FUNDAMENTAL RIGHTS IN THE EUROPEAN UNION SEEN THROUGH THE LENSES OF THE 2012 DATA PROTECTION REFORM PROPOSAL

Cristina SISERMAN*

Abstract

Due to the fact that technological progress and globalization have profoundly changed the way our personal data is collected and processed, in January 2012, the European Commission has proposed a comprehensive reform on the European Union's data protection rules. The reform package consists of a proposal for a General Data Protection Regulation, meant to replace the 1995 Data Protection Directive, as well as a new Data Protection Directive which shall provide for data protection in the areas of police and judicial cooperation in criminal matters. This reform initiative came as response to major critics according to which the 1995 rules on data protection have not been implemented in a uniform and efficient way by the EU Member States and, therefore, the rules need to be modernized in order to better respond to the current needs of the digital age. Supporters of the reform put forward that this reform is also needed due to the fact that data protection has acquired the status of a separate fundamental right in the EU, in the Charter of Fundamental Rights (article 8), which is distinct to the right to respect for private and family life. In this context, the study aims to answer whether the new reform legislation has the potential to augment the internal market dimension of data protection, increase the effectiveness of the fundamental right to data and, at the same time, enhance the coherence of the EU data protection framework. With this objective in mind, the study will present and analyze the EU standards regarding data protection and analyze some of the main items of the proposed reform. It will also provide an overview of the best practices in the Member States and the deficiencies that need to be taken into consideration by policy makers in order to achieve more efficient results. The study will also present and evaluate some of the most relevant jurisprudence of the European Court of Human Rights and European Court of Justice in the field of data protection and human rights.

Keywords: *fundamental rights, data protection authorities, judicial cooperation, effective remedy etc.*

1. Introduction and preliminary considerations

Personal data or information relating to individuals is collected and used in many aspects of our lives, starting from registration to a library, to gym membership,

* Cristina SISERMAN is a Ph.D. Student in International Law at the Faculty of Law, University of Vienna, Austria.

opening of a bank account or maintenance of a health insurance. Personal data has been defined as any information associated to an individual, whether it is related to his/her private, professional or public life[1]. The personal data can range from simple information that identifies an individual, such as name, telephone number or photo, to more complex data like biometric or medical data. Personal data can be collected through many different means: directly from the individual or through transfers from existing data bases. The great danger resides in the fact that this data could be subsequently used for other reasons or purposes than those initially stated and can be shared with other parties[2].

Advancements in technology and telecommunication networks enables data to travel across borders with greater ease. Data concerning the citizens of one Member State can be processed in other member State of the EU. Therefore, since the exchange of data between member States becomes more and more frequent, having a strong legal framework that regulates these exchanges is very much in need.

The European Union is an economic and political union of 28 Member States, whose structure and ways in which it ensures the protection of fundamental rights is considered to have been profoundly affected by the entry into force of the Treaty of Lisbon, in December 2009[3]. Currently, fundamental rights are protected in the EU legal framework through three complementary perspectives[4]: a) as general principles in the EU derived from the European Convention on Human Rights and the constitutional traditions of the Member States[5]; b) as defined by the Charter of Fundamental Rights of the European Union[6]; c) and as protected by the European Convention on Human Rights[7].

In 2000, the EU has adopted the Charter of Fundamental Rights of the European Union, which introduced in its article 7[8] the fundamental right to privacy and in its article 8[9] the fundamental right to the protection of personal data. Article 8 establishes

---

[1] *See* European Commission, Fact Sheet: Why do we need an EU data protection reform?, 2012, p. 1. Available online: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf.

[2] *See* European Union Agency for Fundamental Rights, Handbook on the European data protection law, Luxembourg: Publication Office of the European Union, 2013. Available online: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf.

[3] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, OJ C 306, 17 December 2007, at 1-271. EU treaties and relevant adopted or under adoption legislation as well as other official documents are also available online at http://europa.eu/documentation/legislation/index_en.htm

[4] European Union Agency for Fundamental Rights, Handbook on the European data protection law, Luxembourg: Publication Office of the European Union, 2013, p. 17-21.

[5] *See* Art. 6(3) of the Consolidated Version of the Treaty on European Union (TEU). Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, OJ C 83, 30 March 2010, at 1-388.

[6] Charter of Fundamental Rights of the European Union, 18 December 2000. Available online: http://www.europarl.europa.eu/charter/pdf/text_en.pdf

[7] Art. 6(1) TEU.

[8] Art. 7 of the Charter, "Respect for private and family life," reads: "Everyone has the right to respect for his or her private and family life, home and communications".

[9] Art. 8 of the Charter, "Protection of personal data," reads: "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by

that data concerning individuals must be processed fairly, for specific purposes, and on the basis of their consent or a legitimate basis laid down by law; that everybody has the right to access and rectify the data collected concerning them and that compliance with these rules shall be subject to control by an independent authority[10]. Moreover, article 47 of the Charter provides the right to an effective remedy before a tribunal. Consequently, because an effective remedy cannot be separated from the need to effectively enforce all fundamental rights[11], these two fundamental rights will be analysed together.

Meanwhile, acknowledging the fact that technological progress and globalization have profoundly changed the way our personal data is collected and processed, in 25 January 2012, the European Commission has proposed a comprehensive reform on the EU's data protection legislation, initiating thus the most important reform in the EU in this area in the last 20 years. As described by the European Union Agency for Fundamental Rights, "the importance of personal data protection, an area of EU responsibility, to key business actors and third countries across the globe has made this reform package as one of the most important EU legislative files in the civil liberties area"[12]. This reform initiative came as a response to major critics according to which the 1995 rules on data protection have not been implemented in a uniform and efficient way by the EU Member States. The reform initiators believed that the rules need to be modernized in order to better respond to the current needs of the digital age. At the same time, other supporters put forward the fact that this reform is also needed due to the fact that data protection has acquired the status of a separate fundamental right in the EU, in the context of the Charter of Fundamental Rights (article 8), which is distinct to the right to respect for private and family life.

In this light, the main aim of the study is to answer whether the new reform legislation can augment the internal market dimension of data protection, increase the effectiveness of the fundamental right to data and, concurrently, enhance the coherence of the EU data protection framework. In order to answer these questions, the first part the study will present the objectives envisaged by the EU data protection reform. The second part will introduce the EU standards regarding data protection provided by the current legal framework and analyse some of the main items of the proposed reform. In this context, the study will provide an overview of the best practices in the Member States, as well as some deficiencies that need to be taken into consideration by policy makers in order to achieve efficient results. The third part of the study contains an evaluation of the current status of the right to data protection and analyses some relevant jurisprudence of the European Court of Human Rights and European Court of Justice in the field of data protection and human rights. The study

law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority."

[10] *See* art. 8 of the Charter.

[11] European Union Agency for Fundamental Rights, Access to data protection remedies in EU Member States, Luxembourg: Publication Office of the European Union, 2013, p. 7.

[12] European Union Agency for Fundamental Rights, Fundamental Rights: challenges and achievements in 2012, Luxembourg: Publication Office of the European Union, 2013, p. 101.

concludes that the new reform seems to bring a lot of positive changes; however, there is a great need to make sure that all these changes are going to be adopted by the Member States in a uniform manner. In this regard, the study argues that the role of European Court of Justice and domestic national authorities is very important in efficiently interpreting and enforcing these rules.

2. The envisaged objectives of the EU data protection reform

The EU's 1995 data protection Directive is thought to have set a milestone in the history of personal data protection[13]. The main principles of ensuring a functional internal market and an effective protection of fundamental rights still constitute its primary objective. However, the problem that has been identified all along the last decade is that each EU Member States implements the law in an uneven way, providing thus an uneven level of protection of personal data[14]. In this sense, the need of modernisation of the legal framework has to be considered and adapted to keep up with the rapid technological developments brought by globalisation. These advances are especially visible when using social networking sites, cloud computing, location-based services and smart cards[15]. When using these services, the user leaves digital traces with every move he makes. Therefore, it is of no doubt for the EU Commission that in this new data world a robust set of rules is needed[16]. This is the core argument put forward by the European Commission to motivate the so much discussed data reform[17].

