IUS ET SCIENTIA (ISSN: 2444-8478) 2017, Vol. 3, nº 2, pp. 37-62
Crystalie Bourcha, Maria-Louiza Deftou, Dr. Anthi Koskina: *DATA MINING* OF BIOMETRIC DATA: REVISITING THE CONCEPT OF PRIVATE LIFE?
FECHA DE ENVÍO DE ORIGINAL: 15.11.2017 FECHA DE ACEPTACIÓN: 12.12.2017
DOI: http://dx.doi.org/10.12795/IETSCIENTIA.2017.i02.04

DATA MINING OF BIOMETRIC DATA: REVISITING THE CONCEPT OF PRIVATE LIFE?

Crystalie Bourcha, Maria-Louiza Deftou, Dr. Anthi Koskina *

Abstract. Over recent years, a whole new process known as *data mining*, equivalent to automated techniques processing large sets of data in order to extract patterns, relationships, trends and other information not traceable through usual 'human' reading, has been largely gaining in repute.

By taking advantage of the seemingly indefinite opportunities enabled by applications of data mining techniques, various fields of scientific or medical research, business transactions, state-related and other security-concerned activities, could gain unprecedented benefits. However, notwithstanding established data protection principles reserved also for biometric information, data mining practices, inherently intrusive in the private sphere of individuals, have generated various concerns and controversy.

As these emerging technological developments create new challenges to the protection of personal data, including primarily the most sensitive category of biometric data, the effectiveness of the concept of privacy under the European Convention on Human Rights (ECHR) and of the existing EU data protection legislation in securing an adequate legal framework is facing a new ordeal.

This paper seeks to review, especially in the aftermath of the recent Luxembourg Court's case law, whether evolving data mining practices materialize the need of adjusting the legal treatment of biometric data protection.

Keywords: Data mining – Biometric data – Private life

*Dr. Anthi Koskina is professor of law, College IdEF-Paris XIII, Athens-Greece, akoskina@idef.gr .Maria-Louiza Deftou is Attorney at law(Athens Bar Association), PhD Candidate at the National and Kapodistrian University of Athens and Researcher at Athens PIL, mardeftou@law.uoa.gr. Crystalie Bourcha is Attorney at Law, registered with the Athens Bar Association, PhD Candidate at the National and Kapodistrian University of Athens and Researcher at Athens PIL, cr.bourcha@gmail.com .
This article was presented at the International Workshop "International Biolaw and… Interactions with Environmental, Human Rights and Health law" in Malaga(Spain), 27 October 2017, hosted by the University of Malaga and the ESIL Biolaw Interest Group.

IUS ET SCIENTIA (ISSN: 2444-8478) 2017, Vol. 3, nº 2, pp. 37-62
Crystalie Bourcha, Maria-Louiza Deftou, Dr. Anthi Koskina: *DATA MINING* OF BIOMETRIC DATA: REVISITING THE CONCEPT OF PRIVATE LIFE?
FECHA DE ENVÍO DE ORIGINAL: 15.11.2017 FECHA DE ACEPTACIÓN: 12.12.2017
DOI: http://dx.doi.org/10.12795/IETSCIENTIA.2017.i02.04

I. Data mining of biometric data: gains and losses

A. Defining Data Mining

The *data mining* (or *pattern mining*) process[1] is an interdisciplinary subfield of computer science which results in the computational –or automated– extraction of understandable patterns in large volume of data sets, also referred to as '*big data'*. The process combines statistics and artificial intelligence tools with database management, so as to obtain previously unknown information.

As it is based on modeling techniques[2] which focus on extracting rules describing specific patterns within the data –e.g. models, sequential associations, etc.–, the results' reliability is closely dependent on the source and number of the collected information, since a wrong input will inevitably result in a wrong output.[3]

According to the types of knowledge they seek to find, modeling techniques used in data mining are divided in two main categories:

(a) The *descriptive modeling*, based on clustering or association rule mining, which aims at extracting patterns or discovering hidden relationships (i.e. summary statistics, anomaly detection, etc.) among large data sets divided into random groups, and

(b) The *predictive modeling*, standing on classification and regression analysis,[4]aiming at predicting previously unknown or hidden data, which can be decisive for scientific progress in fields like medicine or pharmaceuticals. In

[1] Zhang Y., '*TIETS34 Seminar: Data Mining on Biometric identification'* ,Computer Science, School of Information Sciences' University of Tampere, <http://www.uta.fi/sis/tie/seminarbi/schedule/Introduction%20I.pdf.> accessed 13 November 2017.

[2] "Modeling is simply the act of building a model in one situation where you know the answer and then applying it to another situation that you don't (…)".You note these similarities and build a model that includes the characteristics that are common [*to the ones you found in similar situations*]. With these models in hand you sail off looking [*for the same results*] where your model indicates it most likely might be given a similar situation in the past. Hopefully, if you've got a good model, you [*will*] find (…).Once the model is built it can then be used in similar situations where you don't know the answer", Thearling K., 'Information about analytics and data science / An Introduction to Data Mining' (2012) <http://www.thearling.com/text/dmwhite/dmwhite.html> accessed 13 November 2017.

[3] See for data mining applications in medicine Esfandiari N., Reza Babavalian M., Eftekhari Moghadam A.-M. &Kashani Tabar V., 'Knowledge discovery in medicine: Current issue and future trend' [2014],41 *Expert Systems with Applications* 4434.

[4] Regression analysis is a statistical technique that estimates and predicts relations between variables.

that case, the groups are predefined and the search is targeted at finding patterns explaining the differences among them.

Data mining, believed to be free from human bias inherent in the study of small amounts of data, is based on the collection –or enrollment– of various types of information that has been greatly facilitated by substantial technological advancements, like the significant expansion of computer storage capacities. Some of data mining applications appear quite promising and have, therefore, become increasingly popular, in a variety of fields, including business transactions (e-commerce and e-banking, CRM-Customer Relationship Management, insurance, retail), research activities (astronomy, clinical medicine, genetic data analyzing) and state security (financial fraud or credit card fraud detection, based on the consumer's purchasing behavior pattern[5] , border control or detection of criminal and terrorist activities).

However, as a result of technological boundaries, the data mining techniques aren't completely reliable.[6] Errors might occur due to the incorrect integration of data into a data set, or due to the integration of missing data, wrong data or non-standard representation of the same data (named *dirty data*). In addition to that, the design and functionality –i.e. the technology's purpose, which is always adapted to a specific context of use[7]– of the data mining algorithms themselves[8]will usually "reflect the values of [their] designer[s] (…) if only to the extent that a particular design is preferred (by the designer)as the best or most efficient option".[9]

[5] See, for instance, an application of data mining techniques by the Gemalto Assurance Hub, to detect frauds in the context of online banking services, 'La biométrie et le « machine learning »: la combinaison gagnante de Gemalto pour plus de confiance dans les services bancaires en ligne'(2017) <https://www.gemalto.com/press/Pages/Biometrie-et-machine-learning-La-combinaison-gagnante-de-Gemalto-pour-plus-de-confiance-dans-les-services-bancaires.aspx> accessed 13 November 2017.
[6]Pointedly, "*At Frankfurt Airport, a system with an FRR of 1 % would produce more than 1,000 false alarms per day",* See Hornung G., 'The European Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards' [2007] 4 *SCRIPT ED* 257.
[7] "It thus cannot be assumed that an observer's interpretation will correctly reflect the perception of the actor rather than the biases of the interpreter", Mittelstadt B.D., Allo P., Taddeo M., Wachter S. and Floridi L.,'The ethics of algorithms: Mapping the debate'[2016] *Big Data & Society*, 1,<https://www.academia.edu/29344788/The_Ethics_of_Algorithms_Mapping_the_Debate>, accessed 13 November 2017.
[8] "The most commonly used techniques in data mining are: Artificial neural networks, Decision trees, Genetic algorithms**,** Nearest neighbor method, Rule induction etc.", Thearling K., supra note 2.
[9] "Development is not a neutral, linear path; there is no objectively correct choice at any given stage of development, but many possible choices (Johnson, 2006)", Mittelstadt B.D., supra note 7.

