <http://epic.org/privacy/ftc/googlebuzz/EPIC_Google_Buzz_Settlement.pdf> accessed 23 January 2013. See also Todd Jackson, 'A new Buzz start-up experience based on your feedback' <http://gmailblog.blogspot.co.uk/2010/02/new-buzz-start-up-experience-based-on.html> accessed 23 January 2013. Todd Jackson was Product Manager, Gmail and Google Buzz.

10 See Data Protection Commissioner, 'Facebook Ireland Ltd. Report of Re-Audit', 21 September 2012 <http://dataprotection.ie/docs/Facebook_Audit_Review_Report/1232.htm> accessed 23 January 2013. See also Ingrid Lunden, 'Facebook Turns Off Facial Recognition In The EU, Gets The All-Clear On Several Points From Ireland's Data Protection Commissioner On Its Review' (*TechCrunch*, 21 September 2012) <http://techcrunch.com/2012/09/21/facebook-turns-off-facial-recognition-in-the-eu-gets-the-all-clear-from-irelands-data-protection-commissioner-on-its-review> accessed 23 January 2013.

systems of analyses and of dominant positions held by big companies, the self-determination of the single individual is inadequate and insufficient to create an effective and conscious market activity concerning personal data.

As emerged from the recitals in the preamble to the EU Directive 95/46/EC, the original goal of data protection was to increase trust in data collecting and managing services realized by governments and companies. This perspective is not considered if data protection is only viewed as an economic burden. The announcement of the death of privacy is only apparently useful for aggressive policies based on data exploitation, since the lack of attention on data protection exposes companies to litigations, has negative effects on their reputation and leads to a loss of clients. In this sense, the marketing strategy adopted by European ICT companies in offering services in the US is revealing: they stress the higher level of data protection guaranteed by their services in comparison with the US providers.

The increasing demand for data protection due to new technological applications and the necessity to reinforce user's trust in services provided by the public and private sector is inducing legislators to approve data protection laws or amend the existing regulations in order to adapt them to the technological evolution and new challenges.[11]

In this context the US and EU regulations have a central role due to the dimension of their marketplaces and the consequent impact of data protection on consumer protection. Furthermore, both the US and EU have a relevant influence on foreign legal models. On the one hand, the US uses its political influence in the APEC context in order to promote a model based on FIPPs (Fair Information Practice Principles)[12] in other countries, which has a more limited regulation than the

11 See Graham Greenleaf, 'Global Data Privacy Laws: 89 Countries, and Accelerating' (2012) 115 Privacy Laws & Business International Report, Special Supplement <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000034> accessed 18 February 2013.

12 See United States Department of Health, 'Records, Computers and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems', 1973 <http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm> accessed 26 December 2012. See also Department of Homeland Security, 'Privacy policy Guidance Memorandum', 2008

one emerging from the recent EU Proposal. On the other hand, the EU uses its regulation in order to indirectly influence other countries, by preventing European companies from sending data to non-EU countries that do not ensure "an adequate level of protection".[13]

From this perspective, the impact of the EU Proposal on data protection regulation should be analysed in order to evaluate its effect on online user's behaviour and, consequently, on business strategies.

2. An evaluation of the possible impact of the EU Proposal on online behaviour

The EU proposal for a general data protection regulation represents an evolution of the existing EU model, derived from the implementation in every country of the Directive 95/46/EC. The proposal intends to offer a higher level of protection and a more homogeneous processing of data, due to the adoption of a regulation instead of a directive.

Generally speaking, the proposal is not immune from criticism: the EU Commission probably could have adopted a different strategy, more focused on principles and with less detailed rules. Principles are more suitable for adoption in a world that is continuously changing and if we want to define the rules for the next twenty years, we probably do not need rules that are too detailed. For this reason, the definition of some principles and the concurrent setting up of specific bodies, able to define the

<http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf> accessed 26 December 2012.

13 See Directive 95/46/EC, arts 25, 26. In the absence of these laws, local companies are not be able to work with European partners, because they cannot receive personal data concerning consumers, suppliers and partners. Faced by the choice between adopting European standards on data protection or losing commercial relations requiring trans-border data flow. The United States has also come to terms with the European Commission, see 'Safe Harbor Privacy Principles' and annexed 'Frequently Asked Questions' approved by European Commission with decision 2000/520/CE, 26 July 2000 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML> accessed 20 December 2012. See also Paul M. Schwartz, 'The E.U.-US Privacy Collision: A Turn to Institutions and Procedures' <http://www.harvardlawreview.org/symposium/papers2012/schwartz.pdf> accessed 16 March 2013.

practical applications of these principles, seems to be an appropriate response to the needs of an evolving world.