Through the reform started in 2012, the EU Commission proposal aims to update and modernise the following principles[18]: reinforce individual's rights; strengthen the EU internal market; ensure a high level of data protection in all areas; include police and criminal justice cooperation; ensure proper enforcement of the rules; and set global data-protection standards[19]. Before analysing whether all these envisaged objectives are realistic and feasible to fulfil within the existing legislative framework, a short presentation of each of these objectives is required. Some of these objectives will be indirectly reassessed in the third part of the study when the European legislation in the field of data protection will be presented and some of the deficiencies will be identified.

---

[13] European Commission, Fact Sheet: Why do we need an EU data protection reform?, 2012, p. 1. Available online: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf

[14] *Ibid.*

[15] European Union Agency for Fundamental Rights, Handbook on the European data protection law, Luxembourg: Publication Office of the European Union, 2013, p. 17-21.

[16] European Commission, Fact Sheet: Why do we need an EU data protection reform?, *Ibid.,* p. 2.

[17] For a comprehensive presentation of these objectives *See* Reding, V., The European data protection framework for the 21 century, International Data Privacy Law, Vol. 0, No. 0, 2012. Available online: http://idpl.oxfordjournals.org/content/early/2012/06/25/idpl.ips015.full.pdf+html

[18] European Commission, Commission Staff Working Paper Executive Summary of the Impact Assessment, Brussels, 2012. Available online: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_73_en.pdf

[19] European Commission, Fact Sheet: Why do we need an EU data protection reform?, *Ibid,* p. 2.

2.1. Simplification of the existing rules

Needless to say, the rapid pace of technological change and globalisation have profoundly transformed the way personal data is collected, accessed, used and transferred[20]. The nature of data flows and advanced technology such as cloud computing pose new challenges for data protection authorities, as data can move from one Member State (jurisdiction) to another, including outside the EU[21]. In order to ensure the full protection of the individuals, the rules need to be brought in line with the technological developments[22].

According to the European Commission, the individuals and business community expect that data protection rules to be applied in a uniform manner across the EU so that more economic and legal stability could be enjoyed. In this sense, one of the envisaged aims of the Commission is to increase harmonisation of legislation (especially in areas including police and criminal justice) and thus simplify and streamline the data protection rules across the Europe[23]. The Commission is proposing one single set of technologically neutral set of rules across the EU[24]. This implies that regardless of how technology and digital environment develop in the future, the personal information of individuals will be secure in the EU because all national authorities will work to reach the same objective[25]. Nonetheless, the reform is envisaged to be more consumer-friendly as the latter will have a single point of contact to deal with their requests, i.e. a single data protection authority that would be responsible for a company operating in several countries[26]. The citizens will have a right to data portability (right to obtain a copy of their data from one company and transmit it to another without hindrance), while being assured that all through this process their personal data is fully protected[27].

2.2 Strengthen citizens' rights

Strengthening the citizens' rights is also a corner-key of the reform. In its proposal, the Commission advocates for a strengthen right to be forgotten, which implies that once a person does not wish any more to have his personal data processed and there is no legitimate reason for an organisation to keep it, it must be

---

[20] European Commission, Fact Sheet: How will the EU's reform adapt data protection rules to new technological developments?, 2012, p. 2. Available online: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/8_en.pdf

[21] *Ibid.,* p. 1.

[22] *Ibid.*

[23] European Commission, Fact Sheet: How will the EU's data protection reform simplify the existing rules?, 2012. Available online: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/6_en.pdf

[24] *See* Reding, V., *Ibid.*, p. 6.

[25] *Ibid.,* p. 2.

[26] European Commission, Fact Sheet: How will the EU's data protection reform simplify the existing rules?, p. 2.

[27] European Commission, Fact Sheet: How will the EU's reform adapt data protection rules to new technological developments?, 2012, p. 2.

removed from the system[28]. At the same time, the companies are obliged to inform the consumer in clear, understandable and transparent manner about how their personal data will be used, in order to enable them to decide which type of data they wish to share[29]. With this reform, the providers must take into account the principle "privacy by default", which implies that the default settings should be those that provide the consumers with the most privacy[30].

The vital change of the reform consists in guaranteeing the citizens' easy access to their own data; establishing a right for individuals to freely transfer their data from one service provider to another; and ensuring that consent is given explicitly by individuals when it is required for certain types of data processing[31]. But this is not the only thing. The European Commission is also envisaging improved administrative and judicial remedies in cases of violation of data protection rights[32]. This implies increased responsibility and accountability for those processing personal data through data protection risk assessments and data protection officers[33].

2.3 Strengthen the European business within the internal market

The European Commission has shown that the fragmentation of rules between EU countries is a costly administrative burden that represents a strong deterrent to economic development[34]. In this light, the European Commission is proposing a level playing field for business[35] through one single law applicable to any business across the EU[36]. Furthermore, the Commission is planning to cut the red tape and bureaucratic requirements which impose unnecessary costs on the business. The Commission expects that this harmonisation would save businesses up to 2.3 billion Euros per year[37].

---

[28] European Commission, Fact Sheet: How will the data protection reform affect social networks?, p. 1, 2012. Available online: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf

[29] *Ibid.,* p. 2.

[30] *See* European Parliament, Q&A on EU data protection reform, Citizens' rights and fundamental rights, May 2013. Available online: http://www.europarl.europa.eu/news/en/pressroom/content/20130502BKG07917/html/QA-on-EU-data-protection-reform

[31] European Commission, Fact Sheet: How will the data protection reform affect social networks?, p. 1.

[32] European Commission, Fact Sheet: How does the data protection reform strengthen citizens' rights?, 2012, p. 1.. Available online: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf

[33] *Ibid,* p. 2.

[34] European Commission, Fact Sheet: How will the EU's data protection reform benefit European business?, 2012. Available online: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/7_en.pdf

[35] *See* also Person, A., How the new EU Data Protection Regulation affects your small business?. Article published in 300 Entrepreneurship, April 2012. Available online: http://360entrepreneurship. com/2012/04/03/how-the-new-eu-data-protection-regulation-effects-your-small-business/

[36] European Commission, Fact Sheet: How will the EU's data protection reform benefit European business?, 2012., p. 2.

[37] *Ibid.,* p. 1.

Since companies may have to deal with 28 different sets of data protection rules, the European Commission has pointed out that the result is a fragmented environment with legal uncertainty and unequal protection for the individuals[38]. Moreover, it also causes unnecessary costs and a significant administrative burden for business. It has been noted, that this situation is a disincentive for business, especially for particularly small and medium-sized companies[39]. In this respect, the Commission wants to adopt new rules to remove barriers to the internal market by adopting one single law applicable to the EU, with a "one-stop-shop policy", which implies that each business will be answerable to just one single data protection authority[40]. The EU Commission also envisages a better cooperation between data protection authorities on cases with a wider European impact.

2.4 Strengthen international cooperation

Because personal data is increasingly being transferred across borders and stored on servers in multiple countries, both outside and inside the EU (cloud computing), the globalised nature of the data flows requires a consistent level of protection at international level[41]. In order to achieve this endeavour, the European Commission is proposing a system with clear rules on when EU law applies to data controllers outside the EU. The Commission also supports a streamline procedure for adequacy-decisions that will allow the free flow of information between the EU and non-EU countries[42]. According to the Commission, such decisions will be taken at European level on the basis of explicit criteria which will also apply to police cooperation and criminal justice.[43] The proposal will also promote effective international cooperation[44] for data protection enforcement between the Commission, European data protection authorities and authorities outside the EU, through investigative assistance, information exchange and complaint referral[45].

