ISSN 2704-8012

European Journal of Privacy Law & Technologies

Special issue (2020)

G. Giappichelli Editore

European Journal of Privacy Law & Technologies

Directed by Lucilla Gatt

Special issue (2020)

Edited by Massimo Foglia

G. Giappichelli Editore

European Journal of Privacy Law & Technologies
On line journal
Italian R.O.C. n. 25223

G. GIAPPICHELLI EDITORE - TORINO
VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it

The Journal is one of the results of the European project TAtoDPR (Training Activities to Implement the Data Protection Reform) that has received funding from the European Union's within the REC (Rights, Equality and Citizenship) Programme, under Grant Agreement No. 769191.

Published Online by G. Giappichelli in September 2020
www.ejplt.tatodpr.eu

European Journal of Privacy Law and Technologies

Prof. Manuel Pereiro Càrceles – University of Valencia
Prof. Sara Lorenzo Cabrera – Universidad de La Laguna
Ph.D. Avv. Alessandra Sardu – Università Suor Orsola Benincasa di Napoli
Ph.D. Avv. Anita Mollo – Università Suor Orsola Benincasa di Napoli
Ph.D (c) Avv. Valeria Manzo – Università degli Studi della Campania Luigi Vanvitelli
Ph.D (c) Avv. Livia Aulino – Università Suor Orsola Benincasa di Napoli
Ph.D (c) Emiliano Troisi – Università Suor Orsola Benincasa di Napoli
Ph.D (c) Noel Armas Castilla - Universidad de Sevilla
Ph.D. Sara Saleri – Re:Lab
Ph.D. (c) Hans Steege – Gottfried Wilhelm Leibniz Universität Hannover
Avv. Delia Boscia – Ordine Avvocati Napoli
Avv. Flora Nurcato – Università Suor Orsola Benincasa di Napoli
Avv. Lucio San Marco – Giappichelli Editor
Dr. Simona Latte – Università Suor Orsola Benincasa di Napoli

SUMMARY

page

PREFACE

The contradictions of the privacy law

The volume is a special issue of the European Journal of Privacy Law & Technologies (EJPLT) and constitutes an ambitious collection of the proceedings of the international conference on data protection organised by Professor Massimo Foglia at the University of Bergamo (Italy), at the end of 2019.

The conference was characterized by significant talks on the evolution of the data protection law in Europe after the entering in force of Reg. (EU) 2016/679 (well known as GDPR). The collection of papers of renowned professors, researchers and lawyers with a solid experience on data protection issues, coming from the different European Member States, has been made by Prof. Foglia, who brilliantly put together the works, systematically organising them: from general principles to liability rules, through some practical applications of data protection law (e.g.: minors, consumers, health, public and private institutions).

The collection of the contributions finds its natural place as a special volume of EJPLT which, indeed, is a European Law Scientific Journal, specifically focused on privacy, with particular regard to the ever-important relationship between, law and innovation, humanities and technologies.

In this light, the special volume of the EJPLT is dedicated to the private enforcement of general data protection regulation, underlining the chances as well as the new challenges arising from this reform of data protection law.

The GDPR represents the European Union's attempt to acquire leadership in the privacy field and present itself as a safe place for the circulation of personal data both offline and online (given the absence of the so-called e-privacy Regulation). The GDPR is the origin of the concept of the natural person as *vulnerable* subject [1] regardless of disability, age and other but in himself/herself as sub-

[1] G Malgieri and J Niklas, 'Vulnerable Data Subjects' (Forthcoming 2020) Special Issue on Data Protection and Research, Computer Law and Security Review, 1 ff.. Available at SSRN: https://ssrn.com/abstract=3569808: Abstract '[…]*the starting point for this reflection is wide-ranging development, deployment and use of data-driven technologies that may pose substantial risks to human rights, the rule of law and social justice. Application of such technologies area*

ject interested in the processing of personal data most of all when he/she acts in a digital environment.

However, a careful reading of the regulatory text highlights the double soul of European legislation. In many cases it allows exceptions to the mandatory consent to data processing and, in particular, allows the voluntary transfer of data in exchange for services (almost always provided in a digital environment), making personal data an asset object to exchange even under certain (mainly formal) conditions.

In other words, the GDPR is long and complex and presents numerous antinomies and logical contradictions which, considering also the detailed national regulations, are translated into interpretative issues such as to make its practical application very difficult and diverging not only from one State to another State in the EU but also, within same State, between public and private entities, between natural and legal persons, public administrations and businesses etc.

Think, for example, of the difficulty of taking a clear position on the position (internal or external) of the DPO with respect to the data controller. The relationship between the national Data Protection Authorities (DPAs) and the two European bodies (the European Data Protection Supervisors (EDPS) and the European Data Protection Board (EDPB)) is equally critical. The latter appear overlying and not very dialoguing with the former. At the end, the level of disciplinary uniformity achieved is not high, considering also the breakthrough occurred with *Brexit* of the United Kingdom.

Precisely for these reasons, the volume opens with the uniform interpretation of GDPR concepts as a new challenge for European and national courts in the field of data protection. Contemporary, in the volume are analysed the major international implications of the GDPR both in the private international law and in the administrative international law.

Moving on to the application of the GDPR to some specific areas, reference was made in the first place to minors, and their data protection, with particular regard to the analysis of the effectiveness of consent to the processing of personal data as a regulatory tool to protect the best interest of the child. As a matter of fact, consent is one of the leading lawful bases of data processing, but this regulatory tool often does not guarantee an effective protection of data subjects,

---

can significantly contribute to systematically disadvantage marginalised communities, exploit people in particularly sensitive life situations and lead to discrimination. Considering those problems, we recognise the special role of personal data protection and call for its vulnerability-aware interpretation. However, to better delineate and contextualise the general understanding of human vulnerability we first review the theories of vulnerability and the use of the concept in international human rights law and European law'.

who are often unaware of multiple aspects of the processing of his or her personal data. This happens especially when the data subjects are the weak subjects in a contractual relationship, such as consumers, and it is necessary to avoid unlawful processing of their data, including the commercial use of personal data without that data subject's aware consent.

Secondly, the impact of the new regulation on data protection in the healthcare sector was taken into consideration, comparing different national legal systems of the European Union. In particular, the issues of patient rights understood as data subjects were studied in depth, including them in the wider context of the dignity of the natural person. In addition, the responsibilities and tasks of the healthcare organisations were observed, as well as the conduct of medical research in compliance with GDPR.

Finally, the study of data protection in institutions and bodies was extremely important. More in detail, were specifically investigated the main actions undertaken in order to ensure compliance with the GDPR and some differences regarding the application of this EU legal framework in comparison with private entities and public authorities of the EU Member States.

Moving on to the *ex post* protection, provided for in articles 82 and following of the GDPR, it was deemed necessary to deepen the liability for unlawful processing of personal data by investigating the subjective and objective requirements of this liability (in particular the fault).

This analysis is particularly important because it highlights the ambiguity of the formulation of the rules of the Data Protection Regulation on this topic and, above all, opens the reflection on possible scenarios in which it will be possible to exclude the liability of the data controller or other subjects involved in the processing of personal data in the absence of a lawful basis, simply by introducing a contractual clause with which the interested party consciously consents to the exemption from any liability that could be charged to the subjects mentioned above.

From the perspective of compensation for damages, moreover, it has been verified whether the compensation of non-material damage can be an effective means to ensure legal protection also in the field of data protection.

In conclusion, the horizon of the editor and all the authors of the volume is wide, but the studies are exposed in a precise and coherent way, establishing themselves on a solid basis of scientific depth and mastery of data protection matter. The issue is addressed from the point of view of new technologies because they have completely changed the world we were used to living in, involving many benefits but also numerous risks, first of all in the field of data protection.

The volume represents a valid scientific contribution on the private enforcement of the GDPR that of course should be read by scholars and legal practitioners who deal with data protection issues in the 21st century.

Naples, 18th June 2020

Lucilla Gatt
Full Professor of Civil Law, New Technologies Law and Family Law
Università degli Studi Suor Orsola Benincasa di Napoli
Editor in Chief of EJPLT

UNIFORM INTERPRETATION OF GENERAL DATA PROTECTION REGULATION CONCEPTS AS A NEW CHALLENGE FOR CJEU

Agnieszka Guzewicz, University of Wrocław

Abstract:

The aim of this paper is to provide the key elements of autonomous interpretation of the Court of Justice of the European Union in the field of data protection and to present selected autonomous concepts resulting from the case-law.

Keywords: data protection, personal data, uniform interpretation, autonomous concepts, case-law

1. Introduction

This paper is based on the speech that took place at the University of Bergamo on October 3rd, 2019 during the international conference „Private Enforcement of General Data Protection Regulation. New Chances, New Challenges". Some thoughts presented at the said event are expressed in this paper. First, the phenomenon of autonomous interpretation will be presented. Then, the methods of autonomous interpretation will be discussed in the context of GDPR. Finally, selected autonomous concepts in the field of data protection will be provided. The paper is focused on EU perspective.

2. The phenomenon of autonomous interpretation

As a starting point, the very phenomenon of autonomous interpretation used

by the Court of Justice of the European Union in Luxembourg should be analysed. This particular method of interpretation serves to unify the understanding and application of EU law. For some legal scholars, as well as for practitioners, autonomous interpretation is perceived as the best (and even the only) tool to strengthen the European integration; for others, on the contrary, it does not constitute an effective measure.

The Court's autonomy should not be identified with a creation of new methods (directives) of interpretation. Autonomous interpretation is based on the classical methods known to international law and the laws of the Member States, such as: linguistic interpretation, systematic interpretation, teleological interpretation (purposeful arguments). The specificity of autonomous interpretation of the Court of Justice lies in reducing the importance of linguistic interpretation and attaching greater importance to systematic and teleological interpretation. Moreover, in the interpretation of EU law, comparative analysis and *travaux préparatoires* play an important role (it is particularly noticeable in the opinions of the Advocates General).

Autonomous interpretation is linked with autonomous concepts that should be perceived as "interpretative tools". The autonomous character of the term may be identified with the supranational meaning and with its independence from the interpretation used (accepted) in national legal orders [1]. In other words, the meaning assigned to a given concept in national legal order may be completely different from the uniform EU interpretation [2].

As it was expressed and then developed in the case-law of the Court of Justice:

'Terms used in Community law must be uniformly interpreted and implemented throughout the Community, except when an express or implied reference is made to national law' [3].

'[...] according to settled case-law, the need for a uniform application of European Union law and the principle of equality require that the terms of a pro-

---

[1] See, e.g., G. BENACCHIO, *Diritto privato della Comunità Europea. Fonti, modelli, regole* (Milano 2008), 2nd ed., 49-51; J. ENGBERG, *Autonomous EU Concepts: Fact or Fiction?*, S. ŠARČEVIĆ (eds.), *Language and culture in EU law: Multidisciplinary Perspectives* (Farnham 2015), 170-171. The analysis of private law concepts in the context of EU primary law was conducted in: H.W. MICKLITZ-C. SIEBURGH (eds.), *Primary EU law and private law concepts* (Cambridge 2017).

[2] See A. GUZEWICZ, *Autonomous concepts of commercial law*, B. HEIDERHOFF-I. QUEIROLO (eds.), *European and international cross-border private and economic relationships and individual rights,* A. M. BENEDETTI - I. QUEIROLO (eds.), *Scritti di diritto privato europeo e internazionale* (Roma 2016) 8, 141-147.

[3] Case C-49/71, Hagen OGH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel, ECJ, 1.2.1972, 6.

vision of European Union law which makes no express reference to the law of the Member States for the purpose of determining its meaning and scope must normally be given an independent and uniform interpretation throughout the European Union'[4].

It can therefore be stated that the uniform EU interpretation is restricted by a reference to national law. If EU provision does not refer to national law (what should be understood as an exception), the autonomous interpretation will apply (as a general rule). The interpretation of the Court of Justice is autonomous in nature, which means that the interpretation process cannot be neutral[5]. The Court of Justice applies the autonomous interpretation of EU provisions (in which case the uniform interpretation is concerned) or leaves the process of interpretation to the Member States (in this case a national interpretation is concerned).

When interpreting the EU provisions, the Court uses a new method called 'hybridization'. It involves the use of a broad spectrum of legal instruments, coming from both private and public law. The mix of substantive and procedural elements may also be noticed in the case-law. All these measures are aimed at supporting the functioning of the internal market.

The purpose of the uniform interpretation is to ensure the effectiveness of EU law. The interpretation adopted by the Court of Justice is consistent with the axiology of EU law or, in other words, the "spirit of the Treaty".

3. GDPR and the methods of autonomous interpretation

General Data Protection Regulation (hereinafter as: "GDPR"[6]) is the new EU legal act in the field of data protection. It repealed the Directive 95/46/EC[7]. The

[4] Case C-510/10, DR and TV2 Danmark A/S v NCB – Nordisk Copyright Bureau, ECJ, 26.4.2012, 244, point 33; See also: Case C-327/82, Ekro BV Vee- en Vleeshandel v Produktschap voor Vee en Vlees, ECJ, 18.1.1984, 11, point 11; Case C-287/98, Grand Duchy of Luxemburg v Berthe Linster, Aloyse Linster and Yvonne Linster, ECJ, 19.9.2000, 468, point 43; Case C-5/08, Infopaq International A/S v Danske Dagblades Forening, ECJ, 16.7.2009, 465, point 27; Case C-245/00, Stichting ter Exploitatie van Naburige Rechten (SENA) v Nederlandse Omroep Stichting (NOS), ECJ, 6.2.2003, 68, point 23; Case C-306/05, Sociedad General de Autores y Editores de España (SGAE) v Rafael Hoteles SA, ECJ, 7.12.2006, 764, point 31.

[5] See, M. AUDIT, *L'interprétation autonome du droit international privé communautaire* (2004) *Journal du Droit International*, 798; L. CHARBONNEAU, *Notions autonomes et intégration européenne* (2013) 1 *Cahiers de Droit Européen*, 53.

[6] Regulation (EU) 2016/679 of the European Parliament and of 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 L 119, 4.5.2016, 1-88.

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on

uniform interpretation of GDPR provisions constitutes a new challenge for the Court of Justice. The arguments presented below are grounded on the analysis of the case-law of the Court of Justice based on the GDPR and the Directive 95/46/EC.

As it was highlighted above, the methods (directives) of autonomous interpretation are known to international law and the laws of the Member States but the hierarchy of importance is different.

