THE EU DATA PROTECTION REFORM AND THE CHALLENGES OF BIG DATA:
tensions in the relations between technology and the law

MARIA EDUARDA GONÇALVES
ISCTE - Instituto Universitário de Lisboa, Portugal
maria.eduarda.goncalves@iscte.pt

Resumo: Neste artigo, examinamos alguns aspectos chave do Regulamento Geral de Proteção de Dados (RGPD), recentemente aprovado pela UE, à luz de implicações das tecnologias de "big data". Focaremos especificamente as opções regulatórias originais introduzidas pelo RGPD, baseadas na avaliação e gestão de riscos e na autodefesa pelos utilizadores da Internet, procurando interpretá-las à luz da ideia de desfasamento entre tecnologia e direito versus a ideia do direito enquanto motor do progresso tecnológico; por outras palavras, uma política legislativa guiada essencialmente pela intenção de promover a inovação tecnológica e a competitividade no Mercado Digital Europeu. Na realidade, a presente reforma da proteção de dados pessoais não parece facultar a proteção expectável de uma lei destinada a salvaguardar um direito fundamental. Não obstante as proclamadas aspirações do RGPD, o poder de decisão sobre o que e como coligir, armazenar e processar dados pessoais vem pendendo para os operadores e controladores dos dados em detrimento dos titulares dos dados e das autoridades de supervisão. Se bem que as condições tecnológicas, designadamente a automatização inerente do "data mining" e "data analytics", dificultem a efetividade de princípios chave da proteção de dados, é também verdade que a maior flexibilidade do regime é promovida pelas próprias opções regulatórias do Regulamento Geral. **Palavras-chave**: *Big data*. RGPD. Mercado Digital Europeu.

Abstract: In this article, we examine key features of the new EU General Data Protection Regulation (GDPR) in the light of implications of big data technologies. We will focus specifically on the original regulatory approaches introduced by the GDPR relying on risk assessment and management and on self-defense by Internet users, seeking to interpret them in view of a law-technology lag versus a law-technology driving perspective, meaning a legislative policy guided essentially by the intent to foster technological innovation and competitiveness in the Digital Single Market. Indeed, the current EU data protection reform seemingly fails to provide the appropriate caution that should be expected from a law designed to protect a fundamental human right. Notwithstanding the declared aspirations of the GDPR, the decision-making power on what and how to collect, store, and process personal data is leaning to the operators and data controllers to the disadvantage of data subjects and supervisory authorities. While technological conditions, namely the automatisation inherent to data mining and data analytics, render the effectiveness of key data protection principles harder to pursue, it is also true that the increasing suppleness of the regime is furthered by the Regulation's own regulatory choices.
Keywords: Big data. GDPR. Digital Single Market.

1. Introduction

Law is often perceived as a reactive institution, which lags behind technological advances (Moses, 2007, p. 269). Generally speaking, European law addressing Information and Communication Technologies (ICT) appears to counter this belief[1]. An illustration is Directive 95/46/EC, the Data Protection Directive[2]. Today, as the first broad reform of the EU data protection legislation is being achieved, EU institutions keep their ambition to remain "the global gold standard in the protection of personal data", even feigning to anticipate foreseeable impacts of ICT on this matter[3]. Yet, notwithstanding the confident discourse of EU institutions, a closer examination of the current reform raises scepticism about its ability to safeguard data protection principles and rights effectively in the face of evolving data processing techniques such as those underlying "big data".

One might wonder, however, whether these uncertainties should be attributed to a specific difficulty of the law to cope with technological progresses or rather to the policy choices embedded in the novel General Data Protection Regulation (GDPR) itself.

In this article, we will examine key features of the evolving data protection legislation in the light of implications of big data technologies. We will then address the novel regulatory approaches introduced by the GDPR, relying on risk assessment and management and on self-regulation, and seek to understand them in the light of a "law-technology lag" versus a "law-technology driving" perspective, meaning a policy whereby law is deliberately used as a means to foster technological innovation.

2. The data protection reform and big data technologies

As we write, the General Data Protection Regulation (GDPR) put forward by the European Commission (EC) in January 2012[4] has been approved following five years of intense negotiations (De Hert, Papakonstantinou, 2016)[5].

---

[1] The European Community, now the European Union (EU), has played a pioneering role in the legal regulation of ICT uses since the 1990s. European institutions did respond promptly to technological advances when adopting the directives on the legal protection of computer programmes (1991, revised in 2009), on the legal protection of databases (1996) or on e-commerce (2000), for example.

[2] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[3] "By the 10th European Data Protection Day, we are confident that we will be able to say that the EU remains the global gold standard in the protection of personal data". European Commission Statement, "Vice-President Ansip and Commissioner Jourová: Concluding the EU Data Protection Reform is essential for the Digital Single Market", Brussels, 28 January 2015, <http://europa.eu/rapid/press-release_STATEMENT-15-3801_en.htm> (last accessed 18.03.2016).

[4] Proposal for a Regulation of the European Parliament and 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, 25.01.2012.

[5] Following political agreement reached in trilogue in December 2015, on 8 April 2016, the Council adopted its position at first reading, which paves the way for the final adoption by the European Parliament at its plenary session in April. The regulation is likely to enter into force in spring 2016 to be applicable as of Spring 2018. http://www.consilium.europa.eu/en/policies/data-protection-reform/data-protection-regulation/ (last

Personal data protection has been frequently portrayed as a distinctive European legal innovation, its principles being held up as a standard for best data protection practices (Borghi, Ferretti, Karapapa, 2013, p. 109). In 2010, the EU moved even a step further with the adoption of the Charter of Fundamental Rights as part of the Treaty of Lisbon, upgrading the right to personal data protection to the status of a fundamental right.