In this first section we have seen defined the main objectives of the data protection reform, as stated by the European Commission. These are objectives meant to "build a modern, strong, consistent and comprehensive data protection for the European Union"[46]. In the following section, a short introduction of the European legislation on data protection will be provided, while also analysing whether the objectives outlined above actually match the legal provision laid in the Proposal for Regulation.

---

[38] European Commission, Fact Sheet: How will the EU's data protection reform strengthen the internal market?, 2012. Available online: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/4_en.pdf

[39] *Ibid.*, p. 1.

[40] *Ibid.*, p. 2.

[41] European Commission, Fact Sheet, How will the EU's data protection reform make international cooperation easier?, 2012, p. 1. Available online: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/5_en.pdf

[42] *Ibid.*, p. 2.

[43] *Ibid.*, p. 1.

[44] *See* Reding, V., *Ibid.*, p. 10.

[45] European Commission, Fact Sheet, How will the EU's data protection reform make international cooperation easier?, 2012, p. 1.

[46] Reding, V., *Ibid.*, p. 10.

3. The European legislation on data protection

As presented in the preliminary considerations, the main instrument protecting the personal data is Article 8 of the Charter of Fundamental Rights of the European Union[47], which enshrines the fundamental right to the protection of personal data of every individual in a legally binding nature and defines the basic principles for the protection of personal data. However, besides this instrument, the EU legal framework contains a series of directives and regulations as well as special provisions in the field of common foreign and security policy and police and judicial cooperation in criminal matters. In the following sections some of these legal instruments are going to be presented with a special emphasize on the proposal for the regulation standing at the basis of the data protection reform.

3.1 Data protection under the EU Directives

Historically, the EU has played an important role in driving the development and introduction of national data protection law in a number of legal systems in the EU[48]. The protection of personal data was first addressed in the European Union by the Directive 95/46/EC[49] (the data protection Directive), which was developed to harmonise national provisions in this field[50] [51]. The Directive was a milestone in the history of the protection of personal data as a fundamental right[52]. Legislation at the EU level was essential because the differences in the way Member States approached this issue impeded the free flow of personal data among the Member States[53]. The main objective of the directive was double-targeted: to ensure equivalent protection of data of all the citizens across the Union[54] and to protect the "fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data between Member States"[55] [56]. It stipulates general

---

[47] *See* Charter of Fundamental Rights of the European Union. Available online: http://www.europarl.europa.eu/charter/pdf/text_en.pdf

[48] European Union Agency for Fundamental Rights, Data Protection in the European Union: the Role of National Data Protection Authorities, Luxembourg: Publications Office of the European Union, 2010, p. 6. Available online: http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_ en.pdf

[49] *See* Directive 95/46/EC of the European Parliament and of the Councol of 24 October 1995. Available online: http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

[50] European Union Agency for Fundamental Rights, Data Protection in the European Union: the Role of National Data Protection Authorities, Luxembourg: Publications Office of the European Union, 2010, p. 4.

[51] Goncalves, M.E., Jesus, A., Security and Personal Data protection in the European Union: Challenging Trends from a Human Rights Perspective, Lisbon University Institute, p. 117. Available online: http://www.etc-graz.at/typo3/fileadmin/user_upload/ETC-Hauptseite/human_security/hs-perspectives/pdffiles/issue1_2012/10-HSP12_Goncalves-Jesus__FINAL_.pdf

[52] Reding, V., *Ibid.*, p. 2.

[53] *See* Annex 1: Current EU Legal Instruments for the Protection of Personal Data, p. 2. Available online: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_annexes_en.pdf

[54] European Union Agency for Fundamental Rights, Data Protection in the European Union: the Role of National Data Protection Authorities, Luxembourg: Publications Office of the European Union, 2010, p. 4.

[55] Fuster, G., Gellert, R., *Ibid.*, p. 74.

[56] *See* also Reding, V., *Ibid.*, p. 2.

rules on the lawfulness of the processing of personal data and the rights of people whose rights are processed. The Directive also provides that at least one independent supervisory authority in each Member State shall be responsible for monitoring its implementation.[57]

The Directive was adopted under the Internal Market provisions of European law. The processing of personal data in the areas of common foreign and security policy and police and judicial cooperation, as well as public security defence, state security and criminal law has been explicitly excluded from the scope of application of the Data Protection Directive.[58] [59] The Directive prohibits transfer of data to third countries unless the latter provide an adequate level of protection as determined by the Commission[60]. In this way, the Directive sought to reconcile personal data protection, regarded as a minimum level of protection throughout the European Community, with the free movement of information in the interest of the internal market economy.[61] [62]

As showed in the literature[63], if compared with its predecessor (the Convention for the Protection of Individuals with regard to Automatic processing of Personal Data, 1981), the Data Protection Directive represents a change in the balancing of rights of the individual vis-à-vis the interests of data controllers and processors[64]. The Court of Justice of the EU has relied on this overt foundation of the data Protection to explicitly affirm the existence of a strong link between EU personal data protection law and the right to privacy as recognised by the article 8 of the ECHR.[65]

Regarding the success of implementation this directive, the Commission found in 2007 that the Directive did not manage to fully achieve its internal market policy objective or to remove differences in the level of data protection in the member States[66]. Enforcement was also identified as an area in which more improvement was needed[67]. According to the Commission, the "problems in fully achieving its internal market policy objective, removing differences in the level of data protection actually afforded in the Member States and in ensuring effective enforcement across the EU have become more acute in particular due to the fast and far-reaching development of

---

[57] *See* Annex 1: Current EU Legal Instruments for the Protection of Personal Data, p. 2. Available online: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_annexes_en.pdf

[58] Goncalves. M.E., Jesus, A., *Ibid.*, p. 119.

[59] *See* the European Parliament and the Council, Directive 95/46/EC, Article 3.

[60] *See* also Reding, V., *Ibid.*, p. 4.

[61] Goncalves. M.E., Jesus, A., *Ibid.*, p. 121.

[62] *See* also Reding, V., *Ibid.*, p. 3.

[63] *See* also Robinson, N., Graux, H., Batterman, M., Valeri, L., Review of the European Data Protection Directive, Rand, 2009.

[64] Goncalves. M.E., Jesus, A., *Ibid.*, p. 121.

[65] Fuster, G., Gellert, R., *Ibid.*, p. 74.

[66] Robinson, N., Graux, H., Batterman, M., Valeri, L., *Ibid.,* p. 20.

[67] *See* the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive COM(2007) 87 final, Brussels, 2007. Available online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0087:FIN:EN:PDF

digital technologies and online services"[68]. Some of the main weaknesses of the Directive, as identified by Robinson et al. consist in the following: the link between the concept of personal data and real privacy risks is unclear; some of the measures aimed at providing transparency through better information and notification are inconsistent and ineffective; the rules on data export and transfer to external third countries are outmoded or cumbersome; the role of data protection authorities in accountability and enforcement is inconsistent, while the definition of entities involved in processing and managing personal data is simplistic[69]. Therefore, the fragmentations and uncertainties in the implementation of the Directive 95/46/EC and the new challenges require the EU to adapt the legal framework for the protection of personal data in the EU[70]. Based on this criticism the data protection reform started in 2012 is to be welcomed.

Another important directive is the "E-Privacy" Directive 2002/58/EC[71] which complements Directive 95/46/EC with respect to the processing of personal data in the electronic communication sector, ensuring the free movement of such data and of electronic communication and services in the EU. This directive has been recently amended by Directive 2009/136/EC[72], introducing in particular a mandatory personal data breach notification[73]. However, although relative new, this directive is already subjected to a series of criticism as some of its provisions are subject to various interpretations by the Member States, which shows that a uniform implementation will be difficult to achieve.