FECHA DE ENVÍO DE ORIGINAL: 15.11.2017 FECHA DE ACEPTACIÓN: 12.12.2017
DOI: http://dx.doi.org/10.12795/IETSCIENTIA.2017.i02.04

In this context, the purpose driving data collection and use (e.g. medical data banks can be used for public health purposes or scientific research), as well as the identity of the collector, play a major role.[10]

B. Data Mining applications in biometric data

Inevitably, the development of these cutting-edge technological advancements paved the way of the application of data mining methodology in biometric data. Biometrics are defined as "the measurement and analysis of unique physical(fingerprints or hand geometry, facial thermogram, iris, retinal pattern etc.) or behavioral characteristics(like human voice**,** keystroke dynamics[11] helpful in finding out passwords' or personal identification numbers' frauds etc.), especially as a means of verifying personal identity".[12]

Biometric data are unique to each person and of a permanent character as they cannot be modified nor be susceptible to alteration. In addition to that, they are collectable and quantitatively measurable, as they can be easily scanned and quantified by sensors.[13] Due to the said specific features, they are considered to be more reliable in verifying a person's identity.

In practice, *biometric sensors* scan individuals' characteristics to create a digital representation which will be further processed by a *feature extractor* in order to generate a *template* (i.e. a compact but expressive representation). The templates are then stored in a central database or recorded on movable devices, like magnetic cards, biometric passports, visas or smartcards. They can be analyzed alone or in combination with other types of data–through *multimodal biometric systems*– in order to treat

[10] For instance, a private company is more likely to use information, extracted e.g. from employees' database,for commercial purposes, than a public entity.
[11]Gutierrez F., Lerma-Rascon M., Salgado-Garza L. and Dr. Cantu F., 'Biometrics and Data Mining: Comparison of Data Mining – Based Keystroke Dynamics Methods for Identity Verification in *MICAI '02 Proceedings of the Second Mexican International Conference on Artificial Intelligence: Advances in Artificial Intelligence*, (2002 Springer).
[12]See relatively the definition of the *Merriam-Webster* scientific dictionary <https://www.merriam-webster.com/dictionary/biometrics > , accessed 13 November 2017**.**
[13]See *inter alia* Jain A., Hong L., Pankanti S., 'Biometric identification' [2000], 43 *Communications of the ACM* , 91. See, also, Hernández-Aguilar J.A., Zavala C., Díaz O., Burlak G., Ochoa A. and César Ponce J., 'Biometric Data Mining Applied to On-line Recognition Systems' in Midori Albert (eds), *Biometrics - Unique and Diverse Applications in Nature*, *Science, and Technology* (In tech 2011).

FECHA DE ENVÍO DE ORIGINAL: 15.11.2017 FECHA DE ACEPTACIÓN: 12.12.2017
DOI: http://dx.doi.org/10.12795/IETSCIENTIA.2017.i02.04

together different properties of the same identifier or different perceptions of the same identifier as perceived by different sensors.[14]

Data mining technology, especially when applied to biometric data, can produce outstanding scientific results.[15] However, biometrics seem to be mostly used for verification purposes as a match comparison, named authentication (one-to-one search) or as an associative identification system (one-to-many search),[16] where constructed templates are instantly and electronically checked through central databases, so as to verify a claimed identity and to describe, if required, a pre-registered person.[17]Thus, the consideration of biometrics as more reliable than conventional strategies for identity verifications led to their preferential use for commercial and –mainly– public security purposes.

On the other hand, strong privacy concerns were raised by scholars for inappropriate use of biometric information. These concerns were mostly attributed to the nature of the collection and retention process, since biometric measurements are mainly collected in remote authentication settings, notwithstanding the fact that data mining in biometrics is also used for authentication purposes in other areas, not always correlating with public security issues. In the era of proliferation of terrorist attacks, it is fingerprints and other biometric information that governmental authorities are after. Biometric data are, nowadays, captured in travel documents of all kinds, retained at central repositories of such information, interconnected and, then, opened up to police searches. In this context, the risk of *fishing expeditions,* such as these aiming at finding criminals amongst a population of potential suspects[18], or the tendency of misusing

[14]Sheeba R. and Subha M, 'Data Mining Applications in Biometrics :Multimodel Scheme with Facial and Iris Recognition Based on Gabor Filter' [2013] 2 *IJERT* 12.
[15]" (…) *in 2000, Iceland's parliament sold exclusive rights to all the genetic and genealogical data from each of its 275,000 citizens to the U.S. company de CODE Genetics. Soon thereafter, deCODE signed a $200 million contract with Hoffman La Roche to search for several common human genetic diseases. (…). The Iceland genetic database sale, for example, led to identification of genes linked to disease (…)*", in Kaplan B., 'How Should Health Data Be Used? Privacy, Secondary Use, and Big Data Sales'[2016] 25*Cambridge Quarterly of Healthcare Ethics* 312.
[16]Baldaccini A., 'Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases'[2008] 10 *European Journal of Migration and Law* 31. See, also, Sheeba R., supra note 14.
[17]National Consultative Ethics Committee for Health and Life Sciences, OPINION N° 98. France (2013)<http://www.ccne-ethique.fr/en/publications/biometrics-identifying-data-and-human-rights#.Wgr6TYjQDIU> accessed 14 November 2017.
[18] This applies mainly to individuals with specific characteristics or handicaps, See also Baldaccini A.,supra note 16, 5.

FECHA DE ENVÍO DE ORIGINAL: 15.11.2017 FECHA DE ACEPTACIÓN: 12.12.2017
DOI: http://dx.doi.org/10.12795/IETSCIENTIA.2017.i02.04

biometrics referred to as a "*slope leading from identification to identifying behavior*"[19] rendered this constantly evolving technology as one of the most debatable scientific breakthroughs of the last decades.

Hence, the widespread use of data mining technologies raised two main privacy issues [20]: the anonymization of biometric data and the automated character of the procedure. In general terms, the right to privacy is expected to be preserved through *data anonymization techniques*[21] –and a new challenge for information engineers is presented– but the task seems to be, at the same time, unrealistic, as the available number of linkable data is dramatically increasing (photos, personal data, activities and hobbies voluntarily posted on social networks etc.).[22] At the same time, when it comes to healthcare, responsible scientific treatment of *non*-anonymized biometric data could undoubtedly serve as the basis for better healthcare services, advancements in medical treatment, developments in pharmaceuticals, etc., all core issues for public interest concerns.