The origins of personal data protection go back to the late 1960s and to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, of 1981 (Convention 108). The Convention was gifted with principles that keep being key to the protection of personal data, and came to shape Directive 95/46/EC, the Data Protection Directive (DPD). These principles, to be observed by the data controllers and processors, are, specifically: purpose limitation (ie personal data may only be collected for specified, explicit and legitimate purposes and may not be further processed in a way incompatible with those purposes); data minimization (ie processing of personal data must be restricted to the minimum amount necessary); proportionality (ie personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected); and control (ie supervision of processing must be ensured by member states' authorities). Also, the data subjects are assigned a set of procedural rights enabling them to consent, to have access, and to know what information about them is registered in databases, as well as to rectify the data, and to oppose to data processing in specific situations. In addition, the DPD prohibits the transfer of personal data to third countries unless the latter provide an adequate level of data protection as determined by the European Commission, or unless one of the enumerated exceptions applies.

Both the Convention and the DPD were designed having in mind the computer systems of large organizations, either public or private, to the extent that they collect, store and process personal data for the purposes of their own activities. The DPD, in particular, was drawn up as part of the legal framing of the common market, meaning that data protection law was mainly targeted towards private companies at a time when these companies were not yet engaged into massive data mining. Besides, although adopted in an age when the Internet was already widely known among the technology community and was starting to make its way into households, the DPD did not depict a specific concern regarding the use of the Web, rendering it to naturally lag behind technology from the moment of its enactment, even though some extensive interpretation has been made throughout the years, in order to accommodate the special features of the online environment[6].

accessed 09.04.2016). The consolidated version is available at <https://www.janalbrecht.eu/fileadmin/material/Dokumente/GDPR_consolidated_LIBE-vote-2015-12-17.pdf> (last accessed 18.03.2016).

[6] In 2003, a decision by the European Court of Justice (ECJ) in the Bodil Lindqvist case helped to clarify the applicability of Directive 95/46/EC to the Internet in the specific circumstances in which someone processes and diffuses sensitive personal data of other people on an Internet page. In this instance, the Court considered that the publication of personal data online made the said information available to a countless number of recipients, thus rendering the personal/household exemption prescribed by the article 3 (2) of the DPD not applicable (Warso, 2013, p. 493 ff).

Thus, it is not hard to infer that the increasing amount of sophisticated content and services that emerged throughout the years have rendered this inability more obvious. Even so, one had to wait for 2010 to see the EC recognise the impact of the Internet on this matter. In its Communication on a comprehensive approach to the protection of personal data in the EU, the EC acknowledged the problems raised by the current easiness with which personal data are shared and publicised in social networks together with the increasing capacities for information retrieval in remote servers in the "cloud"[7].

Yet, the atmosphere surrounding the launching of the EC's proposal for a GDPR, in January 2012, looked rather optimistic. The European Data Protection Supervisor (EDPS) welcomed the proposal as a huge step forward for data protection in Europe, robust enough to face future information technology-driven challenges[8]. Likewise, for the Article 29 Data Protection Working Party[9], the proposed regulation fulfilled the ambition to produce a text that reflected the increased importance of data protection in the EU legal order. It retained and strengthened the core principles of data protection, reinforced the position of the data subjects, enhanced the responsibility of data controllers and strengthened the position of supervisory authorities, both nationally and internationally[10]. The suitability of the proposals to "address the new challenges resulting from the pervasive collection and use of personal data in a connected and globalized world" was recognised by the European Data Protection Commissioners in their Resolution on the EU data protection reform adopted at the Spring Conference 2012[11]. Several commentators also saluted the draft regulation for allegedly providing the data subjects with stronger rights, including giving more power to customers of online services and stronger safeguards for EU citizens' data that get transmitted abroad (De Hert, Papakonstantinou, 2012, p. 135; Tene, Polonetsky, 2012, p. 63 ff).

One might, however, doubt whether these beliefs are fully justified since they seem to reveal a somehow perplexing neglect of the challenges arising for data protection principles and rights from the growing availability of large datasets and sophisticated tools in data mining and data analytics, together with the access by surveillance authorities to personal data collected by service providers on the base of their privacy policies for their specific purposes, something that the Snowden affair rendered widely notorious (Mantelero, Vaciago, 2013, p. 161-162).

---

[7] European Commission, Communication of the Commission to the European Parliament, The Council, The Economics and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union, COM (2010) 609 final, Brussels, 4.11.2010.
Available at <http://ec.europa.eu/health/data_collection/docs/com_2010_0609_en.pdf> (last accessed 18.03.2016).

[8] European Data Protection Supervisor, 2012 Annual Report: Smart, sustainable, inclusive Europe: only with stronger and more effective data protection, Publications Office of the European Union, 2013, p. 50.

[9] The Article 29 Data Protection Working Party is an independent committee created by Article 29 of the data protection directive (hence its designation), with advisory functions to the European Commission.

[10] Article 29 Data Protection Working Party, Opinion 01/2012 on the Data Protection Reform Proposals, 23 March 2012, p. 4-5. Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf > (last accessed 18.03.2016).

[11] Resolution on the EU data protection reform adopted at the Spring Conference 2012, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_EU/12-05-04_Spring_conference_Resolution_EN.pdf.