When taking into consideration the general model, the Court of Justice begins the process of interpretation of EU provision with a linguistic interpretation, *id est* the analysis of the wording of the provision (so called literal meaning) [8]. It can be perceived in the judgments based on the Directive 95/46/EC that the Court of Justice examines whole sentences or single terms.

The specificity of EU autonomous legal order is that determining the wording of a provision, as a result of the application of the linguistic interpretation directives, usually does not end the interpretation process. The multilingual nature of EU law and the autonomy of its concepts are the reasons for the insufficiency of this interpretative directive.

After achieving the result of linguistic interpretation, the Court of Justice will turn to the systematic and teleological interpretation.

The basis for the existence of systematic interpretation rules is the assumption that the set of norms in a given legal system is coherent, ordered and has a specific hierarchy. Consequently, a legal provision cannot be analysed in isolation from the legal system in which it operates and, moreover, its place in a given legal act should not be seen as accidental.

The Court of Justice analyses provisions in the field of data protection in their context, taking into consideration their 'place' in the GDPR or Directive 95/46/EC.

Per exemplum, in the case C-345/17 (Buivids) [9] the Court of Justice, analysing the provisions of the Directive 95/46/EC, stated:

(...) according to settled case-law of the Court, the provisions of a directive must be interpreted in the light of the aims pursued by the directive and the system which it establishes [10].

Further arguments of this paper focus on the teleological approach, *id est* searching for the spirit of the provisions. The teleological interpretation pro-

---

the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, 31–50 (hereinafter as: 'Directive 95/46/EC').

[8] See also, A. BREDIMAS, *Methods of Interpretation and Community Law (European Studies in Law)* (Amsterdam 1978), 35.

[9] Case C-345/17, Proceedings brought by Sergejs Buivids, ECJ, 14.2.2019, 122.

[10] *Ibidem* point 49; See also: Case C-73/07, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy, ECJ, 16.12.2008, 727, point 51; Case C-265/07, Caffaro Srl v Azienda Unità Sanitaria Locale RM/C, ECJ, 11.09.2008, 496, point 14.

vides such an interpretation of a legal provision that guarantees its effectiveness (*effet utile*) [11]. Finding the sense (purpose) of EU provision is an inspiration and a main task of the Court of Justice in the interpretation of EU law. The spirit of the Treaty permeates the case-law and should be combined with the axiological foundations of EU law.

Considering the purpose of EU legal acts and the teleological interpretation of the Court of Justice, the crucial role of the preambles should be underlined.

According to the first recital in the preamble to GDPR "the protection of natural persons in relation to the processing of personal data is a fundamental right". Therefore the first recital refers to the Charter of Fundamental Rights of the European Union [12] and to the Treaty on the Functioning of the European Union [13]. The protection of personal data constitutes a fundamental right, however it is not an absolute right.

The second recital of GDPR concerns the processing of personal data, which should be carried out respecting fundamental rights and freedoms [14]. As it was expressed in the fourth recital "the processing of personal data should be designed to serve mankind". The limits, such as the principle of proportionality and the respect for other fundamental rights, should be underlined. Among the fundamental rights, it is worth emphasizing here the respect for private and family life.

New developments (especially technological) and the phenomenon of globalisation require more coherent EU framework for data protection. The increase in cross-border flows of personal data has brought new challenges. These factors are related to the proper functioning of the internal market.

It should also be mentioned that the comparative analysis and legislative history are not forgotten in the process of interpretation of data protection provisions [15].

In the context outlined above, the role of the Court of Justice in interpreting uniformly GDPR concepts cannot be underestimated.

---

[11] See, G. ITZCOVICH, *The Interpretation of Community Law by the European Court of Justice* (2009) 10 (5) *German Law Journal*, 555.

[12] See Article 8 (1) of the Charter of Fundamental Rights of the European Union, OJ C 303, 14.12.2017 (hereinafter as: 'the EU Charter').

[13] See Article 16 (1) of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012 (hereinafter as: 'TFEU').

[14] The purpose of the Directive 95/46/EC was to harmonise the provisions (rules) concerning the protection of personal data and to ensure the free flow between Member States.

[15] In regard to the Court's reference to legislative history of the Directive 95/46/EC, see Case C-345/17 (fn 9) point 52.

4. Selected autonomous concepts in the field of data protection

It will be outlined in this part of the paper how the Court of Justice interprets some basic concepts in the field of data protection, such as 'personal data', 'processing of personal data', 'controller' and 'journalistic purposes' ('journalistic activites'). The aim of this section is to present certain formulas from the case-law of the Court of Justice confirming the autonomous nature of these concepts (not their analysis).

It must be born in mind that in each case the Court of Justice takes a decision in the specific factual circumstances, especially in the preliminary ruling procedure. In this context, some limitations to the interpretation may be involved.

The concepts of 'personal data' and 'processing of personal data' ('processing') will be analysed together. Their definitions are contained, respectively, in the Article 2 of the Directive 95/46/EC and in the Article 4 of the GDPR. The Court of Justice developed these concepts in the case-law. Their interpretation, so far, is based mainly on the provisions of the Directive 95/46/EC.

Per exemplum, in its judgments the Court of Justice argued that an image of a person recorded by a camera '*inasmuch as it makes it possible to identify the person concerned*' [16] or a tax data [17] constitute 'personal data'. The linguistic and purposeful arguments were used.

Referring to the professional activity, the Court stated that '*the fact that information is provided as part of a professional activity does not mean that it cannot be characterised as 'personal data*' [18]'.

For the 'processing of personal data', it is apparent from the Court's case-law that:

'a video recording of persons which is stored on a continuous recording device – the hard disk drive of that system – constitutes (...) the automatic processing of personal data' [19].

'the operation of loading personal data onto an internet page must be regarded as constituting such processing' [20].

---

[16] Case C-345/17 (fn 9) point 31.

[17] Case C-496/17, Deutsche Post AG v Hauptzollamt Köln, ECJ, 16.1.2019, 26; point 55; Case C-73/16, Peter Puškár v Finančné riaditeľstvo Slovenskej republiky and Kriminálny úrad finančnej správy, ECJ, 27.9.2017, 725, point 41; Case C-201/14, Smaranda Bara and Others v Casa Naţională de Asigurări de Sănătate and Others, ECJ, 1.10.2015, 638, point 29.

[18] Case C-345/17 (fn 9) point 46.

[19] Case C-345/17 (fn 9) point 37.

[20] *Ibidem*; Case C-101/01, Criminal proceedings against Bodil Lindqvist, ECJ, 6.11.2003, 596, point 25.

The decisions are taken in individual situations, but the Court's statements can be repeated in subsequent judgments.

With regard to the case C-345/17 (Buivids), the Court of Justice also interpreted the notion of 'journalistic purposes' ('journalistic activities') provided for in the Article 9 of the Directive 95/46/EC. Referring to its previous judgment, the Court held that the concepts related to freedom of expression must be interpreted broadly [21]. Afterwards, following the previous case-law, the Court recalled the autonomous definition of the 'journalistic activities', that is to say: '*those which have as their purpose the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them'* [22]. Finally, the concept 'solely for journalistic purposes' was analysed. The Court's considerations are based on the provisions of the EU Charter which is particularly important. The Court faced a dilemma on how to reconcile two fundamental rights, *id est* the right to privacy and the right to freedom of expression. It stated that the exemptions and derogations provided for in the Article 9 of the Directive 95/46/EC must be applied „*only where they are necessary*" [23]. The significance of the jurisprudence of the European Court of Human Rights was also highlighted.

In the case C-40/17 (Fashion ID) the concept of 'controller' was interpreted [24]. In the process of interpretation the Court reminded the definition contained in the Article 2 (d) of the Directive 95/46/EC (literal meaning). Then the Court focused on the objective of that provision which manifests in '*effective and complete protection of data subjects*' [25]. Furthermore it emphasized the broad definition of the concept of „controller" as it was interpreted in its previ-

---

[21] Case C-345/17 (fn 9) point 51.

[22] Case C-345/17 (fn 9) point 53; Case C-73/07 (fn 10) point 61. In the legal doctrine, see: K. WOLLTER, *Data Protection and "journalistic activities" – ECJ rules on exceptions to the Data Protection Directive* (2009) 2 *Bulletin of international legal developments*, 13-15; W. HINS, *Case C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy, Judgment of the Court of Justice (Grand Chamber) of 16 December 2008* (2010) 47 (1) *Common Market Law Review*, 215-233.

[23] Case C-345/17 (fn 9) point 63; Case C-73/07 (fn 10) point 55.

[24] Case C-40/17, Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV, ECJ, 29.7.2019, 629. In the legal doctrine see: F. MATTATIA, *Données personnelles: la reponsabilité d'un utilisateur des services proposés par Facebook* (2019) 40 *La Semaine Juridique – édition generale*, 1730-1735.

[25] Case C-40/17 (fn 24) point 66; Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, ECJ, 5.6.2018, 388, point 28; Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, ECJ, 13.5.2014, 317, point 34.

ous case-law [26]. Purposeful arguments were particularly important in the final Court's interpretation.

5. Conclusion

It can be concluded that the process of GDPR interpretation, which is in the initial stage at this point, will certainly evolve. The interpretative guidelines for the Court of Justice may be provided from its previous judgments based on the Directive 95/46/EC. The following years will show to what extent the Court of Justice will refer to the interpretation of the concepts contained in the Directive 95/46/EC. The perspective of „new" or rather „old-new" concepts in the area of data protection remains an open question.

In instances, where the ensuring of a high level of protection of the fundamental rights and freedoms of individuals is at stake, it seems that the CJEU will adopt a broad interpretation of the concepts.

Undoubtedly, all the factors mentioned in this paper can affect the application of law in national legal orders. The influence of the uniform interpretation on the application of national law requires further in-depth research.

[26] In the case C-131/12 (fn 25) it can be found the statement: '*It is the search engine operator which determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of that activity and which must, consequently, be regarded as the 'controller' in respect of that processing pursuant to Article 2(d)*'.

GDPR – MAIN INTERNATIONAL IMPLICATIONS

Dulce Lopes, University of Coimbra

Abstract:

The General Data Protection Regulation aims to ensure a consistent and homogenous protection of data subjects rights throughout the territory of the European Union Member States and beyond. The broad scope and international reach of the GDPR is, therefore, a *hot topic,* that is currently under discussion and analysis both in Academia and in Courts. This article contributes to the subject, by examining the major international implications of the GDPR both in the private international law and in the international administrative law arenas, now widely conformed by European Union provisions and case law.

Keywords: Data Protection; Extraterritoriality; Data Transfers; Supervisory Authorities

1. Introduction

The protection of natural persons in relation to the processing of personal data is a fundamental right established, within the European Union, in Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU). This protective aim is transversal to all European Union competencies and policies, even when implemented at a national level, which stands as, it should be added, the rule in the European Union judicial and administrative arenas.

However, this is not the only concern that lies behind Regulation (EU) 2016/679, enacted in 27 April 2016, by the European Parliament and the Council, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and that repealed Directive 95/46/EC (General Data Protection Regulation, GDPR). It is clear from the debates previous to and the recitals of this Regulation that a robust entrepreneurial

reasoning is behind the need to stabilize a clear and coherent personal data protection framework that does not strongly differ from state to state. It is indeed the objective of ensuring "*an equivalent level of protection of natural persons and the free flow of personal data throughout the Union*" that is the basis of the necessary subsidiarity considerations within the GDPR (recital 170) [1].

Absent these considerations, it might have sufficed to maintain Directive 95/46/EC in force but with modifications [2] and with due implementation by Member States [3], and not going full force with a stronger legal harmonisation in this area. Despite this [4], the prevailing narrative is still fundamental rights protection, which is the main reason behind the broadening of the territorial scope of the GDPR and for its major international implications. Both issues constitute the objective of this article.

---

[1] There are two major exceptions or deviations to the application of the GDPR. It does not apply to "purely personal or household activity" [Article 2(1)(c)] such as for instance, establishing a mailing list with friends. Also, according to Article 30 (5), it only applies partially to organisations with fewer than 250 employees (small and medium sized enterprises).

[2] One of these modifications has to do with the new legal basis introduced by the Treaty of Lisbon (article 16 TFEU). No. 2 of this provision does not, however, impose any specific instrument (directive or regulation) in the field, just establishes a defined procedure (the ordinary legislative procedure). For instance, in criminal areas the option was for a Directive, given the sensitivities and national differences in the field [Directive (EU) 2016/680 of the European Parliament and of the Council, on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA]. For the main lines of review of the Directive, cf. P. HUSTINX, *EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation*, M. CREMONA (eds.), *New Technologies and EU Law* (Oxford 2017), 148-151.

[3] See for instance the judgment Case C- 275/06, Productores de Música de España (Promusicae) / Telefónica de España SAL, ECJ, 29.1.2008 that states that "[...] *Community law requires that, when transposing those directives, the Member States take care to rely on an interpretation of them which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order. Further, when implementing the measures transposing those directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality*".

[4] Discussing whether data protection should generally be seen as a fundamental right since it is more akin to market regulation than to traditional human rights instruments, cf. B. VAN DER SLOOT, *Legal Fundamentalism: Is Data Protection Really a Fundamental Right?*, R. LEENES ET AL. (eds.), *Data Protection and Privacy: (In)visibilities and Infrastructures* (Berlin 2017), 3-30.

2. GDPR extraterritorial effects: overview

The protection of personal data faces new challenges. The exchange of personal data between private and public actors has increased widely, mostly due to online activities, paving the way to an unprecedented scale in collecting and sharing of personal data that might run contrary to the protection of fundamental rights.

The harmonized framework on data protection aims to ensure a consistent and homogenous application of the rules for the protection of data subject rights all throughout the territory of the European Union Member States and beyond.

Indeed, GDPR sets an unprecedented paradigm in which extraterritoriality is taken to its highest level. Even if Article 4 of Directive 95/46/EC had already established private international law rules on this issue that were seen as highly innovative – though rather troublesome [5] –, other instruments such as adequacy decisions played a relevant, but not undisputed, role in the EU's data protection framework. These issues are addressed in the GDPR. In addition, new mechanisms were introduced into the GDPR that constituted genuine novelties in this area.

Now administrative and jurisdictional issues related to the monitoring or infringements of data protection law tend to be regulated globally, in all its dimensions and layers. This has naturally reflexed in several areas of law that regulate international situations [6]: private international law (in particular conflict of laws), public international law, international administrative law and international civil (and administrative) procedural law. Let us look briefly at these implications in turn [7].