The Directive requires member States to ensure that the storing of information or the access to information already stored in the user's terminal equipment is allowed only with the user's informed consent. The provisions of the directive read: "the need for users' informed prior consent must be freely given, specific and constitute an informed indication of the data subject's wishes"[74]. In a study published by *Clearly Gottlieb*, the authors showed that the Directive and most national transposition laws do not expressly provide whether the consent should be obtained under the "opt-out" or "opt-in" approach. In this sense, they showed that some Member States do not accept consent given through browser settings and require more explicit acceptance by unambiguously accepting the terms and conditions or a

---

[68] *Ibid.*

[69] Robinson, N., Graux, H., Batterman, M., Valeri, L., *Ibid.,* p. 27-40.

[70] *See* also Reding, V., *Ibid.*, p. 3.

[71] *See* Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Available online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:PDF

[72] *See* Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009. Available online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009: 337:0011: 0036:en:PDF

[73] *See* Annex 1: Current EU Legal Instruments for the Protection of Personal Data, p. 3. Available online: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_annexes_en.pdf

[74] *See* Article 29 Working Party, Opinion 2/2010 on online behavioral advertising, June 22, 2010, Section 4–4.1. Available online: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

pop in/out technique[75]. Similarly, another different opinion is with regard to whether the consent should be obtained before or after the cookie is set. Despite the fact that the consent is desirable to be obtained before the cookie is placed, this is difficult in practice[76].

The way these directives have been interpreted by the Member States shows that their implementation in practice is very difficult to achieve, especially if the uniformity objective is desired. Therefore, a EU regulation might be a better solution for reaching this objective, as a regulation is directly applicable in all Member States, whereas a directive requires further legislation to bring it into force in different jurisdictions. This was the main reason had in mind when drafting the proposal for the reform envisaged in the area of data protection.

3.2 Data protection under EU Regulations

In the field of data protection, the EU has rendered only a small number of regulations. Regulation No 45/2001[77], adopted under article 286 EC, provides the rights of the data subjects and the obligations of those responsible for the processing. It also establishes the European Data Protection Supervisor (EDPS) as an independent supervisory authority for the EU[78]. With the entry into force of article 16 TFEU, the scope of application of the regulation extends automatically to all data processing activities of the EU institutions.

The most important regulation in this field at the moment is "General Data Protection Regulation"[79] which started in January 2012 the discussion on the reform of European data protection law. This reform came as a result that for a number of years, the regime has been criticised for being inconsistent and out of date. It has been put forward that the different ways in which Member States implemented and interpreted the Directive had led to a lack of harmonisation[80]. However, since the objectives and principles of the current European data protection framework are still considered by many[81] as sound and responding to the existing needs, the Regulation[82] retains many of its current concepts, definitions and basic principles[83].

---

[75] Cleary Gottlieb, Alert Memo: New Consent Regime for Cookies to enter into force in the UK, Brussels, 2012, p. 3.

[76] Cleary Gottlieb, *Ibid.*, p. 3.

[77] *See* Regulation (EC) no 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. Available online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:en:PDF

[78] *Ibid.*

[79] 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), 2012. Available online: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[80] *See* Slaughter and May, The new EU Data Protection Regulation - revolution or evolution?, 2013, p. 2. Available online: http://www.slaughterandmay.com/media/1844766/the-new-eu-data-protection-regulation-revolution-or-evolution.pdf

[81] Slaughter and May, *Ibid.*, p. 2.

[82] *See* Supra Footnote 8.

[83] Slaughter and May, *Ibid.*, p. 2.

As already emphasized above, the substantial change resides in the fact that the new proposal is in the form of a regulation rather than a directive. Because the new legislative provisions are in the form of a regulation[84], which is more prescriptive than the current regime, this will help create a more unified data protection regime across the member States[85]. However, it is still likely to create differences in the way Member States interpret and enforce the Regulation[86]. The Regulation also allows the Member States to pass additional measures for certain matters (health and employment) which could lead to further divergences.[87] [88] Nonetheless, this is also linked to concerns that discrepancies in substance and method of implementation between draft Directive on criminal and judicial processing and the Regulation will hinder the desired harmonisation of the reform package as a whole[89].

The regulation contains a series of important issues that are going to be discussed in the course of legislative procedure. Among these, is the scope and transfer of data to third countries, which is regulated in a much more detailed manner than in the European Data Protection Directive, although an important question such as the issue of government access to data that has been transferred to foreign companies remains unsolved.[90] As showed in the section above, another key issue concerns changes that enhance the rights of the data subjects. According to the draft regulation, the national laws in the EU must guarantee a series of rights for the individuals. Among these rights are the right to be informed when personal data was processed and the reason for processing, the right to access the data and if necessary, the right to have the data amended or deleted.[91] National laws regarding data protection demanded good data management practices on the part of the entities that process data, called "data controllers". This includes the obligation to process the data fairly and in a secure manner and to use personal data for explicit and legitimate purposes.[92]

An important change brought by the proposal would be to use modern data protection instruments and underlines the idea of technologically neutral protection. Accordingly, the controller is required to implement appropriate technical and organisational measures and procedures to ensure compliance with the Regulation and safeguard the data subject's rights[93]. The institutional and organisational

---

[84] *See* also Reding, V., *Ibid.*, p. 3.
[85] *Ibid.*, p. 3.
[86] *Ibid.*, p. 3.
[87] *Ibid.*, p. 3.
[88] *See* Hornung, G., A General Data Protection Regulation for Europe? Light and Shade in the Commission's Draft of 25 January 2012, Scripted, Vol. 9, Issue 1, April 2012, p. 68. Available online: http://script-ed.org/wp-content/uploads/2012/05/hornung.pdf
[89] Slaughter and May, Data Protection Reform - preparing for Change, p. 14. Available online: http://www.slaughterandmay.com/media/1957777/data-protection-reform.pdf
[90] Hornung, G., *Ibid.*, p. 73.
[91] *See* also European Union, Data protection in the European Union, p. 3. Publication available on the official site of the EU: http://ec.europa.eu/justice/policies/privacy/docs/guide/guide-ukingdom_en.pdf
[92] *Ibid.*, p. 3.
[93] Hornung, G., *Ibid.*, p. 76.

provisions also account for a substantial portion of the proposal. In this regard, the regulation makes internal data protection officers mandatory for all public authorities or bodies that employ 250 persons or more[94]. It also mandates the establishment of supervisory authorities and it brings the Member States the obligation to provide these authorities with adequate human, technical and financial means[95]. It also changes the competence rules. While each supervisory authority normally covers the territory of the respective Member State, special rules apply to enterprises that are established in more than one Member State. In this case, the Regulation states that the supervisory authority of the main establishment shall be exclusively competent for the entire enterprise[96].

However, the new regulation has already been subjected to a series of criticism. Scholars such as Hornung believe that "the draft offers both light and shade"[97]. In his view, there are a series of new rules, such as those concerning data subjects' rights, technological and organisational duties, and competences of supervisory authorities and defined sanctions, which are commendable[98]. However, a problem resides in the increasing range of competences that the Commission will gain, which in Hornung's view is inadequately wide[99]. The Commission's decision-making competence contravenes the position of the national supervisory authority[100] (or, the draft requests the Member States to grant complete independence to supervisory authorities). Nonetheless, despite the fact that the national laws on data protection in the EU aim to guarantee the same rights, some differences continue to exist. It has been noted that "these differences could create potential obstacles to the free flow of information and additional burdens for economic operator and citizens."[101]

3.3 Data protection in the area of Common Foreign and Security Policy and Cooperation in Criminal Matters

Regarding the Common Foreign and Security Policy, currently there is no specific EU legislation for the protection of personal data in this field[102]. Specific rules may be laid down though the newly introduced Article 39 TFEU for Common Foreign and Security Policy issues. For actions implementing restrictive measures or sanctions, the Member States apply the provisions resulting from the implementation of Directive 95/46/EC[103]. Article 39 of the Union Treaty derogates from paragraph 2 of Article 16 and establishes that specific rules of the protection of personal data processed by Member States in the area of Common Foreign and Security Policy will be laid down by the Council. Consequently, the subjective right to the protection of personal data

---

[94] *Ibid.*, p. 77.
[95] *Ibid.*, p. 78.
[96] *See* article 4(13) of the Proposal.
[97] Hornung, G., *Ibid.*, p. 80.
[98] *Ibid.*
[99] *Ibid.*, p. 81.
[100] *Ibid.*, p. 81.
[101] *See* supra Footnote 45, European Union Data protection in the European Union, p. 3.
[102] *Ibid.*
[103] *Ibid.*

laid down in article 16 TFEU[104] will still apply in this area, but the procedure for the adoption of specific rules will not belong to the European Parliament[105]. Scholars such as Scirocco[106] consider that this aspect is particularly important to note, because the Council and the Commission play a crucial role in managing the "terrorist blacklists", which are lists of individuals and organizations whose assets are frozen because of their personal connection with terrorist organizations. Therefore, in this context, a better definition of data protection rules in the area of Common and Foreign Security Policy will enhance the quality and legitimacy of the Union's action in this area[107].