Leaving aside these aspects concerning the legislative solution adopted, the provisions of the EU proposal have a positive effect in reinforcing user's trust and self-determination in social networks and, at the same time, define a uniform set of rules that reduce unfair competition due to forum-shopping practices[14] and introduce different solutions and remedies which are able to strengthen the level of compliance with the law.

3. Increasing the user's trust

For the past few years, the role of informed consent has been going through a crisis. It remains the most important instrument to affirm the central role of self-determination in data management and to offer individuals the possibility to negotiate their personal information. However, at the same time technology and modern systems of data mining (e.g. Big Data) drastically limit the user's capability to understand data processing, to be aware of it and to refuse consent.

These limitations are more evident in social networks. Firstly, the huge amount of data provided by the users represents the optimal dataset for predictive analyses[15] and, in many cases, the user is not aware of the possibility to extract new and different data from the information provided. The technological solutions used to manage data and how they work are unknown to the user, since they are not evident. Secondly, the information regarding data processing and its related technologies is

14 See Directive 95/46/EC, art 4 (1).

15 See DARPA, 'Total Information Awareness Program (TIA). System Description Document (SDD)', Version 1.1, 19 July 2002 <http://epic.org/privacy/profiling/tia/tiasystemdescription.pdf> accessed 3 January 2013; more sources on TIA are available at <http://epic.org/privacy/profiling/tia/>. See also National Research Council, 'Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment', Washington, D.C., 2008, Appendix I and Appendix J <http://www.nap.edu/openbook.php?record_id=12452> accessed 12 December 2012; Congressional Research Service, 'Report for Congress. Data Mining and Homeland Security: An Overview', 3 April 2008 <www.fas.org/sgp/crs/homesec/RL31798.pdf> accessed 12 December 2012.

given by means of long, unclear and changeable privacy policies, with the result that there is a disclosure that is only formal, but does not represent a sufficient solution in order to guarantee user self-determination. Finally, the presence of big players and the concentration of specific services in the hands of one or two companies (Facebook, Google, Twitter, etc.) induce the users to accept the conditions proposed in order not to lose the opportunities offered by internet services. In this sense, in many cases, big ICT companies have openly declared that our personal information is the due currency to pay their free services.

In this scenario, keeping the focus of data protection on the individual and its decisions is no longer adequate. If legislators consider data protection as a fundamental right,[16] it is necessary to reinforce its protection in order to make it effective and not conditioned by the asymmetries due to the factors described above. In this sense, an efficient way to obtain privacy-oriented technologies is to require a mandatory evaluation of the data protection implications in the product/service design and development phases, in order to make products and services intrinsically resistant to misuse of personal information from the outset.

This aim is implemented by the EU proposal by means of three different instruments: data protection impact assessment, privacy by design/by default solutions and the preference for minimizing data collection (data minimization principle). The later principle already exists in Directive 95/46/EC,[17] but is now reinforced by a new restrictive definition that limits the collection of data "to the minimum necessary in relation to the purposes for which they are processed".[18]

The first two instruments, data protection impact assessment, privacy by design/by default, merit a wider consideration. They do not represent a new approach to data protection, as privacy impact

16 See Charter of fundamental Rights of the European Union (2010/C 83/02), art 8.

17 See Directive 95/46/EC, art 6 (c) ("adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed").

18 See Proposal, art 5 (c). See also Luiz Costa and Yves Poullet, 'Privacy and the regulation of 2012', (2012) 28 C.L.S.Rev. 254, 260 ("Data Protection by Default... implies that in social networks, individual profiles should be kept private from others by default.").

assessment exists in different experiences around the world[19] and principles of privacy by design/by default have been defined and applied for many years.