To tell the truth, the prospects of the EU data protection reform have not been entirely uncontroversial. Reservations have been voiced that data protection laws can be "practically enforced in the transnational, borderless, information-dense world the internet has now created" (Danagher, 2012). Specifically, while the option for a regulation to replace the DPD was greeted as a progress in harmonization within the EU[12], doubts were expressed that a separate legal instrument, the proposed Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offenses or the Execution of Criminal Penalties, and the Free Movement of Such Data (so-called "law enforcement" or "police directive")[13] has been chosen to rule the processing of personal data in the police and judicial sectors with a much lower level of protection (Gonçalves, Jesus, 2013, p. 255 ff)[14]. Two major arguments were advanced in this respect. Firstly, a single EU legal instrument, preferably a regulation, would have been more appropriate for the fundamental right to personal data protection to be fulfilled, since it would give more guarantees to citizens (Blas, 2009, p. 225 ff)[15]. Secondly, in opting to address data protection in the security realm by the means of a special regime, and a directive instead of a regulation, the EC contradicted the comprehensive approach of its Communication, which had paved the way for the reform[16]. Indeed, the importance of a unified regime in this domain looks clearer in the present big data age.

Big data has been defined as "large, diverse, complex, longitudinal, and/or distributed datasets generated from instruments, sensors, Internet transactions, email, video, click streams and/or all other digital sources available today and in the future."

---

[12] "The EDPS supports the proposal because it is based on the correct choice of legal instrument, a regulation." European Data Protection Supervisor, 2012 Annual Report: Smart, sustainable, inclusive Europe: only with stronger and more effective data protection, Publications Office of the European Union, 2013, 50. See also European Data Protection Supervisor, Opinion on Data Protection Reform Package, 7 March 2012, p. 7-8. Available at:
<https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf> (last accessed 18.03.2016).

[13] Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offenses or the Execution of Criminal Penalties, and the Free Movement of Such Data, COM (2012) 10 final, 25th January 2012. See the Council's compromise text, of 2 October 2015. Available at <http://data.consilium.europa.eu/doc/document/ST-12555-2015-INIT/en/pdf> (last accessed 18.03.2016).

[14] Article 29 Data Protection Working Party, Opinion 01/2012 on the Data Protection Reform Proposals, 23 March 2012, p. 4. Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf>; European Data Protection Supervisor, 2012 Annual Report…, p. 16.

[15].In the view of the EDPS, for example, "In the area of data protection a Regulation is all the more justified, since Article 16 TFEU has upgraded the right to the protection of personal data to the Treaty level and envisages or even mandates a uniform level of protection of individual throughout the EU." European Data Protection Supervisor, Opinion on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: 'A Comprehensive Approach on Personal Data Protection in the European Union', p. 9, 11-26.

[16] Communication to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions: "Delivering an Area of Freedom, Security and Justice for Europe's Citizens, Action Plan Implementing the Stockholm Programme", COM (2010) 171 final, 20.4.2010, p. 3.

(National Science Foundation, 2012)[17] Big data relies on the increasing ability of technology to support the collection and storage of large amounts of data, and on its ability to enable analysis, understanding and taking advantage of the full value of data using sophisticated algorithms (The White House, 2014).

Promising fields for big data technologies range from health to intelligent transport systems and smart cities, from social research on human and group behaviour to models of economic growth (Allemand, 2013, p. 27 ff). The other side of the coin is the growing use of big data for consumer profiling and, more than that, for purposes of surveillance and control. One of the greatest values of big data for businesses and governments is derived from the monitoring of human behaviour and resides in its predictive potential, entailing the emergence of a revenue model for Internet companies relying on tracking online activity. Such "big data" should be considered personal even where anonymisation techniques have been applied since it is widely admitted that it is relatively easy to infer a person's identity by combining allegedly anonymous data with publicly available information such as on social media. These may include highly sensitive data such as health data and information relating to our thinking patterns and psychological make-up[18].

All in all, notwithstanding the improvements that big data may bring about to the performance of both commercial and public services, a true apprehension arises that this new paradigm may considerably alter the balances of power with respect to personal data appropriation and control with adverse effects upon the effectiveness of data protection principles and rights.

3. Changing power balances in data control, and how the data protection regime responds

On the European Data Protection Day, 28th January 2015, Vice-President Andrus Ansip and Commissioner Věra Jourová underlined that "citizens and businesses are waiting for the modernisation of data protection rules to catch up with the digital age". The Commissioners reaffirmed their faith in the new data protection rules to "strengthen citizens' rights" and "put citizens back in control of their data"[19]. They also recalled, the "EU Data Protection reform also includes new rules for police and criminal justice authorities when they exchange data across the EU. This is very timely, not least in light of the recent terrorist attacks in Paris".

As the EU approves the GDPR, and the law enforcement directive, the belief thus persists in the ability of this reform to cope with technological progresses. Likewise, EU leaders underline the aptitude of the reform to conciliate economic

[17] Article 29 Working Party (WP29) Opinion 3/2013 on purpose limitation. European Data Prot4ection Supervisor, Opinion 7/2015, Meeting the challenges of big data, November, p. 7.
[18] European Data Protection Supervisor, Opinion 7/2015, Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability, 19 November, 7.
[19] European Fact Sheet, Data Protection Day 2015: Concluding the EU Data Protection Reform essential for the Digital Single Market, Brussels, 28 January 2015, <http://europa.eu/rapid/press-release_MEMO-15-3802_en.htm> (last accessed 18.03.2016).

competitiveness with the rights of the data subjects. "Today's agreement is a major step towards a Digital Single Market. With solid common standards for data protection, people can be sure they are in control of their personal information. We should not see privacy and data protection as holding back economic activities. They are, in fact, an essential competitive advantage", the Vice-President for the Digital Single Market affirmed[20].