In the area of police and judicial cooperation in criminal matters, the current EU framework consists of different rights and obligations for Member States and individuals and of several data protection supervisory authorities. Since 2008, Council Framework Decision 2008/977/JHA[108] aims at creating a general legislative framework for the protection of personal data and judicial cooperation in criminal matters[109]. The implementation of this decision was due in November 2010 and it applies fully to Ireland, Iceland, Norway and Switzerland as it is a development of Schengen *acquis*. It does not replace the rules applicable to Europol, Eurojust, Schengen and the Customs Information System[110]. The framework has been justified on the grounds that it triggers the implementation of cooperation mechanisms under Union law, in particular as regards the exchange of information on terrorist offences between Member States and the transfer of such information to Europol and Eurojust[111].

However, the Framework decision has had a mixed reception[112], with data protection experts considering that the decision does not go far enough to protect citizens' personal data, while others argue that this is as far as the European Council could legally go.[113] It has been commented that the limited scope of the Framework Decision already leads to legal and practical deficiencies for the protection of personal

---

[104] *See* the Consolidated Version for the Treaty of the Functioning of the European Union, Official Journal of the European Union, C 83/49. Available online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0047:0200:en:PDF

[105] *See* article 16 TFEU.

[106] *See* Scirocco, A., The Lisbon Treaty and the Protection of Personal Data in the European Union, Published in the digital magazine Dataprotectionreview.eu, Issue 5, February 2008, p. 3. Available online: http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2008/08-09-19_Scirocco_Lisbontreaty_DP_EN.pdf

[107] *See* Human, H., Sciriocco, A., Schortcomings in EU Data protection in the Third and the Second Pillars. Can the Lisbon Treaty be expected to help?, Common Market Law Review, Vol. 46, p. 1485-1525, 2009. Available online: http://www.edps.europa.eu/ EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-06-02_Shortcomings_DP_EN.pdf

[108] *See* Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. Available online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:01:EN:HTML

[109] *See* supra Footnote 45, European Union Data protection in the European Union, p. 38.

[110] *See* also Reding, V., *Ibid.*, p. 4.

[111] *See* Mitsilegas, V., The third wave of third pillar law: which direction fort EU criminal justice?, Thomson Reuters, E.L. Rev. August, 2009, p. 525.

[112] *See* also Reding, V., *Ibid.*, p. 4.

[113] For a presentation of arguments in both directions *See* Mitsilegas, V., *Ibid.*, p. 524-527.

data at EU level[114]. Accordingly, more and more EU legislation creates harmonised legal obligations upon private or public sector data controllers requiring the processing and exchange of personal data for purposes of prevention, investigation, detection or prosecution of criminal offences, without providing for correspondingly harmonised and comprehensive provisions for the protection of personal data[115] [116].

We have seen in this section of the study the legal framework on data protection in the EU, by emphasizing some of its negative and positive aspects. However, a simple legislative framework is not sufficient enough to tell whether the system is working or not or whether the legal provisions present sufficient safeguards for the respect of personal data. In order to find an answer regarding this question, it is of great necessity to analyse the degree to which personal data is considered a fundamental right in the EU, and consequently protected as such. In doing this, an analyse of some of the jurisprudence of the European Court of Justice is also required.

4. The fundamental right to personal data protection in the EU

In the following paragraphs a short description of the status of data protect in the EU will be presented and the role of this right within the European human rights framework. Then, a short presentation of the jurisprudence will be also provided in order to identify the gaps in the implementation and application of data protection rules, with the purpose of providing further arguments for the strong need of a reform in the field of data protection.

4.1 Status of the right to data protection

In the legal field, it is often reminded that in a democratic society, all exercise of public power is subject to the observance of fundamental rights. This is a characteristic of constitutionalism, which explains the importance of the topic of fundamental rights protection in the European Union[117]. Since the entry into force of the Lisbon Treaty in December 2009, the right to protection of personal data is formally configured as an autonomous fundamental right of the European Union[118] [119].

---

[114] For a detail presentation of the main problems regarding data protection and data security See O'Neill, M., The Issue of Data Protection and Data Security in the (Pre-Lisbon) EU Third Pillar, Journal of Contemporary European Research, Vol. 6, Issue 2, p. 211-235. Available online: http://www.jcer.net/ojs/index.php/jcer/article/view/264/206

[115] *Ibid.*, p. 38.

[116] *See* also Reding, V., *Ibid.*, p. 4.

[117] *See* Besselink, L., The Protection of Fundamental Rights post-Lisbon: The interaction between the EU Charter of Fundamental Rights, the European Convention on Human Rights and the National Constitutions, University of Utrecht, 2012, p. 1. Report available online: http://www.fide2012.eu/index.php?doc_id=94

[118] Fuster, G., Gellert, R., The fundamental right of data protection in the European Union: in search of an uncharted right, International Review of Law Computers and Technology, Vol. 26, 2012, p. 73. Available online: http://www.tandfonline.com/doi/pdf/10.1080/13600869.2012.646798

[119] *See* also Goncalves. M.E., Jesus, A., Security and Personal Data protection in the European Union: Challenging Trends from a Human Rights Perspective, Lisbon University Institute, p. 135. Available online: http://www.etc-graz.at/typo3/fileadmin/user_upload/ETC-Hauptseite/human_security/hs-perspectives/pdffiles/issue1_2012/10-HSP12_Goncalves-Jesus__FINAL_.pdf

It is recognised as such in article 8 of the EU Charter of Fundamental Rights which has since 2009 legal binding force. The first paragraph of article 8 of the EU Charter stipulates that "everyone has the right to the protection of personal data concerning him or her"[120]. The second paragraph establishes that "such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by the law"[121] and that "everyone has the right of access to data which has been collected concerning him or her, and the right to have it ratified". Finally, the third paragraph provides that "compliance with these rules shall be subject to control by an independent authority"[122]. However, the European Charter does not contain an explicit and autonomous right to data protection[123].

It appears thus that the entry into force of the Lisbon Treaty marks a new era for data protection. Article 16 of the Treaty of the Functioning of the EU (TFEU) contains an individual right of the data subject and provides a legal basis for a strong EU-wide data protection law[124]. Moreover, the abolition of the pillar structures obliges the European Parliament and the Council to provide for data protection in all areas of the EU law, allowing for a comprehensive legal framework for data protection[125]. This legal framework is applicable to the private sector, the public sector in the Member States and the EU institutions and bodies.

The inclusion of data protection as an autonomous fundamental right is a recognition by the EU of the importance of technological progress and an attempt to make sure that fundamental rights take into account this progress[126]. According to European Union Agency for Fundamental Rights, this progress is clearly visible when one compares the EU Charter with the 1950 European Convention of Human Rights of the Council of Europe[127].

4.2. Data protection in the jurisprudence of the European Court of Justice and the European Court of Human Rights

In assessing the degree to which data is protected within the European Union, the case law of the EU Court of Justice is of much help[128]. By having a closer look at these cases, some of the crucial questions that would allow for a refined understanding of

---

120 Fuster, G., Gellert, R., *Ibid.*, p. 73.

121 *Ibid.*, p. 73.