With regard to data protection impact assessment,[20] firstly it is necessary to distinguish it from the similar notion of privacy impact assessment. These assessments evaluate ex ante the future impact that a specific services or product could have on privacy or data protection.[21] Assessment should be conducted not only considering individual data processes, but also a global aggregation of the

19 The first regulations on privacy impact assessment were introduced in 90's; for a comparative analysis of the different regulations, see David Wright and others, 'PIAF A Privacy Impact Assessment Framework for data protection and privacy rights', 21 September 2011 <www.piafproject.eu/ref/PIAF_D1_21_Sept_2011.pdf> accessed 3 March 2013. With regard to United Kingdom and Ireland, the first two countries to adopt the privacy impact assessment, see also Information Commissioner's Office, 'Privacy Impact Assessment Handbook'. Version 2.0 <http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.aspx> accessed 3 December 2012; Health Information and Quality Authority, 'Guidance on Privacy Impact Assessment in Health and Social Care', 18 December 2010 <http://www.hiqa.ie/resource-centre/professionals> accessed 3 December 2012. See also the standard ISO standard 22307:2008, 'Financial services. Privacy impact assessment' <http://www.iso.org/iso/catalogue_detail?csnumber=40897> accessed 3 December 2012; David Wright, 'The state of the art in privacy impact assessment' (2012) 28 C.L.S.Rev. 54-61; David Wright and Paul de Hert (Eds.), '*Privacy Impact Assessment*' (Springer 2012).

20 The original notion of privacy impact assessment has its roots in a document adopted by the Canadian Justice Committee in 1984, see David H Flaherty, '*Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*' (University of North Carolina Press, 1989) 277ff, 405; David Wright, 'Should privacy impact assessments be mandatory?' (2011) 54(8) Communications of the ACM, August 2011, 121-131. The first operative applications of this notion are in 90's and, with regard to the European Union, the first experiences were in UK and Ireland. See David Wright and others, PIAF A Privacy Impact Assessment Framework for data protection and privacy rights, 21 September 2011 <www.piafproject.eu/ref/PIAF_D1_21_Sept_2011.pdf> accessed 3 March 2013; Roger Clarke, 'An evaluation of privacy impact assessment guidance documents' (2011) 1(2) IDPL 111-120. See also Information Commissioner's Office (n 19); Health Information and Quality Authority (n 19); PIAF (A Privacy Impact Assessment Framework for data protection and privacy rights) project <http://www.piafproject.eu/Deliverables.html> accessed 16 March 2013.

21 The method adopted in the *privacy impact assessment* is based on the model of risk analysis: it considers the various risks related to each step of information management and defines a possible remedy to tackle them. This

different processes relating to the same information.[22]

However, the concepts of right to privacy and data protection are different. In countries outside Europe, particularly in the US,[23] the right to privacy covers a broad area that goes from informational privacy to self-determination in private life decisions. On the other hand, European data protection focuses on information regarding individuals, without distinguishing between their public or private nature.[24]

As shown by the application of data protection assessment to the RFID technologies,[25] this impact assessment is able to generate privacy-oriented solutions, offering a high level of data protection

---

assessment is usually summarized in a document, which describe the solutions adopted, and their effects on improving privacy.

22 In this sense the interaction between diffident process produces a result that is different from the simple arrogation and sum of them, for this reason a positive evaluation in terms of privacy impact assessment of every single process does not permit to draw the conclusion that also the whole system of linked data processing activities has not a negative impact on privacy.

23 See Luis Henkin, 'Privacy and Autonomy' (1974) 74 Colum.L.Rev. 1419; Raymond Wacks, 'The Poverty of "Privacy"' (1980) 96 L.Q.R. 77-78; Raymond Wacks, '*The Protection of Privacy*' (Sweet & Maxwell, 1980) 10ff; William A Parent, 'A New Definition of Privacy for the Law' (1983) 2 Law & Phil. 305; Diane L. Zimmerman, 'Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort' (1983) 68 Cornell L.Rev. 296, 299; Richard S. Murphy, 'Property Rights in Personal Information: An Economic Defense of Privacy' (1996) 84 Geo.L.J. 2381.

24 See Luiz Costa and Yves Poullet, 'Privacy and the regulation of 2012' (2012) 28 C.L.S.Rev. 255.

25 See Article 29 Data Protection Working Party, 'Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications', adopted on 11 February 2011 <http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-a29wp-opinion-11-02-2011_en.pdf> accessed 3 December 2012; see also European Commission, Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, C (2009) 3200 final, Brussels, 12 May 2009 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009H0387:EN:HTML> accessed 2 December 2012; Resolution of the European Parliament on Comprehensive approach on personal data protection, adopted on 6 July 2011 <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0323+0+DOC+XML+V0//EN> accessed 2 December 2012.

and, in this way, it contributes to increasing users' trust in technology and its related services. Another significant element of this assessment is the continuity of the evaluation that follows the product and the service during their entire lifecycle, redefining the assessment as new features or modifications are introduced. This ex ante and permanent analysis differs from traditional risk analysis, which is based on verification of the level of compliance realized ex post. This approach reduces the need for the legislator to follow technological developments and induces preventive solutions to ensure compliance with the principles of data protection.