It is worth recalling that, from the outset, in line with the objectives of the European Internal Market, the DPD sought to reconcile the protection of personal data (and the inherent right to privacy) with "the free movement of data" (to use the DPD's wording). In reality, the DPD can be regarded as a step in a route whereby data protection principles and rights have been gradually rendered more flexible and open to exceptions. The DPD includes a catalogue of exceptions to the data protection principles, not found in the Council of Europe's Convention of 1981, and largely justified by the DPD's intent not to raise unjustified obstacles to the free movement of the data. This is especially clear in the case of the principle of consent[21]. Article 7 (b) to (f) DPD ultimately allows the processing of personal data on almost any ground, a door opened by exceptions provided by law to the "legitimate interests pursued by the controller". The only criterion offered for assessing the legitimacy of the interests is a balance between them and the "interests and fundamental rights and freedoms" of the data subject, which is quite an evasive criterion. The balancing test is left to a case-by-case determination by the data controllers themselves, without any specific guidance (Zanfir, 2014, p. 237 ff)[22]. This criterion is retaken in the GDPR[23].

In fact, the legitimate interest clause is the criterion upon which the majority of personal data processing takes place (Le Métayer, Monteleone, 2009, p. 136). Now, the way consent is devised seemingly provides a weaker protection for individuals, in the big data age, in the face of the wider power and autonomy of online operators to collect, process and apply personal data, as well as to judge, in the first instance, on how to balance their own interest and the rights to data protection[24]. Moreover, one may reasonably doubt that data controllers have the necessary competency to undertake such a balancing test apart from being in a position of clear conflict of interest (Ferretti, 2012, p. 473). For instance, Google does not collect the unambiguous consent of data subjects and it relies on its legitimate interest to provide and improve services, develop new ones, and protect itself and its users. If broadly

[20] http://europa.eu/rapid/press-release_IP-15-6321_en.htm (last accessed 18.03.2016).

[21] Articles 2 (c) and 7 (a) DPD; Article 4 (8) GDPR. According to Article 7 DPD, personal data may be processed only if the data subject has unambiguously given his consent, or processing is necessary for the performance of a contract to which the data subject is party, for compliance with a legal obligation to which the controller is subject, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

[22] Article 29 Data Protection Working Party, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC. Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> (last accessed 18.03.2016).

[23] Article 6 (1) (f) GDPR.

[24] "Google and Facebook now have far more power over the privacy and free speech of most citizens than any king, president, or Supreme Court justice could hope for." (Rosen, 2012, p. 1525 ff). See infra, section 4.

interpreted, Google's justification concerns an interest in itself allowed by the law[25]. Yet, in a letter of the Working Party, Google was portrayed as not having demonstrated that it endorsed the key data protection principles, with Google's privacy policy signifying the absence of any limit concerning the scope of the collection and the potential uses of the personal data[26]. Maybe on account of the purely persuasive nature of the method used, a letter, Google did not appear too much troubled by the concerns expressed by the Working Party. This led to other data protection authorities legally engaging Google, which has only lately committed with the UK's Information Commissioner's Office (ICO) to reform its views as far as their (unified) privacy policy goes[27].

It is easy to infer that technologies using or, more precisely, re-using larger data sets obtained from diverse unrelated sources, and automatically processed to an extent not dreamed of when the first data protection laws were adopted, render the obtaining of consent more difficult to put into practice (Tene, 2011, p. 273; De Hert, Papakonstantinou, 2016). Big data also challenges the principles of purpose limitation, and of relevance and accuracy of the data since it relies on data collected from diverse sources, and without careful verification[28]. Moreover, although it is foreseen that data processing will be subject to supervision, enforcement and judiciary control (Art. 22 GDPR), reasonable doubts surface as to the effectiveness of these forms of control in the big data age (Lynskey, 2015, p. 273).

As the EDPS itself admitted, "new business models exploiting new capabilities for the massive collection, instantaneous transmission, combination and reuse of personal information for unforeseen purposes have placed the principles of data protection under new strains"[29]. The automatisation inherent to data mining renders the human choice at the stage of data collection rather illusive (Colonna, 2014, p. 299 ff). Besides, individuals can hardly exercise control over their data and provide meaningful consent in cases where such consent is required. This is all the more so as the precise future purposes of any secondary use of the data may not be known when data is obtained, undermining purpose limitation as well. Moreover, controllers may be unable or even reluctant to tell individuals what is likely to happen to their data and to obtain their consent when required[30].

A critical issue actually is the blurring of the public-private information frontier

[25] However, the Article 29 Data Protection Working Party argued that additional guidance is needed in order to have a common understanding of the very concept of legitimate interest. (Article 29 Data Protection Working Party, Opinion 03/2013 on Purpose Limitation, adopted on 2nd April 2013. Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf >).

[26] Article 29 Data Protection Working Party, Letter from the Article 29 Data Protection Working Party addressed to Google along with the recommendations (Brussels, 16 Oct. 2012). Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20121016_letter_to_google_en.pdf> (last accessed 18.03.2016).

[27] Information Commissioner's Office (ICO), Google to change privacy policy after ICO investigation, 30th January 2015. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/01/google-to-change-privacy-policy-after-ico-investigation/ (last accessed: 18.03.2016).

[28] European Data Protection Supervisor (2015), Opinion 7/2015, p. 8.

[29] European Data Protection Supervisor, Opinion 7/2015, p. 3.

[30] Article 29 Data Protection Working Party, Opinion 03/2013 on Purpose Limitation.

(Lyon, 2010, p. 15). In its review of surveillance practices following the Snowden affair, the European Parliament inferred that the current programmes enhanced by technological progress represent a reconfiguration of traditional intelligence, enabling access to a much larger scale of platforms for data extraction than telecommunications surveillance of the past, thus entailing a change in the very nature of these operations. In the United States of America, the NSA has been at the forefront of efforts to collect and analyse massive amounts of data through its PRISM Program, and a variety of other data-intensive programs, whose capabilities are likely to expand (Schmitt, *et al.*, 2013). Similar developments are under way in Europe. The recently adopted French "Loi sur le Renseignement" provides an additional illustration of this trend by governments to resort to mass surveillance through advanced techniques of information retrieval of huge sets of metadata[31].