---

[5] I. REVOLIDIS, *Judicial Jurisdiction Over Internet Privacy Violations and The GDPR: A Case Of "Privacy Tourism"?* (2017) 11 (1) *Masaryk University Journal of Law and Technology*, 9-11; M. BRKAN, *Data Protection and Conflict-of-laws: A Challenging Relationship* (2016) 13 *European Data Protection Law Review,* 326.

[6] It should be mentioned that GDPR establishes, for certain purposes and mostly for administrative and judiciary implications, a distinction between international processing of data and a more defined concept of cross-bordering processing [Article 4 (23)] that includes only the processing of personal data that takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State and the processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

[7] This analysis will be made individually for explanatory purposes. However, the links between these areas of law are very close and intertwined. For instance, extraterritoriality in asserting jurisdiction and in applicable law should comply with basic public international law requirements and traditional public international law instruments such as agreements have been comple-

3. Applicable rules on data protection

The main concepts of GDPR that should be considered in what regards private international law rules inserted into the Regulation are the ones of the controller (the one that determines the processing of the data) and processor (the one that operates the data, whether or not by automated means). Simply put, if company A sells clothes in the European Union using company B, an emailing company to track and engage clients, the controller is company A and the processor company B.

On this account GDPR treats the data controller as the principal party for responsibilities such as collecting consent, managing consent-revoking, enabling right to access, etc. In addition, it introduces direct obligations for data processors that are subject to penalties and civil claims by data subjects and presented in a model that has already been named as a "cumulative" liability regime for controllers and processors [8].

That is why Article 28 (1) GDPR imposes upon the controller the choice of processors "providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject", such as approved codes of conduct, certified mechanisms and standard contractual clauses. However, there is no fixed line between a controller and a processor since if this determines the purposes and means of processing, the processor shall be considered to be a controller in respect to that processing [Article 28 (10)] [9].

These two entities are under specific obligations pursuant to Article 27 (1) of the GDPR since where a controller or a processor not established in the Union is processing personal data of data subjects who are in the Union [10], the controller or the processor should, in principle, designate a representative in the Union [Article 27 (1), recital 80]. This represents the introduction by the European Union of a specific

---

mented by other administrative and privative mechanism that allow for international transfer of data.

[8] B. VAN ALSENOY, *Liability under EU Data Protection Law - From Directive 95/46 to the General Data Protection Regulation* (2017) 7 *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 282.

[9] This allocation of responsibilities incorporates the understanding under the Data Directive that processors can be joint controllers whenever they exert decisive influence over the phases of collection and transmission of data (cf., among others, the judgements Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, ECJ, 5.6.2018 and Case C-40/17, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, ECJ, 29.7.2019).

[10] And whose processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required to such data subjects in the Union, or to the monitoring of their behaviour as far as their behaviour takes place within the Union.

private international law rule [already previewed in Article 4 (2) of the Directive] that requires a special substantive obligation for undertakings in international situations. It materialises the need for a "guarantor" located within the European Union in order to have a representative that should not only act on behalf of the controller or the processor but also be addressed by any supervisory authorities [11].

This requirement is in line with Article 3 of the GDPR, under the title "territorial scope". This rule establishes that "*This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not*" (1). Adding that "*This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services* [12]*, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.*" (2) [13].

---

[11] Also, other obligations are envisaged, namely the necessary appointment of a (joint) data protection officer whenever the requirements of Article 37 (1) are met, which might extend to international controllers and processors not established in the European Union. This obligation might seem to be overreaching but taking into account that the DPO is an independent and concerned person that strengthens the monitoring and compliance of personal data protection, it forms a crucial part of the "division of responsibilities" laid down in the GDPR. Given its advisory position, the GDPR does not provide for rules on liability or sanctioning of the Data Protection Officer although this might be provided for in national legislations (cf. P. VOIGT-A. VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR) – a Practical Guide* (Berlin 2017), 61-62).

[12] This offering of goods and services should be read *cum granum salis.* We do not believe as P. DE HERT-M. CZERNIAWSKI, *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context* (2016) 6 (3) *International Data Privacy Law*, 241, put it that the mere fact of having a website that is accessible in the European Union triggers this possibility (somewhat "*analogous to owning a bookshop*" for others to direct themselves to and browse). Indeed if a company is established outside the European Union and does not have any means of processing in the European Union, it should be considered that it falls under the GDPR if it is apparent (see Recital 23) that it offers through the internet goods and services in the European Union – for instance, by using local currencies such as the Euro, local languages or local top-level domains – and not only if it can be accessed by persons located in the European Union, which would be unreasonable (cf. https://gdpr.eu/companies-outside-of-europe/). These criteria are particularly needed since it is very difficult, if not nearly impossible, to insulate websites from "abroad visitors" (on this, see U. KOHL, *Jurisdiction and the Internet–Regulatory Competence over Online Activity* (Cambridge 2007), 278 ff.; and A. LOPÉZ-T. MARTÍNEZ, *El criterio de las actividades dirigidas como concepto autónomo de DIPR de la Unión Europea para la Regulación de las actividades en internet*, (2017) 69 (2) *Revista Española de Derecho Internacional,* 223-256). For non-exhaustive evidence from which it may be concluded that the activity is directed to persons in the European Union, see, although on another subject-matter, the judgment Joined Cases C-585/08 and C-144/09, Peter Pammer et al., ECJ, 7.12.2010, 93).

[13] Article 3(3) also determines that the Regulation applies to the processing of personal data

This rule widely increase the reach of European Union Law since it not only applies to the processing of data in the context of the activities of establishments of a controller or a processor in the Union, regardless of the nature of the processing, but also to a controller or processor not established in the Union if they offer goods or services to data subjects in the Union or if they perform activities that affect them like, for instance, if they profile a natural person, "*particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes*" (Recital 24).

This amplifies the range of European Union Law provisions on data protection to anyone who is doing business or envisages doing business in the European Union, turning the GDPR into a potential "global legal regime" in line with the European Union role as a "global actor". Therefore, establishments should be aware and respect GDPR whenever they process data that branches over to the European Union.

The primary relevant connecting factor is in line with the case law of the European Court of Justice since it applies to processing in connection with the activities of an establishment in the EU regardless of where the processing happens (*e.g.,* cloud storage abroad) [14]. Indeed, a flexible definition of "establishment" and a broad approach on territoriality was already given by the Court of Justice in the Google Spain and Google and Weltimo cases, although under the Directive framework [15].

The second clause for extraterritorial jurisdiction, in which the controller or processor are not established in the Union, are not, in our view, merely effects based since they entail a link, though tenuous as it may be in some cases, to the European Union, given that data subjects should be in the Union [16]. By extend-

---

by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law like, for instance, within consular posts or embassies. A. DE SOUSA GONÇALVES, *The extraterritorial application of the EU Directive on data protection* (2015) 19 *Spanish Yearbook of International Law*, 202, states that "*in these situations, data protection legislation does not have a truly extraterritorial application, since the application of the law of a Member State in a third State results from public international law and occurs in circumscribed cases*".

[14] Cf. S. BU-PASHA, *Cross-border issues under EU data protection law with regards to personal data protection* (2017) 16 (3) *Information & Communications Technology Law*, 218. According to A. AZZI, *The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation* (2018) 9 *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 128, no more mental gymnastics is required since the EU rules apply "*regardless of whether the processing takes place in the EU*.".

[15] Respectively, Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, ECJ, 13.5.2014 and Case C-230/14, Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, ECJ, 1.10.2015.

[16] It involves, therefore, a clear protective aim that is increasingly accepted in the fundamental

ing jurisdiction, it aims to avoid the interpretative problems raised by Article 4 of the Directive when confronted with cases in which intermediaries seek to avoid jurisdiction of courts by referring to the corporate structure and "means" adopted [17].

But this clause also incorporates the own line of thought and genuine policy of the European Union regarding the extension of its legislative and adjudicative powers [18].

On this note, one should be aware that extraterritoriality is no longer an exception in the international arena [19], and though it is not, nor should it be, the rule, it is a recurring feature in many situations that involve fundamental rights, environmental concerns and/or relevant political aims [20].

---

rights field for all persons, not only European Union Citizens or residents in the European Union (cf., on the widening of jurisdiction on the basis of fundamental rights protection, M. DEN HEIJER - R. LAWSON, *Extraterritorial Human Rights and the Concept of "Jurisdiction", Global Justice, State Duties – The Extraterritorial Scope of Economic,* M. LANGFORD-W. VANDENHOLE-M. SCHEININ-W. VAN GENUGTEN (eds.), *Social and Cultural Rights in International Law* (New York 2013), 153-191). In another approach this is seen as a more "market-place" oriented principle (cf. D. MOURA VICENTE-S. DE VASCONCELOS CASIMIRO, *Data Protection in the Internet: General Report* (Berlin 2020), 33).

Stating that this is an effects based clause because it puts focus on the potential harmful conduct and discards the location of the processing, cf. A. AZZI, *The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation* (2018) 9 *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 131. B. VAN ALSENOY, *Reconciling the (extra)territorial reach of the GDPR with public international law*, G. VERMEULEN-E. LIEVENS (eds.), *Data Protection and Privacy under Pressure – Transatlantic tensions, EU Surveilance and Big Data* (Antwerp 2017), 97, considers that this provision entails a combination of the objective territoriality and the effects doctrine.

[17] C. KUNER, *Data Protection Law and International Jurisdiction on the Internet (Part 2)* (2010) 18 (3) *International Journal of Law and Information Technology*, 240, defended that "*the European Commission should consider revising Article 4(1) (c) to focus it away from the use of in the EU, and more towards the targeting criteria of Article 15(1) of the Brussels I Regulation, although it can be difficult to determine when an online activity is 'targeted' or 'addressed' at a particular State*". Cf, under the same line, L. MOEREL, *The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?* (2011) 1 (1) *International Data Privacy Law*, 28-46. GDPR, according to whom the relevance of the location of the equipment is replaced by a focus on people in the EU.

[18] E. USTARAN, *The Scope of Application of EU Data Protection Law and Its Extraterritorial Reach*, N. ISMAIL-E.L. YONG CIEH (eds.), *Beyond Data Protection – Strategic Case Studies and Practical Guidance* (Berlin 2013), 135- 156, dwells on the evolution of data protection regulation in the European Union in order to reach a right balance and the policy objectives of the European Union legislators.

[19] As defended, for instance, by L. STRISOWER, *L'Exterritorialité et ses Principales Applications,* ACADÉMIE DE DROIT INTERNATIONAL DE LA HAYE (eds.), *Recueil des Cours* (Paris 1925) I, 233.

[20] STEFANO BATTINI considers that the international interdependence converts extraterritoriali-

Jurisdiction is no longer, if it ever was, understood as an incidence of power over a certain territory. It is necessary to complement this dimension with the personal and functional aims of jurisdiction, which allows for jurisdiction based on the principles of nationality (active and passive), protection, universality and nowadays effects [21].

However, there must be a *genuine link* that respects the standards of international law for a state to legitimately assume jurisdiction [22] or a *reasonableness test* according to which the same conclusions are reached [23]. Criteria that seem to have been respected by Article 3 of the GDPR since the aim of this regulation is to ensure an effective protection of data subjects within the European Union, fulfilling its commitment as a fundamental rights organisation [24].

It is naturally expected that the more extraterritorial jurisdiction is accept-

---

ty into a non excepcional phenomenon, and that extraterritoriality *de iure* aims to contradict the impacts of an inevatible extraterritoriality *de facto*, (S. BATTINI, *Extraterritoriality: an Unexceptional Exception* (2008) *Séminaire de droit administratif, européen et global "Extraterritoriality and Administrative Law", 9* available at http://www.sciencespo.fr/chaire-madp/sites/sciencespo.fr.chaire-madp/files/stefano_battini.pdf, and S. BATTINI, *Globalisation and Extraterritoriality: an Unexceptional Exception,* G. ANTHONY-J. B. AUBY-J. MORISON-T. ZWART (eds.), *Values in Global Administrative Law* (Oxford 2011), 67).

On the role of *internet* in reconfiguring extraterritorial jurisdiction, cfr. T. SCHULTZ, *Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface* (2008) 19 (4) *The European Journal of International Law,* 799-839; and D. JERKER-B. SVANTESSON, *Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation* (2015) 5 (4) *International Data Privacy Law*, 227.

[21] In general, on these principles cf., M. AKEHURST, *Jurisdiction in International Law* (1972 - 1973) 46 *British Yearbook of International Law*, 152-166, and C. RYNGAERT, *Jurisdiction in International Law* (Oxford 2015) 2nd ed., 104-141.

On the data protection field, cf. C. KUNER, *Data Protection Law and International Jurisdiction on the Internet (Part I*) (2010) 18 (2) *International Journal of Law and Information Technology*, 176-193, and ID, *Data Protection Law and International Jurisdiction on the Internet (Part II)* (2010) 18 (3) *International Journal of Law and Information Technology,* 227-247.

[22] F.A. MANN, *The Doctrine of Jurisdiction in International Law* (1973) *Studies in International Law,* 37.

[23] C. RYNGAERT, *Jurisdiction – Towards a Reasonableness Test*, M. LANGFORD-W. VANDENHOLE-M. SCHEININ-W. VAN GENUGTEN (eds.), *Global Justice, State Duties – The Extraterritorial Acope of Economic, Social and Cultural Rights in International Law* (New York 2013), 192-211.

[24] We agree in this part with P. DE HERT-M. CZERNIAWSKI, *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context* (2016) 6 (3) *International Data Privacy Law*, 231. Against, C. KUNER, *The European Union and the Search for an International Data Protection Framework* (2014) 2 (1) *Groningen Journal ofInternational Law*, 55-71, and D. SVANTESSON, *Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation* (2015) 5 (4) *International Data Privacy Law,* 234, that allude to the imposition of a privacy model on other jurisdictions instead of contributing to creation of better global privacy standards.

ed, the more political and legal conflict will increase [25], taken that the same conduct might trigger several jurisdiction clauses. This concurrence of jurisdiction is common in the international arena [26], and though international law does not provide a resolution framework for these cases, it has led to a certain international convergence movement in protecting fundamental data protection rights by public and private entities, all of which is welcomed and to which GDPR has widely contributed.