From the perspective of the competitive value of data protection, an efficient assessment can reduce costs, in terms of loss of investments due to the inadequacy of services or products with regard to the existing legal limits. Finally, the benefits of investing in this evaluation process becomes clear if we consider the effect of the assessment in preventing misuse of data or illicit data processing. By contrast, an incomplete and inadequate assessment can have a negative impact in terms of reputation related to data breach, given the increasing attention to data protection among costumers and business partners. In this sense, the provision of Article 33 of the EU Proposal should be considered in a favourable manner, as it tries to address all the critical points positively.[26]

Taking into consideration the specific skills required to realize the impact assessment and its cost, the Proposal does not extend this process to every kind of data processing, but requires the assessment only when there are "specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes".[27] At the same time, the size of the companies, in terms of their resources, is also relevant.[28] In this sense, the Proposal empowers the Commission to adopt delegated acts for the purpose of further specifying the criteria and conditions concerning data protection assessment in order to "consider specific measures for micro, small and medium-sized

26 See David Wright and Kush Wadhwa, 'Introducing a privacy impact assessment policy in the EU member states' (2013) 3(1) IDPL 13-28.

27 See Proposal, art 33 (1). The article also defines specific cases in which the risks are presumed, see Proposal, art 33 (2).

28 See Proposal, art 33 (3).

enterprises".[29]

To increase users' trust in data processing the public availability of impact assessments could be useful.[30] This is a critical aspect due to the need to balance the information about data processing provided to users and the security and competitive issues of enterprises.[31] The conflict between these opposite issues emerged in the Commission work, as is evident from the comparison between the draft version of the proposal[32] and the text finally approved. The first document states that "the assessment shall be made easily accessible to the public", without any prejudice to the protection of commercial, public interests or security of the processing operations.[33] However, in the Proposal

29 See Proposal, art 33 (6).

30 See the guidelines of the Australian Victorian Privacy Commissioner, of the Irish Health Information and Quality Authority and of the British Information Commissioner's Office: Office of the Victorian Privacy Commissioner, 'Privacy Impact Assessments. A guide for the Victorian Public Sector' Edition 2, 20 April 2009 <www.privacy.vic.gov.au> accessed 23 February 2013; Health Information and Quality Authority (n 19); Information Commissioner's Office (n 19). See also Paul De Hert, Dariusz Kloza, David Wright (Ed.), 'PIAF A Privacy Impact Assessment Framework for data protection and privacy rights. Deliverable D3. Recommendations for a privacy impact assessment framework for the European Union', Brussels–London, 19 November 2012, 31 <http://www.piafproject.eu/ref/PIAF_D3_final.pdf> accessed 3 March 2013.

31 See Gus Hosein and Simon Davies, 'PIAF A Privacy Impact Assessment Framework for data protection and privacy rights. Deliverable D2. Empirical research of contextual factors affecting the introduction of privacy impact assessment frameworks in the Member States of the European Union', August 2012, 34-35 <http://www.piafproject.eu/ref/PIAF_deliverable_d2_final.pdf> accessed 3 March 2013. In order to balance these opposite issues, it is possible to provide sensitive information in a separate annex to the impact assessment report, which will not be made public, or publish a short version of the report without the sensitive contents. See also Recital 51 in the preamble to the Proposal.

32 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), Version 56, 29 November 2011 <http://www.statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf> accessed 16 March 2013. All the following references and footnotes concerning the Draft are indicated simply as Proposal (Draft).

33 See Proposal (Draft), art 30 (5).

any reference to the public availability of the assessment has been deleted.

The data protection assessment procedure is also fundamental in order to define an adequate strategy to limit privacy risks. It is important that a synergy develops between this kind of analyses and the adoption of solutions of privacy by design.[34] Both privacy by design and by default are generally adopted by the EU Proposal, which empowers the Commission to detail these solutions.[35]

The adoption of privacy-oriented technologies or processes, which embed data protection into their structure, is more suitable than ordinary "behavioural" rules to address the transnational dimension and continuous evolution aspects of ICT regulation.