Even if not fully expressed in the recent ruling of the Court of Justice of the EU on the validity of the Safe Harbour agreement between the EC and the USA government, Google and Facebook are not only private data miners, but also data miners that are in a very close relationship to US national security, although not necessarily to EU national security[32]. In effect, the collaborative model of big companies and public authorities is not only based on mandatory disclosure orders issued by courts or administrative bodies, but also on an indefinite grey area of voluntary and proactive collaboration furthered by technological opportunities[33]. The "collect-everything approach" applied to monitoring and intelligence definitively connects mass surveillance to big data[34].

These developments signal that EU law making regarding personal data protection is not easily keeping pace with the especially delicate defies of big data. Yet, strikingly, the EC keeps maintaining that the core principles of the DPD are still valid and "its technologically neutral character should be preserved"[35]. Such a belief in technology neutrality looks puzzling. Indeed, technology neutrality means that the same regulatory principles should apply regardless of the technology used (Maxwell, Bourreau, 2014). Yet, the functionalities of big data technologies represent a leap through in ICT. In these circumstances, it may not be sufficient to simply adapt the law.

While data mining and data analytics are as such not new practices, the scale of

---

[31] See the final version of this law at http://www.assemblee-nationale.fr/14/ta/ta0542.asp.

[32] Judgment of the Court (Grand Chamber) of 6 October 2015 (request for a preliminary ruling from the High Court (Ireland)) — Maximillian Schrems v Data Protection Commissioner (Case C-362/14), <http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d567a327f531c448e985d7b20aa2584baa.e34KaxiLc3eQc40LaxqMbN4Och4Se0?text=&docid=172254&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=185134> (last accessed 18.03.2016).

[33] So the concept of "total surveillance" has been put forward to qualify the way such large-scale processes of strategic management relying on big data operate today. (Couldry,. Powell 2013, 1-5; Abdo, Toomey, 2013; Andrejevic, Gates, 2014185-196).

[34] Fears have been expressed that these data, collected for fighting terrorism and crime, are used also for tax evasion, for advantaging some private companies in their contracts and for profiling the political opinions of groups considered as suspect.

[35] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union, COM (2010) 609 final, Brussels, 4.11.2010, p. 3. Whereas 13 of GDPR (Final version).

data collection, tracking and profiling allowed by the growing capacities of technologies portray the big data phenomenon as a defining moment in ICT uses and their aftermaths for both individuals and society.

> Definitely, the spread of big data is changing the relationship between a person and the data about him or her, as the notion that data protection is designed to empower the individual by giving him/her rights to control the processing of his/her data looks growingly illusory (Colonna, 2014, p. 299).

These developments look especially problematic in view of the upgrading of data protection to the rank of a fundamental right by the Treaty of Lisbon (Article 16 of the Treaty on the Functioning of the European Union) and the Charter of Fundamental Rights (Article 8). This move opened up the expectation that the balancing of the right to personal data protection with market freedoms would lean towards the former by the means of heavier constrains on rights restrictions (Gonçalves, Gameiro, 2014, p. 21 ff). Indeed, current trends in personal data uses increase the imbalance between large corporations and consumers, the Article 29 Data Protection Working Party admitted[36]. What's more, the GDPR itself endorses the move towards personal data appropriation and control by the operators by means of risk-based approaches and self-regulation, as it will be shown below.

At the end of the day, the issue is, how legislation could be possibly construed so as to respond more adequately to the challenges for data protection.

4. The turn to risk-based and self-regulatory approaches

At the end of the day, the recognition of the difficulty to apply key data protection principles to the big data context, although not openly assumed, may explain the leaning of the EU legislator on alleged "more realistic" approaches to protect personal data, i.e. risk-based and self-regulatory approaches (Zanfir, 2014, p. 237 ff; Lynskey, 2015, p. 81 ff).

Let's recall some major innovations have been introduced by the GDPR in this direction, *i.e.*: the data protection impact assessment; the prevention of ex-post misuse of data through prompt notification of data breaches; and the "right to be forgotten"[37].

Let's start with Article 33 GDPR's command that data controllers and processors carry out a data protection impact assessment "prior to risky processing operations". The data protection assessment procedure looks instrumental to the implementation of technical and organisational measures that the data controllers are due to apply in order to comply with the GDPR, and be able to demonstrate it (so-called privacy by design and privacy by default) (Articles 22 and 23). In so doing, the data controllers are due to have regard not only of the state of the art of technologies, but also of the cost of implementation (Article 23), which may actually widen the

[36] Article 29 Data Protection Working Party, Opinion 03/2013 on Purpose Limitation.
[37] Recital 53 and Article 17 GDPR.

margin of autonomy of the controller to choose the means to protect the data. This impact assessment is required, according to the Regulation, only when data processing presents "specific risks" for individual rights and freedoms, such as those involving certain sensitive information or a systematic and extensive evaluation or prediction of personal aspects relating to a natural person, which is based on automated processing, and on which measures are based that produce legal effects or significantly affect the individual[38]. To fulfil this duty the controller itself is expected to evaluate the likelihood and severity of risks for individual rights in the light of the nature, the scope, the context and the purposes of the processing.

Personal data breaches, the GDPR also acknowledges, may entail potentially severe damages to the rights of individuals. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should without undue delay notify the breach to the competent supervisory authority, as well as the data subject, unless the controller is able to demonstrate that the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals (Articles 31 and 32)[39].