However, despite the wide variety of beneficial results in this field,[23] anonymity pertaining to biometric information is considered as the critical factor of preserving privacy. Since such data , if *non-anonymised*, can be easily matched with medical data creating personal health profiles from birth to death, the door is left open for data controllers or machines of modern medicine to invade the individuals' private sphere with potentially detrimental effects.[24]

Another issue of substantial concern emanates from the automated character of these practices that excludes *ipso facto* the fulfillment of the prior consent principle, basic prerequisite in data protection law. In particular, the data subject is not able to

[19]Ibid., 3.
[20]Sermondadaz S., 'Avec les Big Data et la biométrie, Big Brother s'invite au bureau, Sciences et Avenir', [2017], https://www.sciencesetavenir.fr/high-tech/data/avec-les-big-data-et-la-biometrie-big-brother-s-invite-au-bureau_110644 accessed 14 November 2017.
[21] See in relation to data anonymization policies Gal T.Z., Kovacs G., Kardovacks Z., 'Survey on privacy preserving data mining techniques in health care databases' [2014] 6 *Acta Univ. Sapientiae, Informatica,* 1, 33.
[22]Scientists tend to argue against anonymization: "the more you try to hide sensitive private information, the less valuable it is for analysis (…). If personal or sensitive data (…) can only be accessed, transferred or handled by entities explicitly stated in regulations, and with the consent of the data subject, researchers working with such databases will stumble very early in the legal limitations",Ibidem.
[23] See Kaplan,supra note 15, 319
[24] See in this respect Rajaretnam T., 'Data Mining and Data Matching: Regulatory and Ethical Considerations Relating to Privacy and Confidentiality in Medical Data' [2014] 9 *J. Int't Com. L. & Tech.* 294, 300.

FECHA DE ENVÍO DE ORIGINAL: 15.11.2017 FECHA DE ACEPTACIÓN: 12.12.2017
DOI: http://dx.doi.org/10.12795/IETSCIENTIA.2017.i02.04

grant his/her consent to potential data mining applications, when the relevant information is being collected.[25]

Nevertheless, as the trust placed on data mining technics can result in a "*de-responsibilisation of human actors or a tendency to hide behind the computer*[26]", and bearing in mind that legislative regulation can either boost or halt the advancement of science and technology, regulatory delimitation of data mining over biometric features should be the focus of particular legal concerns.

Thus, aside from the most positive data mining applications used in healthcare or from the most intrusive ones used in governmental policies, the EU and international legal mechanisms are confronted with newly introduced challenges that require a rigorous evolution of data protection legal framework in order to tackle the detrimental implications of these developments for a more peaceful enjoyment of the right to private life.

II. EU data protection standards: towards an adequate shelter for biometric data?

A. The legislative foundations of European data protection

Within the context of the ongoing technological progress and the cross-border exchange of information, especially *via* Internet, the multiple challenges posed to human rights in relation to the protection of personal data could not have been ignored by the EU legal order or the Council of Europe (CoE) system. Against this background, the European data protection is definitely the most luminous example of legal evolution during the latest decades. In response to the emerging developments in the field of information technology in the 1960s, the concept of privacy in the context of Art.8 of the ECHR, formulated in 1950, needed to be revisited in order to meet with the new technological advancements and to guarantee the protection of the individuals' personal

[25] Ibidem.
[26] Zarsky T., 'The trouble with algorithmic decisions an analytic road map to examine efficiency and fairness in automated and opaque decision making' [2016] 41 *Science, Technology & Human Values* 1,121.

data. As a response to this growing need, the Council of Europe[27] adopted, at first, various resolutions with reference to Art.8 ECHR and, in 1981, adopted the Convention on Personal Data[28](Convention 108), a legally binding instrument providing specific safeguards against abuses from private actors or the state's authorities concerning the fair and lawful collection, storage and automatic processing of personal data. In this respect, the Strasbourg Court applied broadly the notion of private life expanding the protection offered by the Convention, at first, to cases related to interception of telephone communications (as in *Klass*[29] in 1978 and in *Malone*[30] judgment in 1984) and, progressively, to cases with regard to data stored in computers, to video-surveillance in *Peck*[31] or storage of such data to secret registers (as it was the case in *Leander*[32] and *Rotaru*[33]).

This constant evolution on the Strasbourg Court's interpretation of the concept of private life towards a more effective protection of personal data, along with the numerous regulatory transformations in the EU Member states fostered the conditions under which the EU adopted several legal instruments with the aim to harmonise the national data protection legislations of its Member States. To this end, the EU *Data Protection Directive,*[34] adopted in 1995, was seen as "the leading force of globalizing data protection"[35]incorporating most of the principles and requirements of the CoE system.[36]The Directive was later followed by the EU *Regulation 45/2001*[37]addressing

[27]CoE, Committee of Ministers (1973), Resolution (73) 22 on the protection of the privacy of individuals *vis-a-vis* electronic data banks in the private sector, 26 September 1973; CoE, Committee of Ministers (1974), Resolution (74) 29 on the protection of the privacy of individuals *vis-a-vis* electronic data banks in the public sector, 20 September 1974.
[28]Council of Europe, Convention for the Protection of Individuals with regard to automatic processing of personal data, ETS No.108.
[29]*Klass and Others v. Germany*,Application no. 5029/71, 6 September 1978
[30]*Malone v. the United Kingdom*,Application no. 8691/79, 2 August 1984
[31] *Peck v. the United Kingdom,*Application no. 44647/98, 28 January 2003
[32]*Leander v. Sweden,*Application no. 9248/81,23 March 1987
[33]*Rotaru v. Romania*[GC],Application no. 28341/95, 4 May 2000
[34]Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data , OJ [1995] L 281
[35]Birnhack M., The EU Data Protection Directive: An Engine of a Global Regime,(2008) 24 *Computer Law & Security Report*508, 512.
[36]For the connection between the Convention 108 and the Data Protection Directive see the *Handbook in European Data Protection*,2014 <http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf> accessed 10 October 2017 ,p.18
[37]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 institutions and bodies of the Community and on the free movement of such data, [2001]OJ L 8.

FECHA DE ENVÍO DE ORIGINAL: 15.11.2017 FECHA DE ACEPTACIÓN: 12.12.2017
DOI: http://dx.doi.org/10.12795/IETSCIENTIA.2017.i02.04

EU legal bodies and by two more Directives covering more specified fields of the legal protection of personal data, namely the *Directive on privacy and electronic communications*[38] and the *Data Retention Directive.*[39]Under the aforementioned legal framework, the Court of Justice of the European Union (CJEU), in the light of the dynamic jurisprudence on the matter of its Strasbourg counterpart, extended the scope of application of the Data Protection Directive and went so far as to apply its provisions outside the area of the internal market.[40]

However, apart from the guarantees provided by the EU soft law with regard to the right to data protection, its explicit recognition as a fundamental right of equivalent value within the EU legal framework came with the adoption of the *Charter of Fundamental Rights of the Rights of the European Union* (EU Charter or EUCFR).[41] The EU Charter, which came into force on the 1st December 2009, not only contained a provision pertaining to the respect for private and family life, but established explicitly the right to data protection as enshrined in Art.8 EUCFR.[42]Drafted a few years after the adoption of the Data Protection Directive, Art. 8 of the Charter must be deemed as reflecting pre-existing EU data protection law and relevant jurisprudential principles. In this regard, the Charter, not only ensures the right to data protection but establishes also key data protection principles related to the consent of the data subject, the establishment of independent authorities supervising the implementation of the said principles and the access to documents.[43]