Data protection is usually based on rules that permit or prohibit some activities ("behavioural" rules), using a three-phase model focused on prescription, ex post evaluation and sanction. This model is efficient in contexts where individual activities are traceable and the identity of the author of illicit activities can be discovered. However, these conditions are not always present in on-line dimensions or they involve excessive costs. For this reason, it could be useful to design processes and technological instruments in a privacy-oriented way, in order to create a "structural" barrier to their possible illicit use. At the same time, the implementation of technical solutions of data protection is less conditioned by the local legal framework than the implementation of "behavioural" solution and could be realized uniformly in different legal systems. For this reason,

---

34 See Peter Schaar, 'Privacy by Design' (2010) 3(2) Identity in the Information Society 267-274; Ann Cavoukian, 'Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era' in GOM Yee (ed), '*Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards*' (IGI Global 2012) 170-208; Ann Cavoukian, 'Privacy by Design: Leadership, Methods, and Results', in S Gutwirth and others (eds), '*European Data Protection: Coming of Age*' (Springer, 2013) 175-202.

35 See Proposal, art 23. The solutions based on data protection by default are considered by the Article as related to the access to information, data retention, coherence with the purposes of the collection and data minimization. See also Recital 46 in the preamble to Directive 95/46/EC and Article 29 Data Protection Working Party-Working Party on Police and Justice, 'The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data', adopted on 1 December 2009, 12-15 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf> accessed 14 February 2013.

there is a convergence on this approach between the US[36] and EU.

4. Reinforcing user self-determination

Privacy-oriented and trustworthy services increase user propensity to share data, stimulate the digital economy and fair competition. However, the competitive value of data protection can be assured and enhanced only if the user's self-determination over personal data is guaranteed. From this point of view, countering the phenomena of data lock-in and "social" lock-in is fundamental. The first is related to technological standards and data formats and limits the migration from one services to another, which offer the same functions; the second is the consequence of the dominant position held by some big players in the market of social networks that intrinsically limits the user's possibility to recreate the same network elsewhere.

In order to contrast the technological lock-in, the EU Proposal affirms the general principle of data portability. This right, which will be more detailed by the Commission through specific acts, concerns only personal data "processed by electronic means and in a structured and commonly used format". Data portability gives the user the right to obtain a copy of the data undergoing processing "in an electronic and structured format which is commonly used and allows for further use by the

36 With regard to the privacy impact assessment and the adoption of solutions of privacy by design in the recent guidelines provided by the US administration, see the following documents and reports: The department of commerce internet policy task force, 'Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework', December 2010, 34-36, 46 <http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf> accessed 3 December 2012; Federal Trade Commission, 'Protecting Consumer Privacy in an Era of Rapid Change. A Proposed Framework for Businesses and Policymakers. Preliminary FTC Staff Report', December 2010, 41, 49 <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf> accessed 3 December 2012; The White House, 'A Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy', February 2012, 12, 15, 44 <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf> accessed 3 December 2012.

data subject" from the controller.[37]

With regard to the "social" lock-in, there are no adequate answers, due to the fact that this situation draws its origin from the market and the existing barriers to competition. From this perspective, data protection authorities and legislators can only reinforce user self-determination, in order to limit the negative effects of this kind of lock-in. In this sense, the detailed regulation on the right to be forgotten provided by the EU Proposal seems to represent a positive action, since it clarifies how to exercise this right, which was only briefly mentioned in the Directive 95/46/EC.

Article 6 of Directive 95/46/EC stipulates that personal data must only be collected for specified purposes and "not further processed in a way incompatible with those purposes". The same article states that personal data should be kept in a form that permits the 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".[38] Both these rules limit any indiscriminate and endless collection of data. They are focused on the different parameters of the length of the time of retention and the processing purposes, which in the media context needs to be adequately evaluated.[39]

The article does not define the balance between the maintenance and the erasure of the data, which should be determined by the reason of the nature of the specific data collection.