122 *Ibid.*

123 European Union Agency for Fundamental Rights, Data Protection in the European Union: the Role of National Data Protection Authorities, Luxembourg: Publications Office of the European Union, 2010, p. 6. Available online: http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf

124 Goncalves. M.E., Jesus, A., *Ibid.*, p. 135.

125 *Ibid.*, p. 135.

126 European Union Agency for Fundamental Rights, Data Protection in the European Union: the Role of National Data Protection Authorities, Luxembourg: Publications Office of the European Union, 2010, p. 6.

127 *Ibid.*, p. 6.

128 For a comprehensive presentation of the ECJ jurisprudence *See* European Union Agency for Fundamental Rights, Handbook on the European data protection law, Luxembourg: Publication Office of the European Union, 2013.

the nature, scope and limits of the protection granted through article 8 of the Convention could be answered. Moreover, the EU Court of Justice also contributed to the reform package by elaborating case law on a key aspect of the reform package: the requirement of independence of data protection authorities (DPAs)[129].

Until 2000, EU legislation on the protection of personal data was adopted in the name of fundamental rights and freedoms of individuals in general but, more specifically, in the name of the right to privacy as embodied in article 8 of the European Convention on Human Rights. As showed in the sections above, the key piece of EU legal framework for personal protection was the Data Protection Directive, adopted in 1995. The Court of Justice of the EU relied on this Directive to affirm the existence of a strong link between EU personal data protection law and the right to privacy as recognised by article 8[130]. However, during this time, the Court repeatedly emphasized that protecting the right to privacy was not the only purpose of the Data Protection Directive and that Member States had to implement it in order to ensure a fair balance between any rights possible affected. The Court, in the case Lindqvist[131] stated that the implementation had to be in accordance with the Directive's objective to maintain a free flow of data and privacy protection.

Consequently, data protection emerges from the jurisprudence of the European Court of Human Rights in Strasbourg as an aspect for privacy protection[132]. In exchange, article 8 of the EU's Charter of Fundamental Rights acknowledges the centrality and importance that the right to data protection has acquired in our society because of the technological developments[133]. Regarding the case law of the European Court of Human Rights, before 2009, there are many occasions in which the Court has referred to data protection issues. In these cases, the Court has identified in article 8 of the ECHR both positive and negative obligations[134]. A negative obligation for the Member States would be to abstain from interfering with the right to privacy. A positive obligation would be to entail the "adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals themselves"[135].

The Court has rendered a series of judgements in which it laid the principles for the protection of personal data in fields like protection of medical data, surveillance and biometric data (such as fingerprints retention).

Regarding the *protection of medical data*, in M.S v Sweden[136], the Court stated that "the protection of personal data is of fundamental importance to a person's

---

[129] European Union Agency for Fundamental Rights, Fundamental Rights: challenges and achievements in 2012, Luxembourg: Publication Office of the European Union, 2013, p. 101.

[130] Fuster, G., Gellert, R., *Ibid.*, p. 74.

[131] *See* the Judgement ECHR, C-101/01 – Lindqvist, 6 November 2003. Available online: http://curia.europa.eu/juris/liste.jsf?language=en&num=C-101/01

[132] European Union Agency for Fundamental Rights, Data Protection in the European Union: the Role of National Data Protection Authorities, Luxembourg: Publications Office of the European Union, 2010, p. 6.

[133] *Ibid.*, p. 6.

[134] *Ibid.*, p. 13.

[135] *Ibid.*, p. 13.

[136] *See* the Judgement M.S. v Sweden, Application No. 20837/92, 27 August 1997. Available online: http://echr.ketse.com/doc/20837.92-en-19950522/view/

enjoyment of her right to respect for private and family life, as guaranteed by article 8 of the Convention"[137]. In a similar case, in Z. v. Finland[138], the Court further underlined that the protection of medical data is of great value for the person's enjoyment of his or her right to respect for private life, as guaranteed by article 8 of the ECHR[139]. However, in this case the Court set some limits, by noting that "it is accepted in the interest of a patient and the community as a whole in protecting the confidentiality of medical data may be outweighed by the interest in investigation and prosecution of crime and in the publicity of court proceedings where such interests are shown to be of even greater importance"[140].

As far as *surveillance* is concerned, in Leander v. Sweden[141], the Court noted that the storing of information relating to an individual's private life in a secret register and the release of such information represents an interference with his right to respect for private life as guaranteed by article 8(1)[142]. The Court showed that "in view of the risk that a system of secret surveillance for the protection of national security poses of undermining or even destroying democracy on the ground of defending it, the Court must be satisfied that there exists adequate and effective guarantees against abuse"[143]. In Rotaru v. Romania[144], the Court reiterated the principles established in Leander v. Sweden, according to which "the storing by a public authority of information relating to an individual's private life and the use of it amount, interferences with the right to respect for private life"[145]. The Court also

---

[137] *See* Supra Footnote 86. The case concerned the disclosure of medical personal data. The medical records in question contained highly personal and sensitive data about the applicant. Although they remained confidential, they had been disclosed to another public authority and therefore to a wider circle of public servants. The collection and storage of information interfered with applicant's right to respect for private life.

[138] *See* the Judgement Z. V. Finland, Application No. 22009/93, 28 February 1995. Available online: http://echr.ketse.com/doc/22009.93-en-19950228

[139] *See* Supra Footnote 88. The question in this case concerns orders requiring doctors and psychiatrist to give evidence, the seizure of medical records and their inclusion in an investigation file without the patient's prior consent in criminal proceedings concerning her husband, the limitation on the duration of the confidentiality of the medical data concerned and the publication of her identity and her HIV infection in a court judgement given in those proceedings. The European Court of Human Rights found it not established that there had been a leak of confidential medical data concerning the applicant for which the respondent State could be held responsible under Article 8.

[140] European Union Agency for Fundamental Rights, Data Protection in the European Union: the Role of National Data Protection Authorities, Luxembourg: Publications Office of the European Union, 2010, p. 13. Available online: http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf

[141] *See* the Judgement Leander v. Sweden, Application No. 9248/81, 10 October 1983. Available online: http://echr.ketse.com/doc/9248.81-en-19831010/

[142] See Supra Footnote 91. The case concerns a Swedish citizen, whose employment in a museum on a naval base was terminated for national security reasons after secret security checks were conducted on him. In other words, police files containing information about his private life were used for the purposes of assessing his suitability for the employment.

[143] Leander v. Sweden, *Ibid.*

[144] *See* the Judgement Rotaru v. Romania, Application No. 28341/95, 4 May 2000. Judgement available online: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58586

[145] European Union Agency for Fundamental Rights, Data Protection in the European Union: the Role of National Data Protection Authorities, Luxembourg: Publications Office of the European Union, 2010,

added that such interference occurs also from the refusal to allow an opportunity for the personal data to be refuted"[146].

Concerning the *retention of fingerprints*, cellular DNA profiles after criminal proceedings, in S. and Marper v. United Kingdom[147], the Court ruled on the lawfulness of these retentions. The problem raised was that the applicant requested the destruction of his data after the criminal proceedings against him were terminated and he was acquitted. The Court noted that the cellular samples contained much sensitive information about an individual and held that the retention of cellular samples and DNA profiles amounted to an interference with the applicant's right to respect for private life, within the meaning of article 8(1). The Court also observed that the protection afforded by article 8 would be unacceptably weakened if the use of modern scientific techniques in the criminal justice system went away, without carefully balancing the potential benefits of the extensive use of such data against important private-life interests[148].