Lastly, the "right to be forgotten" allows data subjects to request that search engines remove links to pages deemed private, even if the pages themselves remain on the Internet. This novel right has been justified by the need to protect the individual's autonomy to decide what aspects of his/her life are to be kept in a private or public domain (Mantelero, 2013, p. 230). In its decision on Case C-131/12 (Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González) the European Court of Justice clarified that search engines like Google could not escape their responsibilities before EU law when handling personal data[40]. The Court recognised that when the processing of personal data is carried out by a search engine, it may have a greater impact on an individual's right to data protection as it enables a more detailed and organized gathering of information on said individual, while making it more easily accessible. The Court further elucidated that individuals have the right, under certain conditions, to request search engines to remove links leading to information about them (paragraph 93 of the ruling). The Court, however, made it clear that this right is not absolute and needs to be balanced against other fundamental rights, namely the freedom of expression (paragraph 85 of the ruling). A case-by-case assessment is, thus, required whereby the type of information in question, its sensitivity for the individual's private life and the interest of the public in having access to that information, are pondered (Mantelero, 2013, p. 232-233). The Court left no doubt, in its decision, that it is up to Google to assess deletion requests and to apply the criteria mentioned in EU law and the Court's judgment. As a result, a major power is being assigned to Google and, inherently, to other data controllers, to determine whether to delete or keep specific information online, one that may only be controlled ex-post, and under complaint, by national

[38] Whereas 66a GDPR.
[39] Whereas 67 and Whereas 67a new GDPR.
[40] Case C-131/12, Google Spain SL, Google Inc. *v.* Agencia Española de Protección de Datos (AEPD), Mario Costeja González (2014) ECR. Available at: <http://curia.europa.eu/juris/liste.jsf?num=C-131/12> (last accessed 18.03.2016).

supervisory authorities or national courts[41]. This indeed makes it seem as if the right is being "privatised"[42].

Though the right to be forgotten may no doubt contribute to enabling individuals to defend their privacy (and, by the same token, their reputation and, ultimately, dignity), it hardly responds to the challenges of big data with their pervasiveness and actual lack of transparency. In reality, it can be said that, requiring a pre-existent data subject's request to exercise his/her rights, spares a great deal of effort to the operators helping to pave the way for the massive gathering of information enabled by big data mining. Moreover, the supervisory authorities are expected to intervene merely afterward, following denial of the subject's appeal by the operator of the search engine[43].

The above overview renders the reliance of the new data protection regime on self-regulation fairly clear. Efficiency considerations underlay the move towards a risk-based approach to data protection (Lynskey, 2015, p. 84). Definitely, the strengthening of autonomy and control by operators over the processing of personal data, including for the assessment of the risks arising therefrom for the rights and freedoms of data subjects may be understood in connection with the EU legislator's explicit intent, when revising the DPD, to reduce administrative burdens on the operators by substituting the obligation of notification of data processing and the preliminary control by the data protection authority, decreed by the DPD, with measures to be carried out by the controllers themselves[44]. The Vice-President of the EC stated in this connection, "This reform will greatly simplify the regulatory environment and will substantially reduce the administrative burden. We need to drastically cut red tape, do away with all the notification obligations and requirements that are excessively bureaucratic, unnecessary and ineffective[45]. Such "indiscriminate general notification obligations" "did not in all cases contribute to improving the protection of personal data" and should therefore be abolished. This is an odd argument, though, considering that data protection authorities have commonly been judged as having been up to their supervisory responsibilities (European Union Agency for Fundamental Rights, 2010). Moreover, the assumption that risk-based approaches and self-regulation promise to be more effective than public control under the DPD appears, at this stage, little more than wishful thinking[46].

---

[41] Following the Court's ruling, other search engines, such as Bing, have also made available "right to be forgotten" forms for European users (Gerry Berova, 2014, p. 478; Ribeiro, 2014).

[42] On account of the potentially harmful ambiguity of this decision, the Article 29 Data Protection Working Party issued guidelines setting non-exhaustive criteria to be followed by the supervisory authorities when search engines deny a subject's request to remove certain links to information affecting their privacy. (Article 29 Data Protection Working Party, "Guidelines on the implementation of the Court of Justice of the European Union Judgment on 'Google Spain and Inc V. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12", adopted on 26 November 2014, p. 3. Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf)> (last accessed 18.03.2016).

[43] Article 29 Data Protection Working Party, Guidelines…, p. 11-12.

[44] Whereas 70 GDPR.

[45] Viviane Reding, at BBA (British Bankers' Association) Data Protection and Privacy Conference, London, 20 June 2011.

[46] Whereas 70 GDPR.

The EDPS itself recognised, remitting monitoring of compliance predominantly to self-control does not shield against the risk of core principles of data protection being compromised, since it is often a challenging task to decide what is fair and lawful and what is not when it comes to big data analytics[47]. Plus, risks to human rights and freedoms envisaged under the data protection framework remain largely undefined, and further clarification looks especially hard in view of the objective and subjective, tangible and intangible factors involved (Lynskey, 2015, p. 83).

In the end, the key issue resides in leaving the main judgements about how to protect the personal data to the major, mainly private online operators. All things considered, one may doubt that this does not contradict the essential nature of the fundamental right to data protection and the inherent public responsibilities. Indeed, upgrading personal data protection to the rank of a fundamental right, as did the Treaty of Lisbon and the Charter of Fundamental Rights (Article 8), should be regarded as more than a symbolic move. Accordingly, the Charter has been regarded as an effort to make human rights "determine" rather than merely "limit" a EU legal system predominantly designed to guarantee market freedoms (Von Bodgandy, 2000, p. 1321). The issue ultimately is whether the difficulty to render consent and purpose limitation (not to speak of data minimisation) effective in the face of big data applications should not have given rise to an alternative regulatory path, one that better conciliates greater responsibility and accountability of data controllers with reinforcement of the basic data protection principles, including that the basic data protection rules continue to be "subject to control by an independent authority". This could be done by the means, in particular, of more transparency about how operators and data controllers process personal data, hence, facilitating rights' enforcement. A recent opinion by the EDPS provides pertinent propositions in this direction[48].