[38]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*), [2002]OJ L 201.
[39] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC,*(Data Retention Directive),* [2006] OJ L 105/54, invalidated on 8 April 2014.
[40] De Hert P.,Gurtwirth S., 'Data protection in the case law of Strasbourg and Luxemburg : constitutionalisation in action' in Gurtwirth S., Poullet Y., De Hert P., Nouwt S. , De Terwangne C. (eds),*Reinventing Data Protection ?* ,(Springer Science, Dordrecht 2009),18-19.
[41] Charter of Fundamental Rights of the European Union [2012] OJ C 326/391. The Charter was granted legally binding force when the Treaty of Lisbon entered into force on 1 December 2009.
[42] Article 8 of the EU Charter reads as follows: "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 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."
[43]Handbook on European data protection law , European Union Agency for Fundamental Rights and Council of Europe (2014) 20,21.

IUS ET SCIENTIA (ISSN: 2444-8478) 2017, Vol. 3, nº 2, pp. 37-62
Crystalie Bourcha, Maria-Louiza Deftou, Dr. Anthi Koskina: *DATA MINING* OF BIOMETRIC DATA: REVISITING THE CONCEPT OF PRIVATE LIFE?
FECHA DE ENVÍO DE ORIGINAL: 15.11.2017 FECHA DE ACEPTACIÓN: 12.12.2017
DOI: http://dx.doi.org/10.12795/IETSCIENTIA.2017.i02.04

B. The enhanced protection of the CJEU in data protection cases

i. Google Spain: the application of data protection rules in search engines

It is in this context that the recent and famous case of *Google Spain*[44] should be examined with regard to the applicability of data protection legislation to *internet search engines*. In the light of several post-Lisbon judgments [45] of the CJEU recognizing the *valeur juridique* of the EU Charter and enhancing the individuals' protection through a rather strict interpretation of the data protection law, this milestone ruling of the Court was seen by some scholars as conferring to the data subjects the *right to be forgotten* and to control, therefore, their online reputation. Particularly, in *Google Spain,* M. Gonzalez who asked for the deletion of the published information in the online version of *La Vanguardia* newspaper regarding his personal data related to his participation to a real-estate auction held in 1998, alleged *inter alia* that when an internet user searched for his full name in the Google search engine, he would obtain access to two links to the newspaper's website on which the announcements with his personal data appeared. As the publisher of *La Vanguardia* and *Google Spain*, which in the meantime forwarded M. Gonzalez's request to *Google Inc.*, denied to remove or rectify the relevant information, the plaintiff, addressed subsequently his complaint to the Spanish DPA. The latter rejected the request as far as the newspaper was concerned, ordering, however, Google Spain to delist the aforementioned information from its search results.

Under this factual basis, the Court was expected to pronounce on the material scope[46] of the Data Protection Directive and particularly on whether the activity of internet

[44] Case C-131/12,*Google Spain SL και Google Inc. v Agencia Española de Protección de Datos (AEPD) and MarioCosteja González* [2014]ECLI:EU:C:2014:317.
[45] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007,[2007] OJ C 306/1.
[46] Regarding the material scope of the Directive's application see also Kulk S. and ZuiderveenBorgesius F.,**'***Google Spain v. González*: Did the Court Forget about Freedom of Expression?' [2014] *European Journal of Risk Regulation,*3 ; Kuner C., 'The Court of Justice of the EU Judgment on Data Protection

FECHA DE ENVÍO DE ORIGINAL: 15.11.2017 FECHA DE ACEPTACIÓN: 12.12.2017
DOI: http://dx.doi.org/10.12795/IETSCIENTIA.2017.i02.04

search engines, namely indexing automatically, storing temporarily and making available information published on different websites to internet users as per a particular order of preference[47], fall within the notion of "*processing personal data*" ofArt.2(b) of the Directive. The Court found the latter applicable to search engines operators like Google, as it considered them *controllers of the processing.*[48]In response to Google's allegations that no personal data processing relating to its search engine took place in Spain and that the said processing was exclusively carried out by *Google Inc.*, the Court adopted an extraterritorial interpretation, when examined the territorial scope of the aforementioned legislation.[49]More precisely, the Court ruled that the activities of the subsidiary are "*inextricably linked"* to those of the search engine operator such as the activities of the Google headquarters in the U.S.A in view of the fact that these activities allow *Google Inc.* to be economically workable.[50]

Finally, the Court was asked about the extent of the responsibility of the search engines operators and, therefore, the applicability in the present case of Art.12(b) and 14(1)(a) of the Data Protection Directive establishing the right to erasure, rectification or blocking of the processing of personal data. Unlike the position of *AG Jääskinen* on the matter,[51] according to the CJEU's assertion these provisions should be interpreted as granting to the data subject the right to have a search engine delist from its search results the links to third parties' websites related to his name. However, the Court emphasized that this right must be balanced with the legitimate interests of the internet searchers with regard to the relevant provisions of the Charter, namely Art.7 and Art.8.

From the fundamental rights' perspective, even though it is clear -especially after the attribution of full legal effect to the Charter- that the CJEU opting for a broader interpretation of the relevant legislation sought to ensure a higher level of protection for the EU citizens with regard to data protection law, this ruling caught many by surprise. In *Google Spain,* the Luxembourg Court definitely made some significant pronouncements. For the first time -and before the adoption of the General Data Protection Regulation- recognized explicitly the right of an individual to have his/her

---

and Internet Search Engines', *LSE Law, Society and Economy Working Papers 3/2015* < http://eprints.lse.ac.uk/61584/> accessed 15 November 2017, 7.

[47] See *Google Spain*, supra note 44,paras 20-21.

[48] Ibid, para.33.

[49] Ibid, para 55.

[50] Ibid, para 56.

[51] Opinion of AG Jääskinen in *Google Spain* delivered on 25 June 2013.

FECHA DE ENVÍO DE ORIGINAL: 15.11.2017 FECHA DE ACEPTACIÓN: 12.12.2017
DOI: http://dx.doi.org/10.12795/IETSCIENTIA.2017.i02.04

personal data suppressed from the list of search results made available by an internet search engine pursuant to a search based on the individual's name. Nevertheless, the Court's judgment dealt with only one aspect of the right to be forgotten as enshrined for the first time in Art. 17 GDPR[52], since it only focused on its application to internet search engines. It, thus, seems inaccurate to misinterpret the decision as concluding to a comprehensive recognition of the right to be forgotten.[53]

However, the key judgment in *Google Spain* captures perfectly the willingness of the CJEU to enhance data protection legal standards while implementing the Lisbon framework particularly in the light of the proposed EU *General Data Protection Regulation*[54] in 2012. However, its implications raised questions as the Court seemed reluctant to shed light to several issues with regard to the disproportionately broad scope of the Directive's application and the exercise of balancing of the individuals' fundamental rights. Hence, as Kuner correctly deduced "the judgment provides a strong affirmation of online data protection rights, but fails to indicate a way forward for their effective implementation and realization, the development of which will likely be a struggle for data controllers, DPAs, and courts".[55]

As previously discussed, striking the correct balance in the data protection legal field is not a new territory for the EU judges but now, it is under the umbrella of the EU Charter that this exercise will be constantly carried out and this time, not only between fundamental rights and EU internal market freedoms, but also between conflicting fundamental rights both embodied in the Charter.[56]

---

[52] This actually constitutes one of the limitations of the judgment. Judging from the notion of Internet search engines as seen in the Google Spain decision, search engines like Google, Yahoo etc are covered but it remains unclear whether a number of others are left out. For instance the question remains open for websites with large-scale search function such as social networks, Internet archives, news databases, which are also overly used by millions of individuals.