Comparing Article 3 GDPR provision with the former Article 4 of the preceding Directive, it seems clear that the GDPR no longer contains a conflict-of-laws provision determining the applicable law of a particular Member State for the processing of personal data [27]. It now includes a unified set of rules that Member States directly apply without need for further implementation to their national legislations, except certain situations. The scope of application of GDPR provisions is therefore defined in a self-limited way. This means that GDPR provisions will be applicable to all situations that involve data processing that fall under Article 3 unilateral conditions. Taking an international contract on services provision that states that personal data processing is regulated according to a non-European Member-State legislation, and where such data processing impacts data subjects located in the European Union, GDPR norms should nonetheless be applicable.

This points out to the qualification of the relevant provisions as overriding mandatory provisions, taking into consideration the definition in Article 9 of the Rome I Regulation. Indeed, they aim to safeguard fundamental political, economic and social interests on data protection common to Member States and to the European Union, which provides them with an imperative weight in international situations. And if this characterisation was already envisaged regarding Article 4 of Directive [28], it is now clear from both the wording and the

---

[25] I. JALLES, *Extraterritorialidade e Comércio Internacional – Um Exercício de Direito Americano* (Lisboa 1988), 205-208.

[26] F.A. MANN, *The Doctrine of Jurisdiction in International Law* (1973) *Studies in International Law,* 3.

[27] M. BRKAN, *Data Protection and Conflict-of-laws: A Challenging Relationship* (2016) 13 *European Data Protection Law Review,* 336, points that out since the regulation itself unifies the legal regime on processing of data.

[28] C. PILTZ, *Rechtswahlfreiheit im Datenschutzrecht?* (2012) *K&R – Kommunikation & Recht*, 640-645; M. BRKAN, *Data Protection and Conflict-of-laws: A Challenging Relationship* (2016) 13 *European Data Protection Law Review,* 333-334. Arguing that this characterisation had not been cleared by the European Court of Justice, cf. I. REVOLIDIS, *Judicial Jurisdiction Over Internet Privacy Violations and the GDPR: A Case of "Privacy Tourism"?* (2017) 11 (1) *Masaryk University Journal of Law and Technology,* 12. We believe, however, that judgment Case C-191/15, Verein für Konsumenteninformation v Amazon EU Sàrl, ECJ, 28.7.2016 sufficiently supports this characterisation.

teleology of Article 3 GDPR that it is the rightful one [29].

However, as Jiahong Chen clearly states, this is not the end of the story since there are still remaining problems of applicable national law once the GDPR continues to leave relevant areas for national interpretation and further regulation (or derogations) from Member States, which, for that Author, creates a serious loophole that could possibly cancel out most of the improvements brought by the reform [30].

Although we agree that it might have been clearer to establish conflict of law rules in cases where diversity between Member States is allowed for, we do not believe that the situation is as calamitous as it is made out to be.

The application of the GDPR itself may not respond sufficiently or clearly to all questions relevant to Court proceedings or to related questions. However, in a situation in which there is a contract between the data subject and the data controller, it is acknowledged that the Rome I Regulation will provide sufficient guidance on the choice of applicable law. However, the application of Rome II Regulation to these cases in non-contractual situations continues to be a grey zone given the fact that it is not applicable to privacy issues [31].

---

[29] P.A. DE MIGUEL ASENSIO, *Jurisdiction and Applicable Law in the New EU General Data Protection Regulation* (2017) 69 (1) *Revista Española de Derecho Internacional,* 104.

[30] J. CHEN, *How the best-laid plans go awry: the (unsolved) issues of applicable law in the General Data Protection Regulation* (2016) 6 (4) *International Data Privacy Law,* 311-316.

[31] Article 1(2) of the Rome II Regulation provides that '*[t]he following shall be excluded from the scope of this Regulation: [. . .] (g) non-contractual obligations arising out of violations of privacy and rights relating to per- sonality, including defamation'.* J. CHEN, *How the best-laid plans go awry: the (unsolved) issues of applicable law in the General Data Protection Regulation* (2016) 6 (4) *International Data Privacy Law,* 319, argues that even if the Charter distinguishes between these two rights (right to data protection and right to privacy), it is very difficult to separate them in Courts, because we "*will need a handle on the traditional tort law system in order to translate the language of data protection law into the language of private law. Without such a handle – right to privacy – the claim of breach of data protection can hardly find its way into the private law system*". P. HUSTINX, *EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation*, M. CREMONA (eds.), *New Technologies and the Law* (Oxford 2017), 172, takes a different view and proposes that article 8 of the Charter to reach its fullest potential should be better distinguished from article 7, meaning that "*Article 8, involving all processing of personal data, should not be confused with the question of wether the fundamental right to data protection has been interfered with*". Along the same line, cf. J. KOKOTT-C. SOBOTTA, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR* (2013) 3 (4) *International Data Privacy Law*, 222-228; O. LYNSKEY, *Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order* (2014) 63 (3) *International and Comparative Law Quarterly*, 569-597; and G. GONZÁLEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Berlin 2014), 268-272.

Going against the mainstream current [32], we believe that the Rome II Regulation should govern non-contractual issues related to data protection. Indeed, long before this Regulation was passed, Directive 95/46/EC already established a conflict-of-laws provision that explicitly governed data privacy [see, among many others, recital 11 and article 1(1)] [33]. This Directive is even mentioned in the Rome II Regulation (Article 30, review clause), but was not directly affected by it (Article 27) [34]. The conclusion possible is, henceforth, that the concept of privacy incorporated – after strong debate – in Article 1 (2) (d) of the Rome II Regulation did not include data privacy, by then governed by Directive 95/46/EC and the implementing laws of the Member States. This conclusion goes along the lines of the debate in which the main issues at stake in the Rome II Regulation were more "traditional" violations to privacy such as, for example, publications, defamation and slander in newspapers, magazines and, of course, the internet - all of which more related to freedom of the press and freedom of expression in other media than with data protection [35].

This means that when Directive 95/46/EC was repealed by the GDPR, the concept of privacy under the Rome II Regulation did not "expand" its scope to include data protection. In fact, as an exception to the general scope of application of this instrument, the concept of privacy should continue to be read as it once was, and not include matters that were (re)regulated by the European Union in the GDPR. Consequently, in the absence of a European Union Instrument that defines specific rules-of-conflict for data protection, the Rome II Regulation should apply to all non-contractual issues that were not fully harmonised by

---

[32] See for instance, U. GRUŠIC' ET AL., *Cheshire, North & Fawcett: Private International Law* (Oxford 2017) 15th ed., 798-799, according to which "The exclusion does however extend to violations of data protection laws"; and D. MOURA VICENTE-S. DE VASCONCELOS CASIMIRO, *Data Protection in the Internet: General Report* (Berlin 2020), 37-38. Less stringently, see A. DICKINSON, *The Rome II Regulation – The Law Applicable to Non-Contractual Obligations* (Oxford 2008), 240 and P. A. DE MIGUEL ASENSIO, *Jurisdiction and Applicable Law in the New EU General Data Protection Regulation* (2017) 69 (1) *Revista Española de Derecho Internacional,* 105.

[33] A concept that has been developed and that does equate fully with the right to privacy. Cf. the seminal study of L. A. BYGRAVE, *Data Privacy Law: An International Perspective* (Oxford 2013). To mark the distinction between privacy and data protection, in the GDPR reference to privacy has been omitted entirely. Which, from our point of view, is an indicator of an increasing distinction, both doctrinal and legislative, of both concepts.

[34] Indeed, the proposal of the European Parliament in the 1st and 2nd reading positions that extended the special rule to "violations of privacy or of rights relating to the personality resulting from the handling of data protection" did not survive the legislative process.

[35] See, among many others, J. MEEUSEN, *Rome II: A True Piece of Community Law,* J. AHERN-W. BINCHY (eds.), *The Rome II Regulation on the Law Applicable to Non-Contractual Obligations – A New International Litigation Regime* (Boston 2009), 15.

the GDPR and that were not excluded from the scope of application of Rom-II Regulation.

This is, in our opinion, the only reading that salvages the teleological and autonomous interpretation of the concepts of European Union Law [36], to which the European Union and Member-States are bound and the one that puts an end to countless controversies and divergences in the field [37]. And if the application of the Rome II Regulation to some aspects of data protection may cause fragmentation of the applicable law, given the fact that the *loci damni* can be widespread [38], it will at least give clarity on many other issues that would have otherwise had to be solved under the also divergent applicable international private rules of the Member-States.

One of the main refractions of this scope of application resides in Article 82 (right to compensation and liability) that defines specific rules to allow for private enforcement of the GDPR. It clearly states that any person who has suffered material or non-material damage as a result of an infringement of GDPR rules have the right to receive compensation from the controller or processor for the damage suffered. This points out that GDPR and other European Union provisions will also be the guiding criteria in non-contractual matters.

4. International data transfers

In what regards transfer of data from the European Union to third countries and international organisations, it is established that both Union and Member States might conclude international agreements as long as such agreements respect GDPR and other European Union provisions on data protection. They should, therefore, guarantee an appropriate level of protection for the fundamental rights of the data subjects (Recital 102).

---

[36] Indeed, the wording of the provision of Rome II, which only refers to privacy, its history and background (media violations and non-technical aspects of data protection), the systematic context in which the provision is found, including its relation to other provisions in other European Union instruments (at the time the Directive that explicitly regulated data privacy), and the objectives of the provision in question and the objectives and scheme of the overall Regulation, that aims to be a general scheme on all non-contractual obligations, point out the fact that it now includes data protection issues.

[37] Therefore, unlike what is defended by H. HIJMANS, *The European Union as Guardian of Internet Privacy the Story of Art 16 TFEU* (Berlin 2016), 66-68, there are relevant legal effects in distinguishing between privacy and data protection on the internet.

[38] For an analysis on this issue, cf. D. SVANTESSON, *Rome II Regulation and Choice of Law in Internet-Bases Violations of Privacy and Personality Rights - On the Wrong Track, but in the Right Direction* (2011) 16 *Austrian Review of International and European Law,* 275-298.

The relevance of this level of protection goes so far as to impeding the recognition of enforcement of decisions of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data when it is not frameworked by an international agreement such as a mutual assistance treaty, or other grounds of transfer included in the GDPR (Article 48).

This means that international agreements are not the only basis for international transfer of personal data and allows for other mechanisms of unilateral or contractual nature to take place; instruments that, it should be emphasized, require no previous agreement between States. The other grounds for transfer mentioned in the Regulation include the issuance of adequacy decisions, appropriate safeguards and derogations for specific situations.

Adequacy decisions are implementing decisions from the Commission with binding effect for the entire Union that establish that a third country, a territory or specified sector within a third country, or an international organisation offer an adequate level of data protection (Article 45). The adoption of such decisions involves a lengthy and complex process and is mainly why, at the time of this writing only these third countries ensured an adequate level of protection: Andorra, Argentina, Canada (commercial organisations) Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay (private sector organisations) and the USA (if the recipient belongs to the Privacy Shield) [39].

The agreements and adequacy decisions on data protection have been subject to criticism, mostly in what involves data protection transfers between the European Union and the United States. In the wake of the Schrems "saga", the Court of Justice decided that Commission's Decision 2000/520/EC of 26 July 2000, regarding the adequacy of the protection provided by the safe harbour privacy principles, was invalid since the appropriate level of protection required by European Union data protection law (at the time the Directive) was not met. Furthermore, the protection granted was not general and interference from United States authorities was permitted given the prevalence of the United States public interest; additionally, restrictions were not proportional with no adequacy and necessity in the identification of storable data [40].

---

[39] Cf. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[40] Case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECJ, 6.10.2015. This case is also of great relevance to the competencies of the Supervisory Authorities since while they are bound by the Commission's Decision when considered valid, this shouldn't prevent them from fully using their investigative powers when facing claims on the (in)adequacy of protection afforded by third countries.

In general, these difficulties to meet the requirements of data protection in the European Union opened the door to alternative forms of demonstrating that respect in a "case by case" basis. The finding that a third country itself ensures a level of protection essentially equivalent to that imposed by European Union law and that, as a consequence, personal data may be transferred to that country without the controller being required to obtain specific authorisation, has proven to be quite difficult [41].

In this case, appropriate safeguards should apply in the absence of an international agreement and an adequacy decision to allow for a controller or processor to transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available (Article 46). This implies that a set of instruments that include binding corporate rules, standard data protection clauses, approved codes of conduct or approved certification mechanism that ensure an appropriate level of data protection are available for public and private data importers.

These tools basically rely on a contractual commitment undertaken by a third state data importer to conform to a set of obligations relating to the processing of data that comply with the GDPR provisions and whose respect must be safeguarded both by the data-importer and the data-exporter. Also, since these contracts must confer effective legal remedies, the data subject is usually considered a beneficiary of the contract in order to be able to react against both the data importer and/or exporter. These contracts, though usually private in nature, require a public element given that they have to be approved by a national supervisory authority who is called to assess the existence of appropriate safeguards and means of redress [42].

But again, despite its practical relevance [43], this mechanism has not been

[41] C. KUNER, *Developing an Adequate Legal Framework for International Data Transfers*, S. GUTWIRTH ET AL. (eds.), *Reinventing Data Protection?* (Berlin 2009), 263-273 proposed that, given the difficulties in reaching adequacy decisions (length and complexity, political tensions, overload and lack of means for the adequacy assessment), there should be other ways to prevent circumvention of European Union law under an accountability standard.

[42] We agree with M. MANTOVANI, *Contractual Obligations as a Tool for International Transfers of Personal Data* (2020) availabe at https://eapil.org/2020/01/20/contractual-obligations-as-a-tool-for-international-transfers-of-personal-data/, that this does not change the civil and commercial nature of most contracts as they are usually linked to other contractual arrangements between the parties. Also, like the author we believe that this is a relevant governance tool since it allows for a wider acceptance *from within* of European Union data protection standards and contribute to its dissemination in areas outside of its normal reach.

[43] The most popular method by far for data transfers outside the EU is the use of standard contractual clauses (88% of respondents), followed by compliance with the EU-U.S. Privacy Shield arrangement (60%), according to the IAPP-EY Annual Governance Report 2019, available at https://iapp.org/store/books/a191P000003Qv5xQAC/.

well received. At the time of completing this paper, a decision is pending in the Court of Justice (the so called Schrems II case) against the Commission Implementing Decision (EU) 2016/1250 – EU-U.S. Privacy Shield –, that is applicable to data transfers between the European Union and the United States. However, it is also aimed against the Commission Decision 2010/87/EU, of 5 February 2010, regarding standard contractual clauses for the transfer of personal data to processors established in third countries.