From 2000 to 2009, the European Charter had no legal biding force. However, during this time, the legislator demonstrated its awareness of the fact that the text contained at least two separate provisions especially relevant for the protection of personal data[149]. The Court progressively moved towards accepting the idea that personal protection data is a right on its own; however, it is still described as "closely connected" to the right to privacy[150]. In 2009, the Lisbon Treaty affirmed that the EU Charter had the same value as the EU Treaties, granting to its provisions biding legal force. According to Fuster, this change came along with a series of uncertainties, particularly concerning the role of the Charter among other sources of fundamental rights protection, relevant for the EU legal system, and the interpretation of its provisions[151].

---

p. 13. Available online: http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf

[146] *See* Supra Footnote 94. The applicant, a lawyer, had been prosecuted for membership of student protest groups during the Communist dictatorship in Romania in 1946. After the collapse of the Ceausescu regime he applied for compensation under legislation which provided that citizens who had been punished for political protest during the Communist regime should receive redress. He obtained his compensation, but during the course of the litigation a letter was sent from the Romanian Intelligence Service suggesting (RIS) that from 1946 the applicant had been part of a Legionnaire movement. The applicant complained that he had been deprived of his right to respect for private life under Article 6. He also complained of breaches of Article 8, because, he said, the RIS held and could at any moment make use of information about his private life, some of which was false and defamatory.

[147] *See* the Judgement S. and Marper v. United Kingdom, Application Nos. 30562/04 and 30566/04, 4 December 2008. Available online: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-90051

[148] European Union Agency for Fundamental Rights, Data Protection in the European Union: the Role of National Data Protection Authorities, Luxembourg: Publications Office of the European Union, 2010, p. 13. Available online: http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf

[149] Fuster, G., Gellert, R., *Ibid.*, p. 74.

[150] Fuster, G., Gellert, R., *Ibid.*, p. 79.

[151] *Ibid.*, p. 75.

Regarding the recognition of the right of the protection of personal data, the EU Court of Justice avoided for a long time any reference to the fact that article 8 establishes this right. However, the Court seems to be applying the *modus operandi* of the right to private life to the protection of personal data. It was only in January 2008, in the judgement related to Promusicae v. Telefonica de Espana[152] that the Court, noting the mentioned direct reference found in the preamble of the e-Privacy Directive to article 8 of the Charter, observed that the said provision expressly proclaims the right to the protection of personal data[153]. However, this remark had no consequences for the reasoning of the Court, which had previously argued that the protection of personal data serves the protection of private life[154].

In May 2009, the Court pronounced the Rijkeboer judgement[155] in which it asserted that the purpose of the Data Protection Directive is to protect the privacy of the individuals. In this case, the Court also provided a detailed description of what it considered to be covered under such concept of privacy, allegedly encompassing many different facets of the right established in article 8 of the EU Charter, namely the right to the protection of personal data[156]. Thus, in this case privacy becomes synonymous with the right to personal data protection.

A lot of critics believe that the Court relies on a misconception of the specificity of the nature of right to the protection of personal data. Views have been expressed that both rights should be envisaged as of diverging essence. In Fuster et al. view, "privacy can be regarded as a positive freedom: it consists of granting a prerogative to an individual. Yet, because this prerogative is not absolute, some criteria on how to lawfully limit it have been laid down. In contrast, data protection can be coined as a negative freedom, i.e. protecting the freedom and autonomy of individuals not by empowering them with a determinate prerogative, but by challenging the behaviours of others, as they might infringe upon this very freedom"[157]. The basic assumption underlying data protection law is that data processing is unavoidable in modern societies. Therefore, once the conceptual differences between the two rights have been acknowledged, the set-up for the right to personal data protection in the case law of the EU Court of Justice might get clearer.

This section presented the way the jurisprudence in the field of data protection evolved in the last three decades and how it was shaped by the legislative reforms and changes that took place in this long period. Without going farther from the main question of this study, i.e. assess the way the new reform might affect the protection of the right to personal data, the next section will present some of the main challenges

---

[152] *See* the Judgement C-275/06, Promusicae v. Telefonica de Espana, 28 January 2008. Judgement available online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006J0275:EN:HTML

[153] *See* also Fuster, G., Gellert, R., *Ibid.*, p. 76.

[154] *Ibid.*, p. 77.

[155] *See* Judgement C-553/ 07, College van burgemeester en wethouders van Rotterdam v. MEE Rijkeboer, 7 May 2009. Available online: http://curia.europa.eu/juris/liste.jsf?language=en&num=C-553/07

[156] Fuster, G., Gellert, R., *Ibid.*, p. 77.

[157] *Ibid.*, p. 80.

regarding data protection, which have been identified by the European Union Agency for Fundamental Rights.

4.3. Challenges regarding the enforcement of data protection legislation

In 2010, before the proposal of a reform in data protection, the European Union Agency for Fundamental Rights identified a series of challenges for the data protection system in the Union. Which are the main issues that represent a concern and how should they be addressed? What should be done in order to find a solution for these challenges so that the data protection reform would be successful?

To begin with, FRA identified the *lack of independence of Data Protection Authorities (DPA)*[158]. It has been pointed out that there are concerns reported about the effectiveness and capability of the officers of DPA to perform their task with complete autonomy. According to FRA, DPAs should also play a role in the enforcement of the data protection system, by having the power to issue sanctions, including fines, or procedures that could lead to sanctions[159]. Another problem they experience is the limited powers that they possess (i.e. they are not endowed with full powers to investigate, intervene in processing operations, offer legal advice and engage in legal proceedings)[160]. In various member States, data protection officers are directly appointed by the Governments, a thing which has raised serious concerns[161]. In this regard, the EU seeks the effective independence of national DPAs from political branches of government[162]. The guarantee of independence is assured by the procedure of nomination and removal of the officers of the DPAs[163]. The control over the financial resources represents a second relevant element in ensuring the autonomy of supervisory authorities[164]. This is still an issue that has not been completely solved in the regulation. In this regard, a possible solution for the Member States could be to pay more attention to cultivating their public profile and focus on promoting their existence at national level, by also seeking closer cooperation with other human rights institutions and civil society organisations[165].

Secondly, another deficiency identified by FRA resides in the l*ack of enforcement of data protection system*. Surveys showed that in some Member States, prosecutions

---

158 European Union Agency for Fundamental Rights, Data Protection in the European Union: the Role of National Data Protection Authorities, Luxembourg: Publications Office of the European Union, 2010, p. 6.

159 European Union Agency for Fundamental Rights, Access to data protection remedies in EU Member States, Luxembourg: Publications Office of the European Union, 2013, p. 9.

160 European Union Agency for Fundamental Rights, Data Protection in the European Union: the Role of National Data Protection Authorities, Luxembourg: Publications Office of the European Union, 2010, p. 6.

161 *Ibid.*, p. 8.

162 Hustnix, P., The Role of Data Protection Authorities, In Reinventing Data Protection Authorities?. Springer, 2009, p. 131-137.

163 European Union Agency for Fundamental Rights, Data Protection in the European Union: the Role of National Data Protection Authorities, p. 8.

164 *Ibid.*, p. 8.

165 European Union Agency for Fundamental Rights, Access to data protection remedies in EU Member States, p. 53.

and sanctions for violations of data protection law are limited or non-existing[166]. FRA also showed that the legal systems of various Member States rule out the possibility to seek compensation for the violation of data protection rights. This is due to the difficulty of establishing the burden of proof, of quantifying the damages and because of the lack of support from the supervisory bodies[167] [168]. Therefore, the EU's objective is to guarantee for effective enforcement of data protection by granting the DPAs with the power to either issue sanctions or to initiate procedures that can lead to sanctions *ex oficio.*[169][170]

Thirdly, *the lack awareness of the EU citizens in regard to their rights* also represents a deficiency for the system. According to the Eurobarometer surveys on data protection published in 2008, the EU citizens were unaware of the existence of DPAs where they could claim reparation for the damage incurred[171] [172]. As showed above, it appears necessary that the DPAs should promote closer cooperation and synergy with other guardians of fundamental rights such as national human rights institutions and equality bodies to secure the right to an effective remedy[173]. In most national systems, DPAs together with the courts are the bodies most frequently involved in remedying data protection violations. Other non-judicial bodies and administrative institutions, such as the ombudsperson institution or a communication authority can offer assistance on different types of remedies[174]. The support and advisory role of intermediaries, in particular that of the civil society and organisations, throughout the process could also be useful[175]. However, it is not always clear what type of guidance a specific institution or body can provide. The EU Member States can improve the existing data protection mechanisms by taking the necessary steps to increase the awareness of the available complaint mechanisms and how they work[176]. Moreover, the FRA report showed that the Member States should also strengthen the

---

[166] European Union Agency for Fundamental Rights*,* Data Protection in the European Union: the Role of National Data Protection Authorities*,*, p. 6.