[53]See also Iglesakis I., 'The Right To Be Forgotten in the Google Spain Case (case C-131/12): A Clear Victory for Data Protection or an Obstacle for the Internet? [2014] 12 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2472323>accessed 12 November 2017. See also Supra note 46, Kuner , 7

[54] The EU General Data Protection Regulation explicitly enshrines the "right to be forgotten".(Art.17)Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ EU L 119/1, 4 May 2016 <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC>accessed 11 November 2017.

[55] Supra note 46,Kuner, 21

[56] Fontanelli F.,'The European Union's Charter of Fundamental Rights two years later'[2011]3*Perspectives on Federalism* 3.

FECHA DE ENVÍO DE ORIGINAL: 15.11.2017 FECHA DE ACEPTACIÓN: 12.12.2017
DOI: http://dx.doi.org/10.12795/IETSCIENTIA.2017.i02.04

ii. Digital Rights Ireland: the end of Data Retention Directive

The abovementioned tendency was manifestly confirmed in the landmark *Digital Rights Ireland* ruling,[57]in which the Luxembourg Court did not restrict itself to invalidate some aspects of the EU legislation under scrutiny, but opted for striking down the Data Retention Directive[58] in its entity. In the case at hand, the preliminary reference procedure, initiated by the Irish High Court and by the Austrian Verfassungsgerichtshof, touched upon the legality and, thus, the validity of the said Directive in the light of Art.7 and 8 of the Charter. In the aftermath of the terrorist attacks in Europe, the Directive placed an obligation on Internet and telephone service providers to retain specific types of data relating to communications of individuals for security purposes. These retained data were telecommunications, traffic data in regard to e-mails, internet access and internet telephony, location data and data needed to identify a subscriber or a registered user. Despite the lack of a legal basis for retaining the content of these telecommunications, the whole background of the Directive appeared problematic.[59]

The Court focused, first and foremost, on the validity of the Directive at stake in light of the rights to privacy, data protection and freedom of expression as embodied in the EU Charter. After having declared the relevance of Art.7 and 8 with regard to the validity of the Directive, the CJEU stated that "those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."[60]

---

[57] Joined cases C-293/12 and C-594/12,*Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014] ECLI:EU:C:2014:238.

[58] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, O.J. 2006, L 105/54.

[59] See Lynksey O., 'The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: *Digital Rights Ireland***,** Joined Cases C-293 & 594/12, *Digital Rights Ireland Ltd and Seitlinger and others*, Judgment of the Court of Justice (Grand Chamber) of 8 April 2014,nyr.,[2014]'51*Common Market Law Review* 6.

[60] Supra note 57,*Digital Rights Ireland* judgment, para 27.

FECHA DE ENVÍO DE ORIGINAL: 15.11.2017 FECHA DE ACEPTACIÓN: 12.12.2017
DOI: http://dx.doi.org/10.12795/IETSCIENTIA.2017.i02.04

Therefore, the Court ruled that the obligations deriving from the Directive to retain data as well as the access to that data by the MS's authorities constituted an interference with the right to privacy and, since the Directive was also providing for processing of personal data, it violated the right to the protection of personal data.

In relation to the justification of the infringement, the CJEU examined the proportionality of the violation pursuant to Article 52(1) EUCFR and stressed that the essence of the rights at stake was respected. Subsequently, it attempted to ascertain whether the *Data Retention Directive* fulfilled an objective of general interest and did not go beyond what was suitable to achieve its purpose, concluding that, under the circumstances of the present case, the Directive fulfilled this purpose.

With regard to the examination of the final element of necessity of the proportionality test, the CJEU reiterated that derogations from fundamental rights should be accepted only when strictly necessary and held that the Directive did not provide clear and precise rules regarding the extent of the interference.[61] The EU legislature did not require a clear and strong connection between the data retained and serious crime or public security.[62] Additionally, the Directive failed to designate particular substantive and procedural conditions delimitating the access and use of the data retained by competent national authorities.[63] Regarding data security, the Directive lacked clear safeguards for the protection of the retained data. Moreover, the Directive abstained from clarifying that the data must be retained within the European Union and, therefore, within the scope of control of national Data Protection Authorities. On these grounds, the Directive was declared *ab initio* invalid by the Court.

The Court, for the first time, blatantly used the EU Charter as a *vehicle* to strike down an entire EU Directive and to put severe pressure on EU institutions in order to modify the legal context of the retention of data, confirming the tremendous significance of the protection of privacy and data protection within the EU.

The first and more practical consequence of this milestone judgment relies on its immediate effect. Since the Court's judgment manifestly declared the data retention legal scheme as incompatible with the EU Charter, all legislative measures adopted by the member states in the aim of implementation of the said Directive will not bear

[61] Ibid., para 56.
[62] Ibid., para 59.
[63] Ibid., para 64.

judicial scrutiny. Thus, as Federico Fabbrini noted, "the effects of the ECJ judgment, therefore, are likely to spill over into the national legal system, ensuring a new advanced standard of protection for privacy and personal data throughout the EU".[64]

During the last decades, the European judicial *fora* were repeatedly confronted with cases in which human rights were clashing with public interest objectives. As for the reasoning which the Court did provide, the surprising aspect of the CJEU's appraisal is that the Court clearly makes a distinction between the two: respecting the very essence of a right is not sufficient because even if the latter is respected, the legislation at stake can still be disproportionate.

Another significant element of the *Digital Rights Ireland* ruling is, as Steve Peers correctly stressed, "the development of a doctrine indicating when strict scrutiny of the EU legislature's interference with fundamental rights should apply."[65] That definitely relies on the ECtHR's relevant jurisprudence, cited many times by the Court in the course of its reasoning.[66] Nevertheless, the application of the EU Charter by the CJEU gave the opportunity to the latter to raise even more the standards posed by its Strasbourg peer which, clearly served as "springboard" for the development of the CJEU's case law in this field as it expanded significantly the application of Art.8 ECHR.[67]

All that said, this ruling definitely laid the ground for a stricter scrutiny exercised by the Luxembourg Court particularly in cases in which digital rights are at stake. In this respect, despite the definite impact of the ECtHR, the Charter appears to be the true *game-changer*, a development also reaffirmed by another milestone data protection case, the *Facebook* case or the *Schrems* case,[68] delivered by the CJEU in 2015.

---

[64]Fabrini F., 'Human Rights in the digital age, The European Court of Justice ruling in the Data Retention Case and its lessons for Privacy and Surveillance in the U.S.', *Tilburg Law School Studies Research Paper Series No15/2014*,<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2482212>,accessed 14 October 2017 ,26.