The legal provisions, as they appear in the following Article 12 of Directive 95/46/EC, consider the relationship between memory and oblivion and moreover have a wider range of applications concerning the right to obtain the erasure "of data the processing of which does not comply with the

37 See Proposal, art 18. See also Luiz Costa and Yves Poullet, 'Privacy and the regulation of 2012' (2012) 28 C.L.S.Rev. 257. Criticisms have been expressed by Peter Swire and Yianni Lagos, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique' (2013) 72/2 Md.L.Rev. 335-80.

38 Both the rules admit specific exceptions for historical, statistical or scientific purposes, giving adequate safeguards.

39 See Alessandro Mantelero, 'U.S. concern about the European right to be forgotten and free speech: much ado about nothing?' (2012) 2 Contratto e Impresa Europa 727-740 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2169615> accessed 18 march 2013, on the right to be forgotten in Europe and US, with specific regard to media activities.

provisions of this Directive" from the controller.[40] Erasure is not strictly related to the dynamics of media communication, but to any data processing realized without the consent of the data subject or without providing adequate information to the data subject or outside the legal framework defined by data protection laws.

From this perspective, the length of time of the data processing and its purposes has a key-role.

For this reason, the expression "right to be forgotten" used in Article 17 of the Proposal is inappropriate and misleading, as it represents the English translation of *droit à l'oubli*, a right recognized by different decisions in France and in other European countries and not unknown in US case law.[41] But the *droit à l'oubli* is not the general right to delete personal information; it represents a limit to media activities in disseminating individual facts connected to past events that have no relationship with the present lifestyle or activities of the data subject and the relevance of these social or political facts does not prevail over their private nature.[42] This contradiction is more evident due to the fact that Article 17 of the proposed Regulation does not consider the right to be forgotten from the media perspective and provides an explicit exception with regard to this aspect.[43]

---

40 See Directive 95/46/EC art 12 (b). See also Randall P. Bezanson, 'The right to Privacy Revisited: Privacy, News, and Social Change, 1890-1990' (1992) 80 CLR 1133, 1150-1551, 1168, on the new paradigm of the right to privacy in the modern age and the relevance assumed by the individual choice and control over data.

41 See Mantelero (n 39) 728-733.

42 From this perspective, when the period of time in which interest in a specific private event is justified by its impact on the community has elapsed, the individual has the right to regain an anonymous life and privacy. This conception of the right to be forgotten is based on the fundamental the need of an individual to determine the development of their life in an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action performed in the past, especially when these events occurred many years ago and do not have any relationship with the contemporary context.

43 Proposal, art 17 (3) (a) declares that the right to be forgotten does not impact on freedom of expression and, in accordance with art 80, Member States shall provide for exemptions or derogations "for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression in order to reconcile the right to the protection of personal data with the rules governing freedom of expression". We should also underline that the notion of "journalistic purposes" adopted by the Proposal is broad and not strictly limited to media

Considering the wide notion of "journalistic purposes" adopted by the Proposal,[44] the provision of Article 17, concerning "the right [of the data subject] to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data"[45] will concern principally non-media companies, which are active in the sector of search engines, marketing or database services.

The new provisions of Article 17 do not seem to represent a revolutionary change to the existing rules with regard to protected interests, since the central prescription concerning the right to erasure is analogous to the above-mentioned Article 12 of the Directive 95/46/EC.[46] The proposed Article defines the different situations in which this right can be invoked,[47] but the various cases are still

activities. This notion includes any activities connected to "the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them" by the media, but also by different entities acting for both profit and non-profit making purpose. Also individual non-profit activities, such as managing a blog, seem to fall outside the scope of the Regulation, in accordance with art 2 (2) (d) which provides that the regulation does not apply to the processing of personal data "by a natural person without any gainful interest in the course of its own exclusively personal or household activity". This opinion is also supported by the wording of the Proposal, changed from the original of the last draft version in which this exception for personal was admitted "unless personal data of other natural persons is made accessible to an indefinite number of individuals", that represents the usual condition of the dissemination of information through blogs.

44 See above n 43.

45 We could also observe that the different representation of the right to be forgotten as the right to have personal data completely removed is consistent with the notion of *droit à l'oubli*, but in this case it has a wider scope, because the erasure of the data is not only related to the loss of interest in past events, but also to other situations (e.g. wrongful or illicit data processing) that do not concern the balance between media and individual life.