In this case, Advocate General SAUGMANDSGAARD ØE, taking into consideration the GDPR provisions, considered, in 19 December 2019, that the standard contractual clauses framework is sufficient. In situations where the safeguards in the standard contractual clauses may be reduced or eliminated (for instance when the law of the third country of destination imposes obligations that are contrary to the requirements of those clauses on the importer or edits blocking Statutes), it should be, on a case-by-case basis, up to the controller or, when it discharges its obligations, up to the supervisory authority to examine the situation and, if necessary, to prohibit or suspend such transfers. Additionally, if the Supervisory Authority does not exercise its corrective competences under the GDPR, it may be subject to a judicial action from the complainants, given its reduced discretionary powers on this field [44].

Furthermore, GDPR also allows for derogations for specific situations in a very similar fashion to what was already established in the Directive. In this case a transfer or a set of transfers of personal data to a third country or an international organisation will take place only on the basis of typified justifications laid down in Article 49 GDPR. The most important of these derogations in quantitative terms is the explicit consent of the data subject to the proposed transfer, but other relevant clauses, with underlying private or public concerns, are also established. Given that these are derogations, they must be last resort and occasional according to their exceptional nature as established in Guidelines 2/2018 on derogations of Article 49 [45].

---

[44] Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems, ECJ, 9.5.2018. In what regards the Privacy Shield Adequacy Decision, the Advocate General has argued for the practical irrelevance of its invalidity analysis. However, this raises doubts in what regards the safeguards around the equivalence of the United States surveillance measures and the role of the Privacy Ombudsperson: if they can indeed compensate for insufficiencies of the judicial protection afforded to individuals whose data is transferred to the United States. For other criticism on this framework, see S. BU-PASHA, *Cross-border issues under EU data protection law with regards to personal data protection* (2017) 26 (3) *Information & Communications Technology Law,* 224 - 227. There is also another case pending before the General Court Case T-738/16, La Quadrature du Net and Others v Commission, GC, 25.10.2016 only directed towards the Privacy Shield Framework.

[45] GDPR additionally offers a last resort mechanism [Article 49 (1) last paragraph] according to which, when none of the above-mentioned exist "*a transfer to a third country or an interna-*

There are, therefore, several ways to framework international transfer of data that go far beyond the typical public international law mechanisms and that allow for unilateral decisions and contractual arrangements in the field. These should, however, be justified and comply with the appropriate level of data protection set forth in the GDPR, which will be under the control of the Supervisory Authorities, the focus of our analysis at present.

5. The supervisory mechanism

With more responsibility comes more supervision. Therefore, the role of supervisory authorities and the personal data supervisory mechanism is essential to the design of the GDPR.

The Court of Justice has previously ascertained that the supervisory authorities are the guardians of fundamental rights and freedoms put at stake by data processing operations and, therefore, their independence is an essential element of their protection and cannot be restricted in any way [Article 8 (3) of the Charter] [46].

Supervisory authority or Data Protection Authority (DPA) is a "mandatory" independent public authority established in each State which is concerned by the monitoring of the processing of personal data because "*(a) the controller or processor is established in the territory of the Member State of that supervisory authority; (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or (c) a complaint has been lodged with that supervisory authority*" [Article 4 (22)].

The tasks of each supervisory authority are defined in Article 57. The number and nature of such tasks are impressive. They range from: monitoring and enforcement, providing information to private and public entities, raising cooperation awareness, handling and investigating complaints, adopting standard contractual clauses, encouraging the drawing up of codes of conduct, approving binding corporate rules, authorising contractual clauses and provisions, and act-

tional organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data".

[46] On this issue, Case C-518/07, European Commission v Federal Republic of Germany, ECJ, 9.3.2010; Case C-614/10, European Commission v Republic of Austria, ECJ, 16.10.2012; Case C-288/12, European Commission v Austria, ECJ, 8.4.2014.

ing in certification and accreditation procedures. Correspondingly, the powers of such authorities are very wide and allow for various forms of investigation and audits: the imposition of fines or other penalties or of temporary or definitive limitation including a ban on processing or suspension of international data flows, the ordering of rectification or erasing of personal data and the withdrawal of certifications, etc.

This is a relevant difference regarding the Directive since it has already imposed on states a minimum status for their supervisory authorities (Article 28), but the powers entailed were not as broad nor as intrusive as the ones established in the GDPR [47]. A definitive option towards strong and legally well-equipped supervisory authorities was made because the implementation of all mechanisms established in the GDPR so require.

Furthermore, considering that a great number of situations involve data protection issues and concerns in many member states, GDPR defines which authority should be the lead in each case to enable a more effective monitoring and control of GDPR rules as well as to detect and pursue eventual infractions. This "one-stop-shop" system aims to enable more than just mere cooperation obligations between supervisory authorities [like the ones previewed in Article 28 (6) of Directive] [48], since it represents an institutionalisation of common and integrated procedures between member states that might lead to the adoption of decisions with transnational effects, that should be automatically recognised in other member states [49].

---

[47] According to the Final Report of the European Commission on the Comparative Study of Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, of 20 January 2010, pp. 43-44, available at https://op.europa.eu/en/publication-detail/-/publication/9c7a02b9-ecba-405e-8d93-a1a8989f128b, "*DPAs have great insight and knowledge, and provide helpful guidance on the law - but they are not effective in terms of enforcement: "Policing" of data protection compliance by DPAs is generally weak and ineffective*".

[48] The GDPR's cooperation and consistency mechanism only applies to controllers with an establishment, or establishments, within the European Union. If the company does not have an establishment in the EU, the mere presence of a representative in a member state does not trigger the one-stop-shop system. This means that controllers without any establishment in the EU must deal with local supervisory authorities in every member state they are active in, through their local representative. However, there are relevant doubts as to whether those representatives can be subject to enforcement proceedings in the event of non-compliance by the controller or processor. This is mentioned in Recital 80 but not provided for in the binding articles of the Regulation, so there is controversy as to whether a representative may incur some sort of liability, in addition to the operator (on this, cf. A. AZZI, *The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation* (2018) 9 *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 133).

[49] This might be particularly relevant on de-referencing decisions, in which a mere territorial effect might not suffice to guarantee the effective and complete protection of data subjects' rights since it shouldn't necessarily be restricted to national domains. In this situation, the European

Article 56 establishes as lead supervisory authority the one of the main establishment or of the single establishment of the controller or processor [50], except when processing is carried out by public authorities or private bodies acting in the public interest. In this case the supervisory authority of the member state concerned will always be competent, Article 55 (2).

As a lead supervisory authority, it takes up the instruction of the administrative procedure and conducts itself in such a way as to reach the highest level of consensus between the other Supervisory authorities concerned. Of course, the instruction phase of the procedure can be developed in articulation between these entities by the provision of mutual assistance (Article 61) and the conducting of joint operations (Article 62). But it is up to the lead supervisory authority to, after the necessary diligences and if the decision isn't urgent, case then Article 66 applies, to "*submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views*" – Article 60(2).

If this draft proposal is accepted or not opposed by the other concerned supervisory authorities, "*the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it*" (No. 6). In this case the "*The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision*" (No. 7). Therefore, the decision of the lead supervisory authority produces real transnational effects in other member states [51].

Court of Justice already ruled that a de-referencing in all search engines might not be necessary and proportional; however, it pointed out the necessity of balancing of competing rights by the controller and of cooperation between supervisory authorities in order to reach a consensus and a single decision which is binding on all those authorities and the controller [Case C- 507/17, Google LLC, ECJ, 24.9.2019, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)]. For a comment on this case, cf. Y. MIADZVETSKAYA- G. VAN CALSTER, *Google at the Kirchberg Dock. On Delisting Requests, and on the Territorial Reach of the EU's GDPR* (2020) 1 *European Data Protection Law Review,* 143-151.

[50] If there are doubts regarding this issue, it is up to the Board to adopt a binding decision on which of the supervisory authorities concerned is competent for the main establishment [Article 65 (1) (b)]. In order to avoid some of these doubts, the Article 29 Data Protection Working Party has issued guidelines for identifying a controller or processor's lead supervisory authority on 13 December 2016, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235.

[51] On transnational acts and their effects, see J. RODRIGUEZ-A. MUÑOZ (eds.), *Recognition of Foreign Administrative Acts* (Berlin 2015) and D. LOPES, *Eficácia, Reconhecimento e Execução de Actos Administrativos Estrangeiros* (Coimbra 2018), 339 ff.

In cases where one or more of the other concerned supervisory authorities expresses a relevant and reasoned objection to the draft decision, two possibilities open. If the lead supervisory authority does not agree with such objection, a consistency mechanism is in order [article 60 (4)] and a dispute resolution by the Board takes place (article 65). Within this procedure, the European Data Protection Board adopts a binding decision on the matter that is reported to the supervisory authorities and to the Commission. However, it is up to the lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged to adopt its final decision on the basis of the Board's decision that should be attached to it.

In the case where the lead supervisory authority intends to follow the relevant and reasoned objection made, it submits a revised draft decision for their opinion [Article 60 (5)] to the other supervisory authorities concerned. Nevertheless, if a concerned Supervisory Authority still objects, the consistency mechanism also applies.

These new forms of mixed administration raise questions of justiciability of the decisions taken since the right to an effective judicial remedy should be, in principle, directed towards the decisions of the Supervisory authorities (Article 78) even in cases in which they are preceded by an opinion or a decision of the Board in the consistency mechanism [knowing that the Board is a body of the Union and has legal personality, Article 68(1) GDPR]. Though in these cases the opinion or decision of the Board should be forwarded to the Court and, therefore, should be taken into consideration, the appraisal of their validity will be out of the national Courts reach since they are pledged, in these cases, to ask for a preliminary ruling from the Court of Justice.

There are areas, however, that are still dependent upon "nationalised" indirect administration: administrative fines and other penalties. Nevertheless, in order to reinforce supervisory authorities powers, general conditions for imposing administrative fines are established in the GDPR (article 83) [52] and other penalties, usually of criminal nature, are explicitly allowed for (article 84) [53].

Another aspect that merits attention is the fact that these supervisory rules do not extend as far as the material scope of GDPR, and leave international enforcement [54] mainly to international cooperation efforts [55] and prin-

[52] Article 29 Data Protection Working Party has issued guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, 3 October 2017, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237.

[53] However, there is no harmonisation of the use of criminal sanctions. Cf. P. DE HERT, *The EU data protection reform and the (forgotten) use of criminal sanctions* (2014) 4 *International Data Privacy Law,* 262-268.

[54] Though extraterritorial prescriptive jurisdiction has augmented, this tendency has been less

cipally to the adjustment of controllers and processors to a high level of data protection.

6. International civil and administrative procedural law

Regarding international civil and administrative procedural law, GDPR establishes special rules on jurisdiction that show how far the European Union has come in trying to complement private and public enforcement in data protection issues [56].

In the first case, the right to an effective judicial remedy against a controller or processor should be brought before the courts of the member state where the controller or processor has an establishment. Alternatively, such proceedings based on the material scope of the GDPR may be brought before the courts of the member state where the data subject has his or her habitual residence unless the controller or processor is a public authority of a member state acting in the exercise of its public powers (Article 79).

There is, therefore, alternativeness between these two grounds for jurisdiction. The data subject should choose, if those grounds are not coincidental, which is more favourable: if the courts of the place of establishment where an enforcement of the decision might be easier to practically accomplish [57], if the courts of his/her habitual residence taking into consideration, for instance, the knowledge of the judicial system and the language factor.

---

visible and effective in what regards enforcement jurisdiction. Therefore, it is common in the international arena that there is prescription without enforcement. Cf. D. W. BOWETT, *Jurisdiction: Changing Patterns of Authority over Activities and Resources* (1982) 53 *The British Yearbook of International Law,* 1 and P. VAN SLOT-E. GRABANDT, *Extraterritoriality and Jurisdiction* (1986) 23 (3) *Common Market Law Review,* 548.

[55] There are, nonetheless, cases in which states cooperate in the enforcement of foreign administrative decisions as in the internet arena, for example. Cf. B. H. OXMAN, *Jurisdiction of States*, R. WOLFRUM (eds.), *The Max Planck Encyclopedia of Public International Law* (Oxford 2012) 6, 547 and H.L. BUXBAUM, *Territory, Territoriality, and the Resolution of Jurisdictional Conflict* (2009) 57 *The American Journal of Comparative Law,* 673.

[56] Nevertheless, the judicial and administrative lines of jurisdiction are not sufficiently interconnected, which means that a full protection of data subject rights may depend on initiating both (cf. P.A. DE MIGUEL ASENSIO, *Jurisdiction and Applicable Law in the New EU General Data Protection Regulation* (2017) 69 (1) *Revista Española de Derecho Internacional,* 92).

[57] It should be noted that a Member State judgment concerning "civil and commercial matters", can nonetheless, be recognized and enforced in the other European Union Member States as well as Norway, Iceland and Switzerland, under Regulation (EU) No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters or the 2007 Lugano Convention.

Questions still arise regarding the relation between this specific provision and the European Union Regulations. The wording of recital 147 – "*(w)here specific rules on jurisdiction are contained in this Regulation, in particular as regards proceedings seeking a judicial remedy including compensation, against a controller or processor, general jurisdiction rules such as those of Regulation (EU) No 1215/2012 of the European Parliament and of the Council (13) should not prejudice the application of such specific rules*" is not clear on this behalf[58].

It is arguable if, besides the GDPR, also general rules on jurisdiction may apply, being the "*actor sequitur forum rei*" principle the most relevant. Since the objective of the GDPR is to provide a wide range of guarantees for data subjects, we tend to agree with Lundstedt that these grounds do not supplant but supplement the general rules on jurisdiction[59]. One thing is certain, general rules that contradict the jurisdictional grounds laid down in Article 79 are not admissible as, for instance agreements that establish exclusive choice of court clauses[60].

Regarding administrative procedures, Article 78 enshrines the right to an ef-

---

[58] Also, article 67 of Regulation (EU) No 1215/2012 stipulates that it "*shall not prejudice the application of provisions governing jurisdiction and the recognition and enforcement of judgments in specific matters which are contained in instruments of the Union*".