[65]Peers S., 'The data retention judgment: The CJEU prohibits mass surveillance' (2014) *EU Law Analysis Blog*<http://eulawanalysis.blogspot.fr/2014/04/the-data-retention-judgment-cjeu.html>accessed 15 October 2017

[66]Supra note 57, *Digital Rights Ireland*,paras 35, 47, 54–55

[67]Petkova B., 'Towards an Internal Hierarch y of Values in the EU Legal Order, Balancing the Freedom of Speech and Data Privacy'[2016]23 *Maastricht Journal of European and Comparative Law* 3, 431.

[68] Case C-362/14,*Maximillian Schrems v Data Protection Commissioner,* 6 October 2015 ECLI:EU:C:2015:650 .

iii. *Schrems: paving the way for new data protection standards in the era of social networks*

In light of the Edward Snowden revelations and the heating discussion on mass surveillance conducted by US intelligence services, Maximillian Schrems, an Austrian national and a Facebook user, addressed a complaint to the Irish DPA arguing that his transferred personal data were subject to mass surveillance in the USA. The legal basis of such transfers of personal data was the EU/US 'Safe Harbour' agreement, reaching back in 2000. The said agreement was built upon a Commission decision adopted under the *Data Protection Directive* which declared the United States as an *adequate* destination for personal data.

The Irish data protection authority refused to pronounce on the applicant's complaint, so he challenged subsequently the DPA's decision before the Irish High Court, which clearly expressed doubt that the "Safe Harbour" legal framework was compatible with EU law. It addressed, thus, a preliminary question to the CJEU asking whether the DPAs of Member States should have the power to oppose data transfers to the US in similar cases.

The CJEU dealt first with the conditions under which a country is declared adequate for data transfers and, then, in case of declared adequacy as in the case under discussion, upon the competence of the national authorities to control these transfers.[69]

Addressing the first issue, in line with the Opinion of the AG,[70] the Court ruled that the term *adequate level of protection* of the Data Protection Directive should be interpreted as "requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the EU."[71]Additionally, the CJEU relied on the independent character of the DPAs in order to reaffirm the ongoing obligation of the European Commission or competent DPA to review any adequacy decision in light of any changes in circumstances having arisen in the aftermath of the decision's adoption. The challenged decision failed to guarantee a

[69] For an analysis of the background of the case see Cohen N., 'The privacy follies : a look back at the CJEU's invalidation of the EU/US Safe Harbor Framework' [2015] 1 *Eur. Data Prot. L. Rev.* 240.
[70] Opinion of Advocate General Bot delivered on 23 September 2015.
[71] Supra note 68, *Schrems* case, para 73.

FECHA DE ENVÍO DE ORIGINAL: 15.11.2017 FECHA DE ACEPTACIÓN: 12.12.2017
DOI: http://dx.doi.org/10.12795/IETSCIENTIA.2017.i02.04

sufficient level of data protection in the US equivalent to the one designated by the EU data protection law requirements.

Therefore, the CJEU underlined that provisions of the Data Protection Directive must be applied in conformity with the fundamental human rights as ensured by the EU Charter and, most importantly, with the rights to a private and family life, the protection of personal data, the right to an effective remedy and to a fair trial. In this regard, despite the fact that the Commission's decisions "are in principle presumed to be lawful and accordingly produce legal effects until such time as they are withdrawn, annulled in an action for annulment or declared invalid following a reference for a preliminary ruling or a plea of illegality(...) a Commission decisionadopted pursuant to Article 25(6) of Directive 95/46, such as Decision 2000/520, cannot prevent persons whose personal data has been or could be transferred to a third country from lodging with the national supervisory authorities a claim" and hence, "a decision of that nature cannot eliminate or reduce the powers expressly accorded to the national supervisory authorities by Article 8(3) of the Charter and Article 28 of the directive."[72]In the context of the limits of mass surveillance declared in its prior *Digital Rights* judgment, the additional element of the absence of effective judicial redress was not compatible with the EU Charter either.

Thus, according to the Court's reasoning, the restriction of the DPAs competence when reviewing data transfers in order to determine whether the level of data protection in the USA within the context of the *Safe Harbour* Agreement is adequate or not, was also considered as another legal flaw of the EU Commission's Decision. All that said, the Court of Justice invalidated in its entirety the contested decision.

When shedding light to the basic aspects of the case, it is more than evident that, following the Court's findings in *Google Spain* and *Digital Rights Ireland,* the Court now declares that even when a separate regime regulating external transfers is under scrutiny, an almost identical level of protection is required so as to guarantee compatibility with the EU Charter's provision related to data protection. However, as Steve Peers correctly observed, "with respect, the Court's interpretation is not convincing, since the word 'adequate' suggests something less than 'essentially

[72] Ibid.,paras 52,53

FECHA DE ENVÍO DE ORIGINAL: 15.11.2017 FECHA DE ACEPTACIÓN: 12.12.2017
DOI: http://dx.doi.org/10.12795/IETSCIENTIA.2017.i02.04

equivalent', and the EU Charter does not bind third States. But having said that, the American rules on mass surveillance would violate even a far more generous interpretation of the meaning of the word 'adequate'."[73]

The CJEU's standing not only reveals its belief that, in the post-Lisbon era, an even higher level of data protection is required under the Charter, but reflects its position in favour of an extended protection regarding data transfers to third countries, introducing, thus, an extraterritorial effect of the Charter's provisions in relation to digital rights.

The Court takes the right to privacy so seriously that reaches the conclusion that extended access to personal data by public authorities and law enforcement authorities, even in the name of national security, affects the "essence" of the right to private life under Art. 7 EU Charter. In this respect, no proportionality test or balancing exercise involving other rights and freedoms is required as far as the core of this right is breached.[74]

In conclusion, despite the criticism initially raised against the Court of Justice for not taking fundamental rights seriously enough and its reluctance in producing bold judgments in this field, post Lisbon, its case law on the Articles 7 and 8 of the Charter reveals its tendency to be a frontrunner in data protection law, particularly in "the digital age". However, this task is certainly not a walk in the park. In fact, the CJEU's position on the matter needs to be further clarified, especially in view of the Court's active interaction with its Strasbourg peer in this field.

C. Willems case: a U-turn of the CJEU with regard to biometric data?

While the evolution of the CJEU jurisprudence on the matter was already accomplished and –for that reason- incorporated in the recently adopted new *EU General Data Protection Regulation*, applicable as of May 2018 and aiming to fully

[73] Peers S.,'The party's over: EU data protection law after the Schrems Safe Harbour judgment', *EU law analysis Blog* [2015]<http://eulawanalysis.blogspot.gr/2015/10/the-partys-over-eu-data-protection-law.html>accessed 14 October 2017.

[74]Nonetheless, it is striking how the Luxembourg Court concluded to a violation of the essence of right to private life under Art.7 EUCFR but not to a violation of the essence of the right to the protection of personal data as enshrined in Article 8.

harmonise the overlapping data protection rules within the EU, a recent judgment of the CJEU came to shake the waters in relation with the protection of the most sensitive type of data, namely the biometric data.