46 As stated in the Explanatory memorandum of the Proposal, art 17 is more analytical than art 12 of the Directive 95/46/EC in defining the right, only mentioned in the Directive, by providing "the conditions of the right to be forgotten". See Proposal, Explanatory memorandum, 9. See also Luiz Costa and Yves Poullet, 'Privacy and the regulation of 2012' (2012) 28 C.L.S.Rev. 256-257.

47 See Proposal, art 17 (1); see also Recital 53 in the preamble to the Proposal.

within the two main hypotheses already defined, albeit more rigidly, by the Directive 95/46/EC in force:[48] erasure due to data retention in contrast with the law or due to the original or supervening lack of the reasons that legitimate the processing of information.

With regard to the problem of social lock-in, described above, Article 17 (1) (b) and (c) are relevant, as they provide the erasure of the data when "the data subject withdraws consent" or exercises the right to object.[49]

The most critical aspect of Article 17 is defining the subjects to whom the rules are addressed, particularly with regard to Article 17 (2) and the related case in which "the controller [...] has made the personal data public" and consequently should take "all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data".[50]

If the rules do not show particular difficulties in the application to marketing activities,[51] their application to social network providers could be more controversial, because in these cases the notion of joint-controller is significant.[52] However, the interpretations given by the Article 29

---

48 See respectively Directive 95/46/EC, arts 6(1), 7(a), 12 (b), 14. With regard to the last Article 14, the proposed new definition of the right to object seems to offer a wider protection, see Proposal, art 19.

49 On the right to object, see Proposal, art 19.

50 See also Proposal, art 13, which states that the controller shall communicate any erasure, or rectification, "to each recipient to whom the data have been disclosed" and is released from that obligation only by proving that this communication is impossible or involves a disproportionate amount of effort.

51 See Proposal, arts 17 (1) (c), 19 (2).

52 See Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' adopted on 16 February 2010, 21 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf> accessed 26 January 2013. With regard to social networks and search engines the information are generated and managed both by users for their personal purposes and by the service providers for their (mostly commercial) purposes.

Working Party suggests that these cases should be considered under Article 17.[53]

In social networks, the presence of a high number of contacts could exclude the application of the so-called "household exception"[54] to the user, considering her as data controller, but also in this case the service provider assumes an active role in managing this user's information,[55] that legitimises the application of Article 17.

Despite the criticism expressed by internet companies, the burden related to the application of Article 17 does not seem excessive in the present phase of the information age. In a context in which few companies are managing an enormous amount of data and spreading or organizing it in order to make it accessible online, the balance between the individual right to be forgotten and the "right to make profits" cannot be found by requiring data subjects to have an active role in searching for any information concerning them, when this information has been spread on-line due to the business-model adopted by the controller. At the same time the EU proposal does not impose a general obligation to erase data managed by third parties, but requires only that third parties be informed that the data subject has requested them to delete any links or copy or replication and then further restricts this obligation by introducing the notion of proportionality. In this sense, it requires they take all "reasonable" steps to achieve its aim.[56]

Criticism about the right to be forgotten based on the freedom of expression are not well addressed.

---

53 See, with regard to search engines, Article 29 Data Protection Working Party, 'Opinion 1/2008 on data protection issues related to search engines' adopted on 4 April 2008, 14-15 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf> accessed 3 March 2013. Also search engines should be considered under Article 17 and considered as controllers, both when they act purely as intermediaries (with regard to the removal of personal data from their index and search results) and when they perform value-added operations and services, by reason of the control exercised on the information.

54 See Directive 95/46/EC, art 3 (2).

55 See Article 29 Data Protection Working Party, 'Opinion 5/2009 on online social networking', adopted on 12 June 2009, 5-6 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf> accessed 3 March 2013. See also Article 3 of the Proposal.

56 See Proposal, art 17 (2); see also art 17 (7), (9).

The provision of Article 17 (3) explicitly excludes the possibility to invoke the right to be forgotten (rectius the right to erasure) when "the retention of the personal data is necessary […] for exercising the right of freedom of expression", with reference to Article 80 that considers freedom of expression related to "journalistic purposes or the purpose of artistic or literary expression". This exception does not seem to fit the case of the expression of user's thoughts in social network environments, as the purposes are different from those defined by the law. Only the hypothesis of media activities realized through a social network account can considered be under Article 17 (3). We should draw the same conclusion with regard to search engines, since service providers should be considered as a publisher under press law if we consider the indexing of links related to news as journalistic purposes.