[59] L. LUNDSTEDT, *International Jurisdiction over Cross-border Private Enforcement Actions under the GDPR* (2018) 57 *Stockholm Faculty of Law Research Paper Series*, 253*,* available at *https://ssrn.com/abstract=3159854;* also P.A. DE MIGUEL ASENSIO, *Jurisdiction and Applicable Law in the New EU General Data Protection Regulation* (2017) 69 (1) *Revista Española de Derecho Internacional,* 99-100. IOANNIS REVOLIDIS, *Judicial Jurisdiction Over Internet Privacy Violations and the GDPR: A Case of "Privacy Tourism"?* (2017) 11 (1) *Masaryk University Journal of Law and Technology,* 22-23, remarks that, applied together, GDPR and Brussels Ia [Article 7(2)] would create a multitude of different *fora* in favour of the data subject, which would be detrimental to the administration of justice within the European Union, at least until clarification from the Court of Justice. This profusion of possible competent *fora* was not ignored by the GDPR, which set rules on suspension of proceedings, whenever more than one court of a member state was seized concerning the same subject matter (article 81). According to M. REQUEJO ISIDRO, *Procedural Harmonization and Private Enforcement in the Area of Personal Data Protection* (2019) 3 *Max Planck Institute Luxembourg for Procedural Law Research Paper Series* available at https://ssrn.com/abstract=3339180, the wording of this provision is "*all inclusive: at least at first sight it could be equally applied to judicial proceedings for a remedy against a decision of a supervisory authority, or for a civil remedy between private parties*". Against, P.A. DE MIGUEL ASENSIO, *Jurisdiction and Applicable Law in the New EU General Data Protection Regulation* (2017) 69 (1) *Revista Española de Derecho Internacional,* 102-103, sees it as a rule only applicable in procedures against supervisory authorities since in civil claims Articles 29 and 30 of Regulation (EU) No 1215/2012 should be deemed applicable.

[60] However, jurisdictional clauses as such are not forbidden, if they are not exclusive. They might also help to identify connecting factors and in particular those regarding the location of the establishments of the controller or processor contributing, therefore, to legal certainty (cf. F. FANGFEI WANG, *Jurisdiction and Cloud Computing: Further Challenges to Internet Jurisdiction* (2013) 24 *European Business Law Review*, 616).

fective judicial remedy against a legally binding decision of a supervisory authority concerning them, plus the right to an effective judicial remedy where the supervisory authority does not handle a complaint or does not inform the data subject on the progress or outcome of the complaint lodged within three months [61].

Therefore, not only actions but also omissions should merit a specific judicial response from the member state where such supervisory authority is established. This is particularly relevant in cases of complaints as, for instance, regarding data transfers that are not appropriately investigated and eventually pursued by supervisory authorities. In sum, in the data protection area a full jurisdictional review in administrative matters should be available and entails the possibility of analysing in matters of fact and law decisions or omissions of the supervisory authorities [62].

Another important consequence of this provision is that, unlike what was allowed for under the Directive (and according to a decision of the Court of Justice) [63], national law should not require that the data subject first exhaust administrative remedies before bringing a court action against a Supervisory Authority. Of course other administrative or non-judicial remedies may exist; however they should do not prejudice the immediate right to an effective judicial remedy against such Authorities, which increases the "control" of data subjects regarding their data, escaping the eventual limitations (financial, administrative or others) of the competent Supervisory Authorities to handle their claims.

In any of these cases, where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with the law of a Member State, has statutory objectives which are in the

---

[61] This is a novelty of the GDPR imposing a fixed and uniformised deadline on handling complaints by member states and, therefore, innovating from the usual *lex fori* rule in administrative and procedural matters.

[62] This is seen as a form of furthering the accountability of these expert bodies and to contribute to good governance within the European Union (cf. H. HIJMANS, *The European Union as Guardian of Internet Privacy: the Story of Art 16 TFEU* (Berlin 2016), 376 and M. SZYDŁO, *Judicial review of decisions made by national regulatory authorities: Towards a more coherent application of EU sector-specific regulation* (2014) 12 (4) *International Constitutional Law Review*, 932).

Although no rule of recognition exists within the European Union regarding judicial decisions in administrative matters, it should me mentioned that the total or partial invalidity of a Supervisory Authority decision should have consequences in the other member states where it was recognised and eventually applied as a matter of consistency.

[63] Case C-73/16, Puškár, ECJ, 27.9.2017, in which the European Court of Justice did not in principle exclude the possibility for member states to establish mandatory administrative complaints before bringing a legal action, as long as they were not disproportionate and did not constitute an obstacle to the exercise of the right to a judicial remedy guaranteed by Article 47 of the Charter.

public interest and is active in the field of the protection of personal data[64], to lodge a complaint on his or her behalf with a supervisory authority, exercise the right to a judicial remedy on behalf of data subjects or even, if provided for in Member State law, exercise the right to receive compensation on behalf of data subjects (Article 80 and Recital 142).

This is also a leveling rule between Member States that tries to compensate for the usually atomistic and fragmentary nature of complaints (that, linked to the difficulties and costs of litigation, leads to a so far paucity of judicial claims) by allowing for collective actions, with all of the benefits this might bring, according to the law applicable, in terms of gathering of proof, court fees, and the simplification of procedures.

7. Conclusions

The preceding considerations lead us to what we believe to be self-evident: the ease in accessing personal data, mostly in an internet context, has changed traditional notions of applicable law and jurisdiction when in alliance with what are seen as admissible grounds for extending jurisdiction: fundamental rights. Also, it has changed perceptions on the distribution of regulatory authority between states and allowed for the introduction of new and flexible cooperation schemes between them and other public and private entities.

Although we agree that the traditional scheme of redress divided into three layers – data protection remedies sought before the data controller or processor; data protection remedies sought before supervisory authorities and data protection remedies sought before national courts – still needs improvement[65], we adopt the view that the solutions inserted into the GDPR constitute a sound basis for enhancing personal data protection. In fact, they bring tradition and modernity, distance and proximity, public and private closer together and adopt flexible forms of action both at an administrative and at a court level, which is highly desirable in the ubiquitous and pluriform data protection field.

---

[64] It should be noted, however, that Article 80 requirements lead to the conclusion that only entities that are regarded as private not for profit organisations will have the right to represent data subjects for these purposes, not other organisations such as consumer protection or professional related groups.

[65] Cf., among other critics, A. GALETTA-P. DE HERT, *The Proceduralisation of Data Protection Remedies under EU Data Protection Law: Towards a More Effective and Data Subject-oriented Remedial System?* (2015) 8 (1) *Review of European Administrative Law*, 125-151 and M. REQUEJO ISIDRO, *Procedural Harmonization and Private Enforcement in the Area of Personal Data Protection* (2019) 3 *Max Planck Institute Luxembourg for Procedural Law Research Paper Series* available at https://ssrn.com/abstract=3339180.

GDPR AND CHILDREN RIGHTS IN EU DATA PROTECTION LAW

Federica Persano, University of Bergamo

Abstract:

This work addresses the topic of the protection of digital personal data of minors, with particular reference to the analysis of art. 8 of the EU Regulation 2016/679 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, or GDPR*)* and to the effectiveness of consent as a tool to protect the best interest of the child. both in the case in which the consent to the processing of data is given directly by the minor, and in the case in which it is the authorization by the holder of parental responsibility.

Keywords: Privacy, Minors, Digital Data Protection

1. Introduction

Internet access through mobiles, tablets, smartphones and so on has brought to a digital revolution and to the creation of a "virtual community" where classical international and internal law rules are difficult to apply (and, between those, rules concerning legal capacity and consent).

In the EU everyone has the chance to attend the web and at the same time, according to art. 8 of the EU Charter of fundamental rights and to art. 16, par. 1, of the Treaty on the Functioning of the European Union (TFUE), has the right to the protection of personal data concerning him or her.

At the same time, the right to the protection of personal data is not absolute;

it must be considered in relation to its function in society and balanced against other fundamental rights like freedom of expression, thought, association, participation in the life of relationship and in the construction of the community in which people live [1].

The effort to achieve this balance is enriched by additional elements of reflection, considering that the fact of using social networks happens without distinction between adults and minors [2].

According to the UNICEF Annual Report of December 2017 one in three network users is a minor: children are the most connected age group.

So actually, the minor is no more simply a consumer and a recipient of products and services, but is a buyer, a contractor and a user who takes decisions on its own.

It would be anachronistic not to allow children to access electronic communication as it is a right for the minor to maintain social relations and recognize themselves as an active part of society. And the problem therefore is: until which point is fair for them to enjoy this digital freedom?

In regard to it, it's relevant the initial study of the European Commission in the context of the *Better Internet for Children Strategy* [COM (2012) 196 (final)].

The specific aspects of the protection of children's data and of the risks as-

---

[1] G. ALPA, *Privacy statuto dell'informazione,* in *Riv. dir. civ.,* 1, 1979, 65 ff.; ID., *I contratti del minore, appunti di diritto comparato,* in *Contratti*, 2004, 517; A. BONFANTI, *Il diritto alla protezione dei dati personali come riconosciuto dal Patto internazionale sui diritti civili e politici dall'art. 8 della Convenzione europea dei diritti dell'uomo: similitudini e difformità dei contenuti*, in *Dir. um. Dir. Int.*, 5 (3), 2011, 437; E. BUSS, *What the law should (and should not) learn from child development research* (2009) 38 (13) *Hodstra L. Rev.*, 210; C. CAMARDI, *L'eredità digitale. Tra reale e virtuale*, in *Dir. inf.*, 1, 2018, 65; M. CARTA, *Diritto alla vita privata ed internet nell'esperienza giuridica europea ed internazionale*, in *Dir. inf.*, 1, 2014, 1 ff.; M. DI STEFANO (eds.), *La protezione dei dati personali ed informatici nell'era della sorveglianza globale* (Napoli 2017); A. TERRASI, *La protezione dei dati personali tra diritto internazionale e diritto dell'Unione europea* (Torino 2008), 125; F. PANUCCIO DATTOLA, *Minori ed internet* (Torino 2009); A. TERRASI, *La protezione dei dati personali tra diritto internazionale e diritto dell'Unione europea* (Torino 2008), 125; L. TOMASI, *Commetario all'art. 8*, in S. BARTOLE, P. DE SENA, V. ZAGREBELSKY (eds.), *Commentario alla Convezione europea dei diritti dell'uomo* (Padova 2012), 316; S. RODOTÀ, *Il mondo nella rete, Quali i diritti quali i vincoli* (Roma 2014); B. VAN DER SLOOT, *Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"* (2015) *Utrecht Journal of International and European Law*, 28.

[2] G. CAPILLI, *La tutela dei dati personali dei minori*, in ROCCO PANETTA (eds.) *Circolazione e protezione dei dati personali, tra libertà e regole del mercato, Commentario al Regolamento Ue n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003* (Milano 2019), 247 ff.; M. MACENAITE-L. KOSTA, *Consent for processing children's personal data in the EU; following in US footsteps*, *Information and Communication Technology Law* (2017) 26 (2) 146; F. PANUCCIO DATTOLA, *Minori ed internet* (Torino 2009).

sociated with the dissemination of personal data have been specific object of attention by the EU in the context of the multiannual program for the protection of children using the Internet and other technologies. of communication (*Safer Internet Program*) [COM (2016) – 364 final], which highlights the dangers of communication in a digital environment at the expense of people with a consciousness/ability to understand reality that has not yet been fully trained.

No doubt that children are easily influenced by behavioral advertising: several studies have found that marketing practices through social media, online games and mobile applications have a clear impact on their behavior.

For example, in online games profiling can be used to identify the players most likely to spend or to provide personalized announcements that do not correspond to a maturity on the part of the child in recognizing the commercial reason for a marketing practice. Not only: the relevance of the provisions we are dealing with can be better understood also if we consider that very often the illicit treatment of personal digital data is at the origin of the main dangerous situations present on the web such as, for example, child pornography, cyberbullying, ludopathy. But we can also think to the risks connected with the use of interactive games, like the well-known case of the Cayla doll.

Finally. in some cases, the uncontrolled use of the network can even lead to the occurrence of risks for the physical safety of minors (as in the Blue Whale case).

2. The processing of child's personal data in the GDPR

The General Data Protection Regulation (or GDPR) came into force on May 25, 2018 and was designed to modernise laws protection of personal information regarding individuals.

Among the main novelties, the GDPR is the first European law act that regulates the consent of the minor to the processing of personal data, stating, at Recital 38, first phrase, that children deserve specific protection with regard to their personal data, as they may be less aware of the risks, of the consequences and of the safeguards concerned, as well as their rights in relation to the processing of personal data.

The EU discipline has been inspired by the US Children's Online Privacy Protection Act of 1999 (or COPPA), which was enacted in 1998 to protect the privacy of children under the age of 13. COPPA is a US federal law and it first became effective on April 21st, 2000, with other new changes becoming effective on July 1st, 2013.

COPPA is applicable to US businesses, but it can apply to any foreign business which collects personal information from children under 13 residing in the United States.

This Act provides for a more complex and detailed regulation of the topic of the consent than the GDPR, dealing not only with the age of digital consent (set at 13 years), but also with a long list of methods to verify the identity of the parent in giving the consent, the obligation of the "owner" to adopt security measures and the ban on soliciting data that are not necessary for processing

According to COPPA, if you have a website that collects data from kids under 13 the requirements for the lawfulness of the consent are to: *i*) have an extensive Privacy Policy that explains what is being collected, why it is being collected and with whom; *ii*) provide direct notice to parents about your collection and use of children under 13 personal information; *iii*) get a parent verifiable consent before you start collecting information (optionally, you can use the "email plus" method of getting the consent if you collect minimum information from minors and for internal use only) – and you must disclose this in your Privacy Policy –; *iv*) include a parents' right section where parents can find instruction on their rights over their children collected data, how they can contact you to delete or refuse your collection and use of data.

As we are going to illustrate, the GDPR is less stringent and detailed in its content than the COPPA Law.

3. The protection of child's personal data

Art. 8 GDPR deals with the topic of "*Conditions applicable to child's consent in relation to information society services*".

Let us therefore examine the scope of this provision, which, as we are going to illustrate, does not necessarily lead to a different classification of the *privacy* consent on a general level.

Indeed art. 8, par. 1 states: "*where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child*".

This means that the provision does not concern any online processing of data referring to minors, nor any Information Society Service (or ISS) to which minors can access, but rather applies only: *i*) to the ISS services to direct offer and; *ii*) whose legitimate treatment is based on the consent of the interested party (the minor or the holder of parental responsibility, depending on the age of the child).

First of all, the basic definition of an ISS is in art. 1, par. 1, lett. *b*), of Directive (EU) 2015/1535, referred to in art. 4, par 1, (25) GDPR and includes

websites, apps, search engines, online marketplaces and online content services such as on-demand music, gaming and video services and downloads. It does not apply to traditional television or radio transmissions that are provided via general broadcast rather than at the request of an individual.