[167] *Ibid.*

[168] *See* also European Digital Rights, Data Protection Authorities, Brussels, 2012. Available online: http://protectmydata.eu/topics/data-protection-authorities/

[169] European Union Agency for Fundamental Rights, *Ibid.*, p. 8.

[170] *See* also Deloitte, The Modernization of European Data Protection Rules, p. 4. Available online: http://www.deloitte.com/assets/Dcom-Switzerland/Local%20Assets/Documents/EN/Audit/RCL/ch_en_the_modernization_of_european_data_protection_rules.pdf

[171] European Union Agency for Fundamental Rights, *Ibid.*, p. 6.

[172] The DPAs can also impose sanctions. For an example, See New Statesman, EU data-protection authorities launch joint action against Google, April 2013. Available online: http://www.newstatesman.com/business/technology/2013/04/eu-data-protection-authorities-launch-joint-action-against-google

[173] European Union Agency for Fundamental Rights, Data Protection in the European Union: the Role of National Data Protection Authorities, p. 8.

[174] European Union Agency for Fundamental Rights, Access to data protection remedies in EU Member States, Luxembourg: Publications Office of the European Union, 2013, p. 19.

[175] *Ibid.*, p. 19.

[176] *Ibid.*, p. 53.

professional competence of judges and lawyers by providing training sessions and adding emphasis on data protection in the legal curriculum[177].

Nonetheless, the other main deficiencies identified by FRA reside in the *lack of data protection in the former third pillar of the EU* and the exemptions from data protection for security and defence[178]. FRA has noted that while data protection is highly developed in the former first pillar of the EU, the data protection in the former pillar cannot be regarded as satisfactory[179]. The third pillar of the EU comprises areas such as police cooperation, the fight against terrorism and matters of criminal law where the need for data protection is especially important. Moreover, there is a lack of clarity regarding the extent of the exemptions and restrictions concerning public security, defence and State security[180]. In various Member States, these areas are excluded from the protection of data protection law. Because of this, a considerable large area is left unprotected with potentially serious consequences for fundamental rights protection[181]. Therefore, the main objective of the EU is to widen its protective regime. According to article 52, the limitations on data protection for security or defence reasons will still remain possible, but these limitations must be provided by the law and respect the essence of the right to protection of personal data and the requirement of proportionality[182]. This is still a key issue on which more must be done in order to reach an adequate legislative framework. Data national authorities should also get involved more in solving this issue[183].

4.4. The way forward for the EU data protection legislation reform

The many legal discussion that were associated with the reform, determined the postponement of the EU Data Retention Directive. In order to solve this situation, in 2012 the European Court of Justice asked the European Union Agency for Fundamental Rights (FRA) to deliver an opinion on the compliance of the Directive to fundamental rights. In this regard, in May 2012, FRA brought together experts to focus on the fundamental rights dimension of the data protection package[184]. The experts focused on the following main issues: the right to be forgotten, the right to portability,

---

[177] *Ibid.*

[178] European Union Agency for Fundamental Rights, Data Protection in the European Union: the Role of National Data Protection Authorities, p. 7.

[179] *Ibid.*, p. 8.

[180] *Ibid.*, p. 7.

[181] European Union Agency for Fundamental Rights, Data Protection in the European Union: the Role of National Data Protection Authorities, Luxembourg: Publications Office of the European Union, 2010, p. 7. Available online: http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf

[182] European Union Agency for Fundamental Rights, Data Protection in the European Union: the Role of National Data Protection Authorities, Luxembourg: Publications Office of the European Union, 2010, p. 8. Available online: http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf

[183] *See* also European Digital Rights, *Ibid.*

[184] European Union Agency for Fundamental Rights, Fundamental Rights: challenges and achievements in 2012, Luxembourg: Publication Office of the European Union, 2013, p. 103.

the independence and powers of data protection authorities and the issue of profiling. The results of the meeting were put together in a report published in May 2012[185].

Later in 2012, FRA, at the request of the European Parliament issued an opinion on the proposed EU data protection reform package. In this opinion, FRA suggested ways to strengthen its fundamental rights safeguards. In trying to find a solution to the criticism regarding the extension of powers of the European Commission, FRA suggested in its opinion to insert in the directive a general fundamental rights clause and an explicit guarantee that delegated and implementing acts, which are specific legislative powers given to the European Commission, cannot limit fundamental rights in any way[186]. The opinion observed that the proposed consistency mechanism contained in the draft regulation gives the Commission not only the power to adopt "a reasoned opinion aimed at the suspension of the draft measures of the national data protection authorities, but also the power to adopt implementing acts"[187]. On this point, FRA concluded that the proposed powers of the Commission may be difficult to reconcile with the guarantees of independence under Article 8(3) and 47 of the Charter of Fundamental Rights of the European Union and other international standards of independence[188].

Moreover, the opinion also suggested concrete amendments to the draft text in order to ensure a better balancing of key fundamental rights, such as freedom of expression, freedom of the arts and sciences, freedom to conduct business, the rights of the child or access to documents[189]. Besides this, another important issue which was brought forward by the opinion was the need to incorporate "sexual orientation" into the list of sensitive data, thus qualifying it for a higher level of protection[190]. The way these suggestions are going to be incorporated by the initiators of the data protection reform is still to be see, as currently the discussion the the data protection package is still ongoing.

The purpose of this last section was to present the situation regarding data protection in the EU, by firstly showing the current status of data protection in the EU, then by presenting some of the relevant jurisprudence in the field and thirdly by summarizing under a couple of points the main challenges regarding the enforcement of data protection legislation.

---

[185] *See* European Union Agency for Fundamental Rights, FRA Symposium report – European Union data protection reform: new fundamental rights guarantees, 10 May 2012. Available at: http://fra.europa.eu/sites/default/files/fra_uploads/2280-FRA-Symposium-data-protection-2012.pdf

[186] European Union Agency for Fundamental Rights, Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package, FRA Opinion 2/2012, Vienna, 1 October 2012. Available online: http://fra.europa.eu/sites/default/files/fra-opinion-data-protection-oct-2012.pdf

[187] European Union Agency for Fundamental Rights, Fundamental Rights: challenges and achievements in 2012, Luxembourg: Publication Office of the European Union, 2013, p. 105.

[188] *Ibid.*, p. 105.

[189] *See* European Union Agency for Fundamental Rights, Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package, FRA Opinion 2/2012, Vienna, 1 October 2012.

[190] *Ibid.*

5. Conclusion

Even a shallow lecture of this study can show that there is a web of norms in the field of data protection, aiming to build a satisfying fundamental rights framework for data protection. However, looking at the existing jurisprudence and at the comments provided in the literature regarding the new reform in data protection, in my opinion, there is still a long way to get a balance between the demands of the European security requirements and the fundamental rights of the individuals. This is why the revision of the EU Data Protection Directive was postponed, as national implementation legislation continued to face constitutional challenges in a number of Member States. Having a closer look at the proposed objectives of the data protection reform, there are still areas in which confusion is bound to occur. That is why the debates and discussions on the reform package are still ongoing, generating disagreements and contradictions at the EU level. Despite this, as any other process, in my opinion, this reform still constitutes a step further for the protection of the right to data protection and its possible future implementation definitely represents a milestone in the protection of human rights at the EU level.