Finally, the digital nature of information and its possibility to be shared and re-shared by third parties has been considered a limit to the enforcement of the right to be forgotten due to the potential pluralism of jurisdictions related to multiple re-publication or re-use of information around the world.[57] The decentralized and multi-jurisdictional character of Internet represents a well-known obstacle to the effective protection of individual rights in this environment, but, at the same time, the nature of the right to be forgotten as defined by Article 17 seems to offer elements for a better and more efficient protection. The rules induce controllers to have an active role with regard to third party publication and they place the burden not on the person which the data refer to but on the entities that are in the best position to manage the data flows.[58]

The critical aspect related to these provisions is the necessity for an updated list of third parties receiving any item of data regarding an individual and to follow the information in this circulation through different controllers. This could generate a wide and invasive tracking system. In order to strike a balance, the idea of limiting the obligation to inform third parties to the first receiver of the information should be considered. At the same time, specific provisions should be introduced which

57 See Informal Note on Draft EU General Data Protection Regulation, December 2011, 4-5 <http://edri.org/files/12_2011_DPR_USlobby.pdf> accessed 15 December 2012.

58 See Proposal, art 17 (2), see also art 13.

oblige the controller who received the above-mentioned request, to notify the third parties to whom the data were disclosed. In this way, a self-implementing sequence of requests can obtain the final result of the complete erasure of the information, without any active role of the data subject except for the first request to the first controller, and without tracking the flows of information.

5. Increasing user's confidence and fair competition

The competitive value of data protection and its positive effect on user's confidence also derives from more uniform legislation and from the introduction of different means of control to ensure compliance to data protection regulation. More uniform legislation will be achievable through the adoption of a Regulation that will replace the Directive 95/46/EC and define a single legal framework on data protection in the European Union, without national variations due to the local implementation of the directive. The interpretation of the Regulation will be more uniform by reason of a stronger cooperation between national data protection authorities,[59] the role of the new European Data Protection Board[60] and the task assigned to the European Commission. Leaving aside any consideration on the adequate balance in the distribution of the power of control over data protection between these different authorities,[61] a more centralized and coordinated application of

59 See Proposal, c VII, s 1, 2.

60 See Proposal, c VII, s 3.

61 See Article 29 Data Protection Working Party, 'Input on the proposed implementing acts', adopted on 22 January 2013 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp200_en.pdf> 23 March 2013. See also Article 29 Data Protection Working Party, 'Opinion 08/2012 providing further input on the data protection reform discussions' adopted on 5 October 2012 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp199_en.pdf> accessed 23 March 2013; Article 29 Data Protection Working Party, 'Opinion 01/2012 on the data protection reform proposals', adopted on 23 March 2012, 7 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf> accessed 23 March 2013.

data protection rules will benefit companies and users, reducing differences and contradictions in the interpretations of the rules and, in this way, increasing compliance.

Further elements that guarantee a higher level of compliance are the introduction of specific solutions of monitoring and ad hoc administrative sanctions. Here, the Proposal introduces significant sanctions based on fines determined as a percentage of companies' annual worldwide turnover.[62] This remedy has received various expressions of criticism. Nevertheless, on the one hand, the prescriptions empower data protection authorities to evaluate the entity of the fine case by case, which will not necessarily be the maximum amount. On the other hand, without a relevant economic disincentive the widespread nature of some unfair practices and the asymmetry that exists between users and big companies will produce a limited deterrent effect, especially when the illicit data management does not cause economic losses to the users.

However, the sanctions are not sufficient to induce compliance and fair practice, alone. They should be combined with a more accountable organization of data management. The introduction of the data protection officer,[63] the implementation of mechanisms to ensure the effectiveness of the measures adopted by the controllers and the independent internal or external audits[64] represent different solutions to increase accountability. Another solution in order to increase the accountability of the controller is represented by the provisions concerning the data breach notification.[65]

Finally, it would be useful if the results of data protection compliance were clearer, without a deep analysis of long and technically written policies, by means of more simple and self-explanatory solutions, such as certification labels or data protection seals and marks. In this way, the user will be immediately aware of the essential elements of data protection and of the level of compliance, in order to compare different services and enhance the competitive value of data protection; privacy

62 See Proposal, art 79.

63 See Proposal, c IV, s 4.

64 See Proposal, arts 22 (3), 33 (6).

65 See Proposal, art 31, 32.

policies will therefore become an instrument to offer more detailed information on data processing.