If an ISS is presented through an intermediary, such as a school for example, then it is not offered 'directly' to a child; only ISS which explicitly states that it is for children, or has children of any age as its target audience is clearly related directly to them.

Also an ISS is offered directly to a child when it is made available to all users without any age restrictions or when any age restrictions in place allow users under the age of 18.

The only exception is the case in which an Information Society Service provider clarifies to potential users that the service is offered exclusively to people aged at least 18, and this is not denied from other elements (such as site content or marketing plans); in those circumstances the service will not be deemed to be provided directly to a minor and art. 8 GDPR will not apply.

Secondly, art. 8 applies only when the legal basis of the processing of personal data is the consent of the interested party *ex* art. 6, par.1, lett. *a*) GDPR.

The definition of consent is in art. 4 (11) GDPR, according to which "*consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*".

Pursuant to art. 8, par. 1, first phrase, the consent is validly provided: *i*) by the minor, if he or she is at least 16 years old; or *ii*) where the minor is under the age of 16 years, such processing should be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility.

This with the derogation provided in Recital 38, last phrase, according to which "*the consent of the holder of parental responsibility is not required in the context of prevention or counseling services offered directly to the child*"; here the reference is to services for the protection of minors such as those provided for cyber bullying or in general for child support (like for example, in the Italian case, of the Telefono Azzurro).

Thirdly, with specific reference to the requirement of informed consent, it must be emphasized that according to the GDPR special protection for minors requires transparency measures specific for them.

The data controller is required to guarantee the right to transparency in data processing for both minors and adults: indeed, children, like any other interested party, do not lose their rights to transparency simply because the consent was given/authorized by the holder of parental responsibility.

The communication methods (simplification, clarity, conciseness, exhaust-

iveness, simplicity, etc.) are supposed to be functional by the legislator with the aim of making the consent given by the minor significant, in a so-called perspective. of "cognitive empowerment of the child".

In this perspective, art. 12, par. 1, GDPR supported by Recital 58, establishes that the data controller who turns to minors or knows that his goods or services are mainly used by minors is required to provide them with any information and communication regarding the processing of their personal data in simple and clear language, so that a child can easily understand what will be done with his data (for example by comic/vignette or cartoon-like information and so on).

4. The consent to the processing of child's personal data

As illustrated in the previous paragraph, the general rule is that the processing of personal data of a child will be lawful where the minor giving the consent is at least 16 years old*;* but according to art. 8, par. 1, second phrase, this rule is flexible, as "*member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years*".

The general rule is therefore subject to the possibility for Member States to waive the limit up to 13 years; consequently, by adopting specific national legislation each of them can set a different age limit than 16 years.

The Italian legislator has set the age limit to be applied in 14 years, with Legislative Decree n. 101/2018, which art. 2-*quinquies* establishes that in implementation of art. 8, par. 1, GDPR, the minor who has reached the age of 14 can express his or her consent to the processing of hpersonal data in relation to the direct offer of services of the Information Society; with regard to these services, the processing of personal data of the minor under the age of 14 is lawful only if provided by the person exercising parental responsibility.

To many it has appeared an opportune choice because it conforms itself with rules concerning consent related to other disciplines (see Law n. 184/1983 on adoption and Law n. 71/2017 on cyberbullying).

Other countries also have used the derogation provided in art. 8, par. 1, second phrase, GDPR: *i*) Croatia, Germany, Lithuania, Luxembourg, Malta, the Netherlands, Romania, Slovakia, Hungary - 16 years; *ii*) Greece, Czech Republic, Slovenia, France – 15 years –; *iii)* Austria, Bulgaria, Cyprus, Lithuania – 14 years –; *iv*) Belgium, UK, Spain, Sweden, England, Denmark, Estonia, Latvia, Finland, Poland, Portugal; 13 years old.

Therefore, to check if the child's consent has been validly given, if the holder of the treatment provides a cross border service, he will have to keep in mind the derogation provided into art. 8 as it will be not possible to simply refer to

the law of the State in which the company is established.

For example, since the GDPR is also applicable to companies holders of the treatment not established in the EU who process data of European citizens, to overcome any possible complication an over the top like WhatsApp has chosen to allow the service in Europe only to those over 16 years old (in third countries the minimum age required for the consent is 13 years).

5. The methods to verify the legitimacy of the consent in the GDPR

Art. 8, par. 2, GDPR establishes that "*the controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology*".

Therefore, if the minor claims to have reached the age of digital consent, the data controller will have to make every reasonable effort to verify the truthfulness of the declaration.

If the child is younger than the age for the digital consent, art. 8, par. 2, GDPR establishes that it is up to the company that offers its services on the basis of consent to work to verify that it has been actually provided or authorized by the holder of parental responsibility.

With specific reference to the methods of verifying the consent of the holder of responsibility, it should also be stressed that, unlike the provisions of the relevant US legislation, the GDPR does not provide practical ways to collect it.

Art. 7, par. 1, GDPR only states: "*where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data*". So it's up to the controller to decide whether it is sufficient to verify the parental responsibility by e-mail or it may be necessary to request further evidence to prove consent. Consequently, it is up to the information society to put in place reasonable measures to ensure that the consent is given or authorized by the parent.

By way of example, in Italy the owner who wants to make sure that underage customers subscribe to services exclusively with the consent of their parents or guardians can ask the user if he/she is than 14 years old.

If you say you are 14 years or older, the data controller must carry out appropriate checks to verify the age; if the user, on the contrary, declares to be under the age of 14, the data controller can accept this declaration without further verification.

The service will inform you of the need for a parent (or guardian) to consent or authorize the processing before the service is provided and will then be asked

for a parent's email address; the service will contact the parent to obtain the consent to the processing by e-mail.

Having reached the age of 14, the minor can give consent to the processing of personal data and re-enter in full control of his treatment and can consequently confirm, modify or revoke the consent given or authorized by the holder of parental responsibility. In the case of inactivity of the child, the consent given or authorized by the parent will continue to be a valid prerequisite for treatment. In this regard, in compliance with the principles of correctness and responsibility, the data controller must inform the minor of this possibility.

About sanctions, pursuant to art. 83, par. 4, lett. a) "*general conditions for imposing administrative fines*", states that infringements of art. 8 "*shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher*".

6. The different juridical regimes of the consent to the processing of personal data and of the consent concerning contracts in relation to a child

Finally, art. 8, par. 3, GDPR establishes that rules concerning the consent to the processing of child's personal data *"shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child".*

It expressly introduces a distinction between the protection of personal data and the consent concerning contracts, establishing that the object of art. 8 is limited to the conditions of lawfulness of consent for the purpose of data processing and does not affect the validity of the contract.

Therefore, by way of example, if a minor buys smartphone ringtones online, data collection (name, surname, e-mail address, payment details) it will be necessary for the execution of a contract and therefore the processing of data will be lawful pursuant to art. 6, par. 1, lett. *b*), GDPR according to which in this case 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*".

If, on the other hand, the owner intends to use the e-mail address of the child also for sending newsletters, it will be necessary to collect his or her consent as the processing of personal data for marketing.

Consequently, the requirements for the validity of consent to the use of data relating to minors fall within a legal framework to be considered distinct from national contract law.

Therefore, two different legal regimes can apply simultaneously, but it does not mean that they coincide.

A consent could be lawfully given for personal data treatment but not for the validity of a contract (concluded by the minor), or a contract could be valid because it complies with the normal needs of personality development (of a child) but the processing of data pursuant to art. 8, par. 3, could be illegal.

However, the application of art. 8 GDPR is excluded if the processing is lawful pursuant to art. 6, letter *b*), when personal data treatment is "necessary" for the services deducted in a contract which the minor can conclude on his own.

7. The profiling of child's personal data

According to Recital 38, second phrase, specific protection of children should apply in particular to the use of personal data "*for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child*".

Minors are vulnerable: data controllers should refrain from profiling them for marketing purposes as they are beyond the reach of a child's understanding and therefore lawful treatment.

However, at the same time, art. 6, par. 1, lett. *a*) GDPR states that data processing shall be lawful if and to the extent that the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

This article, read in conjunction with art. 22, par. 2, GDPR legitimizes the automated decisions, including the profiling, when this decision is based on the data subject's explicit consent otherwise prohibited pursuant to art. 22, par. 1, according to which "*the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her*".

Art. 22 does not distinguish whether the data treatment concerns adults or minors, while Recital 71 GDPR just states that decisions based solely on automated processing, including profiling, "*should not concern minor*".

So, on one side, those provisions don't represent an absolute prohibition of this type of treatments in relation to minors: also because there are certain circumstances in which it is necessary for the controller to make decisions based solely on automated processing, including profiling, having legal effects or similarly significant in relation to minors, for example to protect their well-being.

In this case, the processing should be carried out based on the exceptions referred to in art. 22, paragraph 2, as appropriate.

On the other side, even if doesn't exist an absolute prohibition of profiling, the data controller should provide effective guarantees in protecting the rights, freedoms and legitimate interests of the children whose data are processed.

In this perspective, art. 6, par. 1, lett. *f*) GDPR makes explicit reference to children in providing that processing is lawful where it "*is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child*" .

In this perspective the most suitable regulatory solution is that of codes of conduct.

Art. 40, par. 2, lett. *g*), GDPR states that: "*the associations and other bodies representing the categories of data* controllers or processors *can process the codes of conduct, modify them or extend them, in order to specify the application of this regulation, for example in relation to: (...) g) the information provided and the protection of the child and the manner in which the consent of the holders of parental responsibility is obtained on the child*".

Compliance with a code of conduct is a very important element in order to specify the way of application of the GDPR and the information to disclose to protect the minor's personal data.

8. Conclusions

Regarding the protection of digital personal data, as highlighted, the minor requires to be particularly protected from an exposure or overexposure of data for the possible risks on the development of the personality, for the extensive tracing of the person (profiling) during the course of the whole life, for the theft of data or identity, which if related to him can have more serious repercussions.

The GDPR shows that the protection of the privacy of the minor must be understood as: *i*) "data minimization" related to him (art. 5, par. 1, lett. *c*); *ii*) limit to the legitimate interest of the data controller (art. 6, par.1, lett. *f*); *iii*) restriction on use for marketing purposes or creation of user profiles but in general for any collection of data relating to minors (Recital. 38); *iv*) in connection with the "informed consent" (Recital. 58).

With specific regard to the issue of methods for verifying the consent of the minor or of the holder of parental responsibility, as highlighted in paragraph 4 of this work, this is a weak point of the GDPR.

Also because the problem of anonymity on the web or of the anonymous or pseudo-anonymous use of it by the minor represents the main (real) risk to be faced before evaluating each discipline on the child's access to the internet.

In this context, as underlined, art. 8 GDPR does not expressly require verification of the age of the minor and, unlike US legislation, only roughly addresses the problem of identifying the holder of parental responsibility, leaving to the data controller the task to identify the most suitable criteria compatibly with available technologies.

In the perspective described, an indirect advantage that is usually attributed to the lowering of the age of digital consent is that of an increased responsibility for platforms, broadcasters and producers of content intended for minors, which should therefore be brought to pay more attention to what has been put into circulation (especially on platforms), or to put in place technical measures aimed at limiting access by minors. Even if, from this point of view, the content discipline is very diversified, due to the different age limits introduced by the States according to art. 8 GDPR.

And it is also possible, due to the presence of US players in the EU, that, on one hand, the verification methods will be determined and based on the available technologies and on competitive mechanisms, which could be substantially compliant with US law and therefore could result more effective. And, on the other hand, the lack of specific provision in the GDPR prescription of more detailed rules could be overcome through soft law tools, like the codes of conduct referred to in the second paragraph of this work.

This although the adoption of the codes of conduct is optional and on a voluntary basis and consequently in the event of non-adoption it will not be possible to activate any action against the data controller for violation of the rules of conduct.

The way of co-regulation seems much more promising, implemented through the enforced self-regulation scheme, according to which the codes of conduct are elaborated through negotiations with the industry made therein to protect minors from part of the owners and managers of the treatment are made binding by regulatory decision. In this case sanctioning powers are attributed to the supervisory authority (for example, to the Agcom, or to the Guarantor for the protection of personal data or to the Committee referred to in art. 68 GDPR).

All this without forgetting that another crucial node is represented by the implementing of increasingly intelligent navigation technologies, which should be accompanied by a process of development of an adequate "digital culture", to allow adults and minors to increase their knowledge of the dangers of the network so that they can self-determine and freely express their potential.

PATIENTS AND PRIVACY: GDPR COMPLIANCE FOR HEALTHCARE ORGANIZATIONS

Massimo Foglia, University of Bergamo

Abstract:

After the entry into force of the GDPR, the change in the regulatory framework also affected the health profession, since the entire set of rules on data processing, including data concerning health, was amended. This paper argues that the purpose of the personal data protection legislation is not the mere defence of the personal data, but the protection of the most inner dimension and dignity of the natural person. It is from this point of view that any provision with respect to the protection of personal data, including data concerning health, should be read.

Keywords: privacy, patient, healthcare organization.

1. Introduction

After the entry into force of the GDPR, the change in the regulatory framework also affected the health profession, since the entire set of rules on data processing, including data concerning health, was amended [1]. I have divided my presentation in three parts. In the first part I am going to focus on the definition of personal data concerning health within the Italian regulatory framework after the entry into force of the GDPR. In the second part I am going to point out some features of data processing based on the data subject's consent. Finally, I

[1] See also S. SELLETTI-A. SCALIA, *L'impatto della nuova normativa "privacy" sugli studi clinici,* in *Rass. dir. farm. e salute*, 2018, 1009-1014; A. E. MATARAZZO, *Nuovo regolamento UE in materia trattamento dati personali dei lavoratori ed i rapporti con il codice della privacy*, in *Stato civ. it.*, 2016, 66-69.

am going to focus on the role of the Data Protection Officer (DPO) in healthcare organizations.

2. Processing of personal data concerning health

The Italian legislation on personal data protection is based on the Legislative Decree No. 196 of 30 June 2003, which is the so-called "Privacy Code". The Privacy Code was then amended by the Legislative Decree No. 101 of 10 August 2018 in order to comply with the GDPR provisions [2].

It should be noted that no specific definition of "personal data concerning health" existed before the entry into force of the GDPR. A broad definition was laid down in the Italian Privacy Code, which provided for a general category of "sensitive data" [3] including those defined as "data revealing state of health" [4].