Hence, the *Willems* ruling of the Luxembourg Court[75]contributed an alarming approach with regard to biometric data used for issuing passports and identity cards in the EU, in clear contradiction with its prior expansive interpretation of the EU data protection soft law and of the relevant EU Charter provisions. This particular issue is mostly regulated by the Regulation No. 2252/2004 (hereinafter '*Passport Regulation*') [76], amended by Regulation No. 444/2009.[77] According to the latter, the collection, storage and processing of biometric data is targeted only in verifying the authenticity of the travel document or the identity of the holder of such document. The case at hand arose when the applicants, Dutch nationals, after filing their passport applications refused to provide the competent authorities with their fingerprints due to the fact that, under the Netherlands Passport law, the biometric data collected for that purpose are also transferred and stored in a decentralized database in order to be further used for national security or judicial purposes. As a result, Mr. Willems and others challenged the rejection of their applications before the Dutch Courts on fundamental rights grounds. Besides the practical implications that the lack of identity cards had in the daily routine of the applicants, the latter claimed *inter alia* that the retention and further use of their fingerprint data raised severe privacy concerns and violated their fundamental rights under Article 7 and 8 of the EU Charter. The national court referred two questions to the CJEU for preliminary ruling.

The said questions raised, firstly, the issue whether the Passport Regulation is applicable to certain types of identity cards regardless their period of validity. The latter plays a central role for the Dutch identity cards' consideration as travel documents according to the spirit of the aforesaid Regulation. Secondly, pursuant to the applicants' allegations, the CJEU was called to pronounce on whether the re-use for other purposes

[75] Joined Cases C-446/12 to C-449/12, *W.P. Willems v Burgemeester van Nuth and H.J. Kooistra v Burgemeester van Skarsterlân*, and *M. Roest V Burgemeester van Amsterdam*, and *L.J.A. van Luijk v Burgemeester van Den Haag,*[2015] ECLI:EU:C:2015:238.
[76]Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States [2004] OJ L 385/1.
[77]Regulation (EC) No 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States[2009] OJ L 142/1.

of biometric data originally collected for the issuance of passports is compatible with the EU data protection legislation and with Art.7 and 8 of the EU Charter.

At the outset, the Luxembourg Court focused persistently its reasoning on the wording of the Regulation which provides that provided that "identity cards issued to [Member States'] nationals or to temporary passports and travel documents having a validity of 12 months or less". The Court interpreted this particular provision as having no application on national identity cards and, thus, Dutch identity cards fall outside the scope of the Regulation, neglecting not only the fact that they also serve as travel documents within the EU, but also their period of validity which lasts for five years.

As for the second question, the Court concluded that it cannot rule on the further use of biometric data of passports since the latter fall outside the purposes of this Regulation and, therefore, subject to regulation by national law. For that reason, the Court shockingly came to the conclusion that since the potential re-use of such data by national authorities is not governed by the said Passport Regulation, the EU Charter is not applicable either, despite the fact that such a process might be in violation of the ECHR.

Finally, the Court refrained to pronounce on the compatibility of national law with Art.6 and 7 of the *Data Protection Directive*[78] on the grounds that only the correct interpretation of the Passport Regulation was at stake in the present case.

[78]Article 6 of the Data Protection Directive provides that: "1. Member States shall provide that personal data must be: (a) processed fairly and lawfully;(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.2. It shall be for the controller to ensure that paragraph 1 is complied with.Article 7 reads as follows : "Member States shall provide that personal data may be processed only if:(a) the data subject has unambiguously given his consent; or (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or (d) processing is necessary in order to protect the vital interests of the data subject; or(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or(f) processing is necessary 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 which require protection under Article 1 (1)".

FECHA DE ENVÍO DE ORIGINAL: 15.11.2017 FECHA DE ACEPTACIÓN: 12.12.2017
DOI: http://dx.doi.org/10.12795/IETSCIENTIA.2017.i02.04

Consequently, the *Willems* ruling constitutes a step back from the previously discussed jurisprudential progress in the field of data protection. Notably, the Court, in contradiction with its *modus operandi* in previous similar cases, insisted on the wording of the referred questions in order to restrict its own competence.[79] Looking at the previous CJEU's case law, the Court paradoxically misses the chance to elaborate on the intriguing questions of the national Court, particularly in the light of the Charter's standards. Besides its prior data protection case law, it's only in its *Schwarz* ruling in 2013[80] when the CJEU examined the storage of fingerprints under the Passport Regulation in the light of Art.7 and 8 of the Charter and concluded that such a use of biometric data does not constitute a disproportionate interference with the right to private life and the right to data protection respectively, as enshrined in the EU Charter. In any case, the mere fact that the applicants invoked the *Passport Regulation* brought the matter under the scope of EU law and, thereby, of the Charter since the use of biometric data in the new generation of passports relies on an EU obligation.[81]

In addition to this, the unwillingness of the Court to redraft the question on the compatibility with the Data Protection Directive in order to avoid addressing the issue already raised by the national Court "*simply departs from reality*".[82]

III. Conclusions

Under the pressure of proliferation of data mining techniques, developing increasingly intrusive implications in individuals' private life, the legal protection of personal data calls for a systematic and articulate legal regulation.

The concept of privacy as captured under Article 8 of the ECHR, in correlation with the right to data protection as enshrined in the EU Charter (Article 8), point towards an enhanced protection, that could equip the EU Courts with valuable tools in order to review more effectively EU data protection legislation.

[79] Wisman T., 'Willems: Giving Member States the Prints and Data Protection the Finger', 1 *Eur. Data Prot. L. Rev.* 245,2015.
[80] Case C-291/12, *Michael Schwarz v Stadt Bochum*[2013] ECLI:EU:C:2013:670.
[81] Supra note 6,Hornung.
[82] Peers S., 'Biometric data and data protection law: the CJEU loses the plot', *EU Law Analysis blog* [2015]<http://eulawanalysis.blogspot.gr/2015/04/biometric-data-and-data-protection-law.html>, accessed 14 October 2017.

Notwithstanding the strict scrutiny with regard to the use of personal data exercised by the Luxembourg Court and its effort to walk *hand-in-hand* with its Strasbourg counterpart on the matter, the Court seemed in *Willems* case to consider the fate of biometric data collected as completely irrelevant to the EU legal framework.

Regardless of what the impact of this judgment might be in the foreseeable future, it raises great concerns pertaining to the actual enjoyment of the right to private life or the protection of the most sensitive personal data, namely the biometric ones. Most importantly, in the era of mass surveillance and "big data", both the European judicial mechanisms are now engaged in building a more solid legal shelter for the collection, storage and processing of such data.[83] Hence, leaving the further use of biometric data of EU citizens unattended might open progressively the *Pandora's box* for uncontrolled misuse or abuse of data containing biological information of individuals. The new General Data Protection Regulation does not seem to respond sufficiently to this ever-growing anxiety and in this respect, it is largely criticized by numerous scholars even before its entry into force.[84]

Thus, automated profiling or data mining practices, which when intensively applied, might offer a great deal of benefits in the field of scientific research, might also constitute a threat to private life if the EU or international institutions continue to avoid verging into this whole new territory. The viability and efficiency, therefore, of a comprehensive regulatory regime addressing these newly emerging challenges will largely depend on its appraisal by involved legislative and judicial bodies.

BIBLIOGRAPHY

ARTICLES/BOOKS

-Anil J., Hong L., Pankanti S., 'Biometric identification' [2000] 43 Communications of the ACM 2.