Indeed, transparency of automated decisions is taking an increasingly important role with the advent of big data. Big data is based not only on information that individuals knowingly give to organisations, but also on data observed or inferred. Based on such considerations, the EDPS explicitly recommended that "the provisions of the proposed EU Data Protection Regulation on transparency be reinforced" and "a new generation of user control" implying "powerful rights of access" and "effective opt-out mechanisms" be furthered. This should amount to broadening the scope of consent by better informing the data subjects about what data is processed about them and for what purposes, including disclosure of the logic used in algorithms to determine assumptions and predictions"[49]. Remarkably, the EDPS does not conceal its incredulity regarding the effectiveness of the right to object to processing since it is "not frequently exercised in today's practice", thus calling for

[47] European Data Protection Supervisor, Opinion 7/2015, p. 8. Some of the key decisions an accountable organisation must make under European data protection law require a comprehensive balancing exercise and consideration of many factors, including whether the data processing meets the reasonable expectations of the individuals concerned, whether it may lead to unfair discrimination or may have any other negative impact on the individuals concerned or on society as a whole. These assessments cannot be reduced to a simple and mechanical exercise of ticking off compliance boxes, the EDPS alerts.

[48] European Data Protection Supervisor, Opinion 7/2015, p. 4, 8-9 ff.

[49] European Data Protection Supervisor, Opinion 7/2015, p. 10.

specific efforts by operators to render this right more effective and "easy to exercise"[50].

In sum, increased transparency, more powerful rights of access, and effective opt-out mechanisms, together with strengthened powers of supervisory authorities[51] feature preconditions to allow users' control over their data in the big data context. Yet, so far, these views seem to have hardly been incorporated into the new data protection regime.

Against this background, it is legitimate to infer that the policy options embedded in the GDPR offer better explanations for the prominence of self-regulatory approaches than technological change alone. As happened with other ICT as they emerged, the EU legislator has not really explored all possible means to protect the fundamental rights and values threatened by big data technologies (Gonçalves, Gameiro, 2012, p. 320 ff).

5. Conclusion

The current data protection reform seemingly fails to cope with the dynamics of big data technologies, and to provide the appropriate caution that should be expected from a law designed to protect a fundamental human right. Notwithstanding the ambition of the novel regulation, the decision-making power on what and how to collect, store, process and apply personal information is turning to the operators and data controllers to the disadvantage of data subjects and supervisory authorities. Technological conditions, namely the automatisation inherent to data mining and data analytics, render the effectiveness of key data protection principles harder to pursue. But it is also true that the suppleness of the regime is being boosted by the Regulation's own emphasis on self-regulatory modes.

To a certain extent, this trend follows up from the legitimate interest exception and the compatibility assessment requirement upon which the EU data protection regime has relied since its inception. Today, however, the big data context paves the way for an ampler margin for the operators to summon their legitimate interest and avoid the consent of the data subjects. The GDPR's leaning towards self-regulatory approaches relying on risk assessment and management and notification of breaches, as well as on self-defense by Internet users, seemingly guided by the intent not to impair technological innovation and competitiveness in the Digital Single Market, ends up favouring the movement of personal data to the detriment of the rights of the data subjects. So, rather than a specific difficulty of EU law to cope with technological progresses in the ICT domain, the preference for self-regulatory approaches to personal data protection may be better accounted for by the inherent policy choices. Though somehow paradoxically, the novel EU data protection regime thus seems to being used as an indirect means of driving technological innovation.

[50] European Data Protection Supervisor, Opinion 7/2015, p. 11.
[51] European Data Protection Supervisor, Opinion 7/2015, p. 17.

Meeting the big data challenges more effectively requires exploring complementary regulatory approaches focusing on the reuses of personal information, something that the GDPR does not address unambiguously[52]. Likewise, more could be done to strengthen transparency and user control, along the lines of the recent recommendations of the EDPS. Finally, despite the latest approval of the GDPR and of the "law enforcement directive" as separate instruments, considering their merging should not be disregarded definitively. Notwithstanding the former's weaknesses, it still provides a stronger framework than the latter, and a more accurate response to the growing private-public exchange of personal data.

References

Abdo, A.; Toomey, P. (2013), The NSA is turning the internet into a total surveillance system, *The Guardian*, 11.08.2013. <http://www.theguardian.com/commentisfree/2013/aug/11/nsa-internet-surveillance-email>.

Allemand, L. (2013), Dossier: les promesses du big data, December, *La Recherche* 482, p. 27-42.

Andrejevic, M.; Gates, K. (2014), Editorial: big data surveillance: introduction, *Surveillance & Society* 12 (2), p. 185-196.

Blas, D. A. (2009), First pillar and third pillar: need for a common approach on data protection?, in S. Gutwirth, *et al.*, ed., *Reinventing Data Protection?*, Springer, p. 225-237.

Borghi, M.; Ferretti, F; Karapapa, S. (2013), Online data processing consent under EU law: a theoretical framework and empirical evidence from the UK, *International Journal of Law and Information Technology* 21 (2), p. 109-153.

Colonna, L. (2014), Data mining and its paradoxical relationship to the purpose of limitation principle. In Gurwitch, S; Leenes, R.; De Hert, P., ed., *Reloading Data protection: multidisciplinary insights and contemporary challenges,* Springer, p. 299--321.

Couldry, N.; Powell, A. (2013), Big data from the bottom up, *Big Data & Society*, July-December, p. 1-5.

Danagher, L. (2012), An Assessment of the draft data protection regulation: does it effectively protect data?, *European Journal of Law and Technology* 3 (3), <http://ejlt.org/article/view/171/260>.