[83] See *inter alia* Gutwirth S., Leenes R., De Hert P., Poullet Y. (eds.), *European Data Protection: Coming of Age (*Springer 2013).

[84] See for a critical analysis of the General Data Protection Regulation Goncalves M-E., 'The EU data protection reform and the challenges of big data: remaining uncertainties and ways forward'[2017] 26 *Information & Communications Technology Law* 2; De Hert P., PapakonstantinouV., 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?'[2016]32 *Computer Law & Security Review: The International Journal of Technology Law and Practice* 2.

FECHA DE ENVÍO DE ORIGINAL: 15.11.2017 FECHA DE ACEPTACIÓN: 12.12.2017
DOI: http://dx.doi.org/10.12795/IETSCIENTIA.2017.i02.04

-Baldaccini A., 'Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases'[2008] 10 European Journal of Migration and Law 31.

-Birnhack M., 'The EU Data Protection Directive: An Engine of a Global Regime'[2008] 24 Computer Law & Security Report 6.

-De Hert P.,Gurtwirth S., 'Data protection in the case law of Strasbourg and Luxemburg : constitutionalisation in action' in Gurtwirth S., Poullet Y., De Hert P., Nouwt J. & De Terwangne C.(eds), Reinventing Data Protection? (Springer 2009).

-De Hert P., Papakonstantinou V., 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?'[2016] 32 Computer Law & Security Review: The International Journal of Technology Law and Practice 2.

- Esfandiari N., Reza Babavalian M., Eftekhari Moghadam A.-M. &Kashani Tabar V., 'Knowledge discovery in medicine: Current issue and future trend' [2014], 41 Expert Systems with Applications 4434.

-Fabrini F., 'Human Rights in the digital age, The European Court of Justice ruling in the Data Retention Case and its lessons for Privacy and Surveillance in the U.S.', Tilburg Law School Studies Research Paper Series No15/2014.

-Fontanelli F., The European Union's Charter of Fundamental Rights two years later [2011] 3 Perspectives on Federalism 3.

-Goncalves M-E., 'The EU data protection reform and the challenges of big data: remaining uncertainties and ways forward'[2017] 26 Information & Communications Technology Law 2.

-Gutwirth S., Leenes R., De Hert P., Poullet Y. (eds.), European Data Protection: Coming of Age (Springer 2013).

-Hernández-Aguilar J.A., Zavala C., Díaz O., Burlak G., Ochoa A. and César Ponce J., 'Biometric Data Mining Applied to On-line Recognition Systems' in Midori A (ed), Biometrics - Unique and Diverse Applications in Nature, Science, and Technology(In tech 2011).

-Hornung G., 'The European Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards' [2007] 4 SCRIPT ED 246.

-Iglesakis I., "The Right To Be Forgotten in the Google Spain Case (case C-131/12): A Clear Victory for Data Protection or an Obstacle for the Internet?" [2014] accessed 12 November 2017.

-Kaplan B., 'How Should Health Data Be Used? Privacy, Secondary Use, and Big Data Sales' [2016] 25 Cambridge Quarterly of Healthcare Ethics 312.

FECHA DE ENVÍO DE ORIGINAL: 15.11.2017 FECHA DE ACEPTACIÓN: 12.12.2017
DOI: http://dx.doi.org/10.12795/IETSCIENTIA.2017.i02.04

-Kulk S. and Zuiderveen Borgesius F., 'Google Spain v. González: Did the Court Forget about Freedom of Expression?',[2014] 5 European Journal of Risk Regulation 3.

-Kuner C., 'The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines', [2015] LSE Law, Society and Economy Working Papers 3/2015 accessed 15 November 2017.

-Lynksey O., 'The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland, Joined Cases C-293 & 594/12, Digital Rights Ireland Ltd and Seitlinger and others, Judgment of the Court of Justice (Grand Chamber) of 8 April 2014,nyr.'[2014] 51Common Market Law Review 6.

-Mittelstadt B.D., Allo P., Taddeo M., Wachter S. and Floridi L., 'The ethics of algorithms: Mapping the debate' [2016], Big Data & Society 1, , accessed 13 November 2017.

-Peers S.,'The data retention judgment: The CJEU prohibits mass surveillance' (2014) EU Law Analysis Blog [2014] accessed 15 October 2017.

-Peers S., 'The party's over: EU data protection law after the Schrems Safe Harbour judgment', EU Law Analysis Blog [2015] accessed 14 October 2017.

-Peers S., 'Biometric data and data protection law: the CJEU loses the plot' (2015) EU Law Analysis blog [2015] , accessed 14 October 2017.

-Petkova B., 'Towards an Internal Hierarchy of Values in the EU Legal Order, Balancing the Freedom of Speech and Data Privacy' [2016] 23 Maastricht Journal of European and Comparative Law 3.

-Rajaretnam T., 'Data Mining and Data Matching: Regulatory and Ethical Considerations Relating to Privacy and Confidentiality in Medical Data' [2014] 9 J. Int't Com. L. & Tech. 294, 300.

-Sheeba R. and Subha M, 'Data Mining Applications in Biometrics : Multimodel Scheme with Facial and Iris Recognition Based on Gabor Filter' [2013], 2 IJERT V 12.

-Thearling K, 'Information about analytics and data science / An Introduction to Data Mining' [2012] < http://www.thearling.com/text/dmwhite/dmwhite.html > accessed 13 November 2017.

-Wisman T., 'Willems: Giving Member States the Prints and Data Protection the Finger' [2015] 1 Eur. Data Prot. L. Rev. 245.

-Zarsky T., 'The trouble with algorithmic decisions an analytic road map to examine efficiency and fairness in automated and opaque decision making' [2016] 41 Science, Technology & Human Values 1,121

FECHA DE ENVÍO DE ORIGINAL: 15.11.2017 FECHA DE ACEPTACIÓN: 12.12.2017
DOI: http://dx.doi.org/10.12795/IETSCIENTIA.2017.i02.04

-Zhang Y., 'TIETS34 Seminar: Data Mining on Biometric identification, Computer Science', School of Information Sciences, University of Tampere, Finland.

TABLE OF CASES

EUROPEAN COURT OF HUMAN RIGHTS

- Klass and Others v. Germany, Application no. 5029/71, 6 September 1978.

-Malone v. the United Kingdom, Application no. 8691/79, 2 August 1984.

-Leander v. Sweden, Application no. 9248/81, 23 March 1987.

-Rotaru v. Romania [GC], Application no. 28341/95, 4 May 2000.

-Peck v. the United Kingdom, Application no. 44647/98, 28 January 2003.

COURT OF JUSTICE OF EUROPEAN UNION

-Case C-291/12, Michael Schwarz v Stadt Bochum [2013] ECLI:EU:C:2013:670.

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

-Joined cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [2014] ECLI:EU:C:2014:238.

-Case C-362/14, Maximillian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650.

-Joined Cases C-446/12 to C-449/12, W.P. Willems v Burgemeester van Nuth and H.J. Kooistra v Burgemeester van Skarsterlân, and M. Roest V Burgemeester van Amsterdam, and L.J.A. van Luijk v Burgemeester van Den Haag,[2015] ECLI:EU:C:2015:238.