De Hert, P.; Papakonstantinou, V. (2016), The New general data protection

[52] "A privacy doctrine built for the cyber age must address a radical change in the type and scale of violations that the nation—and the world—face, namely that the greatest threats to privacy come not at the point that personal information is collected, but rather from the secondary uses of such information" (Etzioni, 2013, p. 641 ff.) Accordingly, and bearing in mind the diversity of big data applications, a distinction should be held on whether the data processing seeks to simply detect trends and correlations or focuses on individuals.

regulation: still a sound system for the protection of individuals?, *Computer Law & Security Review*, doi: 10.1016/j.clsr.2016.02.006.

De Hert, P.; Papakonstantinou, V. (2012), The Proposed data protection regulation replacing Dir 95/46/EC: a sound system for the protection of individuals, *Computer Law & Security Review* 28 (2), p. 130-142.

Etzioni, A. (2013), A Cyber age privacy doctrine: a liberal communitarian approach, *I/S: A Journal of Law and Policy* 10 (2), < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2348117>.

European Union Agency for Fundamental Rights (2010), *Data Protection in the European Union: the role of national data protection authorities*, Luxembourg: Publications Office of the European Union.

Ferretti, F. (2012), A European perspective on data processing consent through the re-conceptualization of European data protection's looking glass after the Lisbon Treaty: taking rights seriously, *European Review of Private Law* 2, p. 473-506.

Gerry Q. C F.; Berova, N. (2014), The Rule of law online: treating data like the sale of goods: lessons for the Internet from OECD and CISG and sacking Google as the regulator, *Computer Law & Security Review* 30 (5), p. 465-481.

Gonçalves, M. E.; Jesus, I. A. (2013), Security policies and the weakening of personal data protection in the European Union, *Computer Law & Security Review* 29 (3), p. 255-263.

Gonçalves, M. E.; Gameiro, M. I. (2014), Does the centrality of values in the Lisbon Treaty promise more than it can actually offer?: Biometrics as a case study, *European Law Journal* 20 (1), p. 21-33.

Gonçalves, M.E.; Gameiro, M. I. (2012), Security, privacy and freedom, and the EU legal and policy framework for biometrics, *Computer Law & Security Review* 28 (3), p. 320-327.

Le Métayer, D.; Monteleone, S. (2009), Automated consent through privacy agents: Llegal requirements and technical architecture, *Computer Law & Security Review* 25 (2), 136-144.

Lynskey, O. (2015), *The Foundations of EU data protection law*, Oxford: Oxford University Press.

Lyon, D. (2010), Liquid surveillance: the contribution of Zygmunt Bauman to surveillance studies, *International Political Sociology* 4, p. 325-338.

Mantelero, A. (2013), The EU proposal for a General Data Protection Regulation and the roots of the "right to be forgotten", *Computer Law and Security Review* 29 (3), p. 229-235.

Mantelero, A.; Vaciago, G. (2013), The "Dark side" of Big Data: private and public interaction in social surveillance: how data collections by private entities affect governmental social control and how the EU reform on data protection responds, *Computer Review International* (6), p. 161-169.

Maxwell, W.; Bourreau, M. (2014), Technology neutrality in Internet, telecoms and data protection regulation', *Hogan Lovells Global Media and Communications Quarterly*. <http://www.hoganlovells.com/files/Uploads/Documents/8%20Technology%20neutrality%20in%20Internet.pdf>.

Moses, L. Bennett (2007), *Recurring dilemmas: the law's race to keep up with technological change* (April 11, 2007). UNSW Law Research Paper No. 2007-21. <SSRN: http://ssrn.com/abstract=979861 orhttp://dx.doi.org/10.2139/ssrn.979861>

National Science Foundation (2012), *Solicitation 12-499: Core techniques and technologies for advancing big data Science & Engineering (BIGDATA)*, <http://www.nsf.gov/pubs/2012/nsf12499/nsf12499.pdf>.

Reidenberg, J. (2014), The Data surveillance state in Europe and the United States', 49 *Wake Forest Law Review*, p. 583-608. http://ir.lawnet.fordham.edu/faculty_scholarship/645.

Ribeiro, J. (2014), *Bing follows Google in offering the right to be forgotten*, PC World, 17th July. <http://www.pcworld.com/article/2455240/microsofts-bing-follows-google-in-offering-europeans-the-right-to-be-forgotten.html>

Rosen, J. (2012), The Deciders: the future of privacy and free speech in the age of Facebook and Google, 80 *Fordham Law Revi*er 1525. <http://ir.lawnet.fordham.edu/flr/vol80/iss4/1>.

Schmitt, C., *et al.* (2013), *Security and privacy in the era of Big Data: the SMW, a technological solution to the challenge of data leakage*, RENCI, University of North Carolina at Chapel Hill, http://dx.doi.org/10.7921/G0WD3XHT.

Tene, O. (2011), Privacy: the new generations, *International Data Privacy Law* 15, p. 15-27. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1710688>.

Tene, O.; Polonetsky, J. (2012), Privacy in the age of Big Data: a time for big decisions, *Stanford Law Review Online*, 2 February, p. 63-69. <http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-63_1.pdf>.

Von Bodgandy, A. (2000), The European Union as a Human Rights Organization?: Human Rights and the core of the European Union, *Common Market Law Review* 37, p. 1.307-1.38.

Warso, Z. (2013), There's more to it than data protection: fundamental rights, privacy and the personal/household exemption in the digital age, *Computer Law & Security Review* 29 (5), p. 491-500.

The White House (2014), *Big Data: seizing opportunities, preserving values*, Executive Office of the President, May.

Zanfir, G. (2014), Forgetting about consent: why the focus should be on 'suitable safeguards. In Gurwitch, S.; Leenes, R.; De Hert; P., ed., *Reloading data protection: multidisciplinary insights and contemporary challenges*, Springer, p. 237-257.