On the contrary, the GDPR does not define "sensitive data" (as the Italian legislator did in the past) as it was replaced with "special categories of personal data" according to art. 9 GDPR, which should be subject to specific measures so as to prevent significant violation of the rights and fundamental freedoms of natural persons.

In particular, art. 4 of the GDPR defines "data concerning health" [5] as «personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status».

Furthermore, the Recital No. 35 specifies «Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health

---

[2] See V. CUFFARO-R. D'ORAZIO-V. RICCIUTO, *I dati personali nel diritto europeo* (Torino 2019); E. TOSI, *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy* (Milano 2019); V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali*, in *Contr. e impr.*, 2018, 1098 ss.; ID., *Quel che resta di un codice: il D.Lgs. 10 agosto 2018, n. 101 detta le disposizioni di adeguamento del codice della privacy al regolamento sulla protezione dei dati*, in *Corr. giur.*, 2018, 1181 ff.

[3] On the concept of "sensitive data" see F. PIRAINO, *Il contrasto sulla nozione di dato sensibile, sui presupposti e sulle modalità del trattamento*, in *Nuova giur. civ. comm*., 2017, 1232-1240.

[4] See S. CORSO, *Sul trattamento dei dati relativi alla salute in ambito sanitario: l'intervento del Garante per la protezione dei dati personali,* in *Resp. medica*, 2019, 225 ff.; P. GUARDA, *I dati sanitari*, in *I dati personali nel diritto europeo* (Torino 2019) 591 ff.; A. PALMA ORTIGOSA-S. LORENZO CABRERA, *Data in the Healthcare sector* (2019) 2 *European Journal of Privacy Law and Technologies*, 16 ff.

[5] See T. MULDER, *The Protection of Data Concerning Health in Europe* (2019) *European Data Protection Law Review*, 209 ff.

status of the data subject. This includes information […] deriving from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test».

It is worth mentioning that "Data concerning health" are distinguished from "genetic data" [6] and "biometric data" [7] by the GDPR. Genetic data can be considered a specification of health data.

According to Recital no 34: Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.

On the other hand, pursuant to Recital no 14 and no 51: biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Now, as a general rule, the processing of special categories of personal data, including data concerning health, is prohibited according to art. 9 GDPR, with a few exceptions, as I will mention.

The point is that several doubts have arisen on the interpretation of this set of new rules on the processing of data concerning health. Hence, the Italian Data Protection Authority has intervened to provide some guidelines on the application of such rules in the healthcare field with the General Application Order No. 55 of 7 March 2019 [8].

Thus, the Italian Authority has clarified the processing of data concerning health is prohibited with the exception of:

a) reasons of substantial public interest, on the basis of Union or Member State law;

---

[6] On genetic data see L. CALIFANO, *Il trattamento dei dati genetici: finalità di ricerca, esigenze di sicurezza e diritto alla protezione dei dati personali*, in *Cultura giuridica e diritto vivente*, 2017, 13 ff.; R. PACIA, *Campione biologico e consenso informato nella ricerca genetica: il possibile ruolo delle biobanche,* in *Jus civile*, 2014, 40 ff.

[7] On biometric data see F. FONTANAROSA, *Dati biometrici e tutela della "privacy" tra divergenze giuridiche ed esigenze di unificazione*, in *Ann. dir. comp.,* 2019, 807-844.

[8] M. PANEBIANCO, *Il trattamento dei dati nel Sistema Sanitario Nazionale italiano alla luce del Provvedimento del Garante del 7 marzo 2019*, in *Cib. dir.*, 2019, 241-269.

b) reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices (for example health emergencies due to earthquakes or food safety);

c) purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services undertaken by (or under the responsibility of) a health professional subject to professional secrecy or by other person also subject to an obligation of secrecy».

In particular, with regards to the case at let. g) par. 2 art. 9, legal scholars have pointed out that its wording may be too vague and extensive, given that the concept of substantial public interest is deferred to Member States. This might cause abuses and incoherent interpretations, in contrast with the idea of jurisdictions' harmonisation [9].

Furthermore, in relation to the exception at let. h) of the same paragraph, case that can be defined as "health-related purposes" (*finalità di cura*), the Italian Authority observes that - and this is probably the crucial point in the General Application Order - that now, differently from the past, it is no longer compulsory that the physician, subject to professional secrecy, asks for the patient's consent for the processing of data related to the medical treatment, irrespective of the fact that the physician is affiliated to a medical institution.

On the other hand, the Italian Authority made it very clear that processing of personal date not strictly related to the medical treatment requires the data subject's consent. For instance:

a. data processing related to the use of medical App;

b. data processing designed to increase customer's loyalty;

c. data processing in health field undertaken by private entities for promotional or commercial purposes;

d. processing undertaken by health professionals for commercial or voting purposes;

e. processing undertaken through the Electronic Health Record.

In order to add information to the Electronic Health Record, existing provision in the field of health require the data subject's consent (cf. art. 75 Italian Privacy Code) [10]. Nevertheless, in the light of the new regulatory framework,

---

[9] M. Granieri, *Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679*, in *Nuove leggi civ.*, 2017, 165-190; A. Busacca, *Le "categorie particolari di dati" ex art. 9 GDPR. Divieti, eccezioni e limiti alle attività di trattamento*, in *Ordine Internazionale e Diritti Umani*, 2018, 19.

[10] On Electronic Health Record see V. Peigné, *Il fascicolo sanitario elettronico, verso una*

the Italian Authority suggested a possible amendment removing the consent requirement for processing personal health information through the Electronic Health Record. On the other hand, such a solution is considered as dangerous and risky for the security of health information processed beyond the data subject's control.

As far as online medical report is concerned, the Italian Authority made it clear that the current legislation requires the data subject's consent in respect of the delivery of the medical report.

Among the data subject's rights laid down in the GDPR it is useful to mention the right of access which allows the data subject to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data (art. 15 GDPR).

Furthermore, a strong emphasis was placed on the right to erasure (also called 'right to be forgotten')[11]. According to art. 17, par. 1, GDPR, the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay. This rule sets out a substantial right of informational self-determination. Hence, the right to erasure has to be guaranteed not only whereas the personal data have been unlawfully processed, but also in the case of lawful and fair processing.

At the same time, according to Art. 12 GDPR, any communication relating to processing to the data subject should be made in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child[12].

"trasparenza sanitaria" della persona, in *Riv. it. med. leg.*, 2011, 1519-1547; P. GUARDA-R. DUCATO, *Profili giuridici dei "Personal Health Records": l'autogestione dei dati sanitari da parte del paziente tra "privacy" e tutela della salute,* in *Riv. crit. dir. priv.,* 2014, 389-419; E. STEFANINI, *Telemedicina, "mHealth" e diritto*, in *Rass. dir. farm*., 2016, 1023-1032.

[11] On the right to be forgotten V. CUFFARO, *Una decisione assennata sul diritto all'oblio*, in *Corr. giur.,* 2019, 1195-1197; R. SENIGAGLIA, *Reg. UE 2016/679 e diritto all'oblio nella comunicazione telematica. Identità, informazione e trasparenza nell'ordine della dignità personale*, in *Nuove leg. civ. comm*., 2017, 1023 ff.; A. THIENE, *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo regolamento europeo*, in *Nuove leg. civ. comm.*, 2017, 442; S. BONAVITA, R. PARDOLESI, *GDPR e diritto alla cancellazione (oblio)*, in *Danno e resp.*, 2018, 269-281; F. SCIA, *Riservatezza e oblio: diritti dei minori e servizi della società dell'informazione* (2019) 2 *European Journal of Privacy Law and Technologies*, 16 ff.

[12] I. A. CAGGIANO, *"Privacy" e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione*, in *Familia*, 2018, 3-23; A. ASTONE, *I dati personali dei minori in rete. Dall'internet delle persone e all'internet delle cose* (Milano 2019); R. SENIGAGLIA, *Autodeterminazione e minore età. Itinerari di diritto minorile* (Pisa 2019).

One of the most important novelties introduced by the GDPR concerns the role of the Data Protection Officer (DPO) [13].

As is known, the DPO performs a supervisory role in keeping the control over the compliance with regulations on privacy.

As a general rule, either public or private medical institutions must appoint a DPO [14]. With respect to public institution given that the processing is carried out by a public authority or body (art. 37, par. 1, let. a), whilst as far as private institutions are concerned as the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 GDPR (art. 37, par. 1, let. c).

On the other hand, physicians practicing their professional activity outside a medical institution are not obliged to designate a DPO pursuant to Recital 91 GDPR according to which: "The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory".

With particular reference to the so-called E-Health, it is worth mentioning the function of the Data protection impact assessment [15]. According to Article 35 GDPR, «Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the pro-

---

[13] M.C. GAETA, *Hard law and soft law on data protection: what a DPO should know to better perform his or her tasks* (2019) 2 *European Journal of Privacy Law and Technologies*, 61 ff.; S. ANGELETTI, *Data Protection Officer: una nuova professione nelle amministrazioni pubbliche?*, in *RU Risorse umane nella pubblica amministrazione*, 2019, 32-43; S. LINGUANTI, *La figura del DPO/RPD nel regolamento UE 2016/679 in tema di privacy*, in *Disc. comm.*, 2018, 59-62; F. LORÈ, *Il ruolo del Responsabile della protezione dei dati personali nella pubblica amministrazione alla luce del Regolamento generale sulla protezione dei dati personali UE 2016/679*, in *Amministrativamente*, 2018, 22; A. TORTORA, *Il nuovo regolamento europeo per la protezione dei dati (GDPR) e la figura del "Data Protection Officer" (DPO): incidenza sulla attività della pubblica amministrazione,* in *Amministrativamente*, 2018, 19; M. RECIO, *Practitioner's Corner Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability* (2017) *European Data Protection Law Review,* 114-118.

[14] G. PEDRAZZI, *Il ruolo del responsabile della protezione dei dati (dpo) nel settore sanitario*, in *Riv. it. med. leg.,* 2019, 179 ff.

[15] See F. CIRILLO, *The Impact of e-Health on Privacy and Fundamental Rights: From Confidentiality to Data Protection Regulation* (2019) 2 *European Journal of Privacy Law and Technologies*, 95 ff.; V. HORDERN, *The final GDPR text and what it will mean for health data* (2016) *eHealth Law & Policy*, 3-5; L. WILLIATTE-PELLITTERI, *New Technologies, Telemedicine, eHealth, Data...What Are You Talking About? The Lawyer's Point of View*, A. ANDRÉ (eds.), *Digital Medicine, Springer, Cham* (Berlin 2019), 93; N. CORTEZ, *The Evolving Law and Ethics of Digital Health*, H. RIVAS-K. WAC (eds.), *Digital Health Scaling Healthcare to the World, Springer* (Berlin 2018), 249.

cessing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data […]»

On this issue, it might be useful to report a recent decision of the Portuguese Authority (*Comissão Nacional de Protecção de Dados*), which imposed a penalty of four hundred thousand euros on a hospital with CNPD 984/2018 resolution (9932/2018 procedure).

The case was about the failure to define the criteria for access to the healthcare information system called SONHO, a patient management system launched by the Portuguese Ministry of Health.

Basically, the same access to patient data was assigned to physicians as well as technical-administrative staff. This is a clear infringement of the principle of "data minimisation", according to which processing of personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which personal data are processed.

The controller and the processor have the duty to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including the ability to ensure the ongoing confidentiality, integrity and availability of personal data. Therefore, such a violation should have been detected by the DPO.

3. Conclusion

I have tried to point out some of the many fulfilments required to health professionals and especially to health institutions in the perspective of the GDPR compliance.

As I said, the Italian Data Protection Authority argues that patient's consent is no longer necessary for data processing in the case of health-related purposes.

However, it should be borne in mind that the contractual party's consent (on which the health assistance contract is based) does not amount to data subject's consent to data processing [16]. They have different content and purposes.

[16] See G. RESTA-V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi di rete*, in *Riv. trim. dir. proc. civ*., 2018, 411 ff.; V. CUFFARO, *Il consenso dell'interessato*, in V. CUFFARO - V. RICCIUTO (a cura di), *La disciplina del trattamento dei dati personali* (Torino 1997), 221; S. PATTI, *Il consenso dell'interessato al trattamento dei dati personali*, in *Riv. dir. civ*., 1999, 455 ff.; P. MANES, *Il consenso al trattamento dei dati personali* (Padova 2001) 81 ff.; L. GATT-R. MONTANARI-I.A. CAGGIANO, *Consenso al trattamento dei dati personali e analisi giuridico comportamentale. Spunti di una riflessione sull'effettività della tutela dei dati personali*, in *Pol. dir*., 2017, 363 ff.; I.A. CAGGIANO, *Il consenso al trattamento dei dati personali nel nuovo Regolamen-*

Furthermore, it should be pointed out that data concerning health are a peculiar category of data, as they disclose part of the story of the patient's life; they reveal fragments of their identity.

Hence, the purpose of the personal data protection legislation is not the mere defence of the personal data, but the protection of the most inner dimension and dignity of the natural person. It is from this point of view that any provision with respect to the protection of personal data, including data concerning health, should be read.

to europeo. Analisi giuridica e studi comportamentali, in *Osserv. dir. civ. e comm*., 2018, 69 ff.; S. THOBANI, *I requisiti del consenso al trattamento dei dati personali* (Santarcangelo di Romagna 2016); ID., *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento di massa dei dati personali* (Milano 2018), 118 ff.; G. BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione* (Milano 1997) 285; F. CAGGIA, *Il consenso al trattamento dei dati personali nel diritto europeo*, in *Riv. dir. comm.*, 2019, 405-432.

PATIENTS AND PRIVACY: GDPR COMPLIANCE FOR HEALTHCARE ORGANISATIONS IN THE CZECH REPUBLIC *

Martin Šolc, Charles University Faculty of Law

Abstract:

At first sight, 25 May 2018 brought no revolution to Czech health care regarding data protection. The practice of the providers of health services related to medical records has already been aptly regulated by the Act on Health Services of 2011. Nevertheless, GDPR has caused several dilemmas, most importantly in the area of medical research and particularly biobanks. The paper focuses on selected questions related to GDPR compliance in Czech health care and medical research, outlining the answer to the question of what changed with GDPR and what it means to the relevant subjects.

Keyword: General Data Protection Regulation, compliance, health law, data protection in health care, the Czech Republic

1. Introduction

There has been much debate on the practical effects of the General Data Protection Regulation [1] (hereinafter "GDPR") application in many sectors where the

* The paper was written with the support of the Charles University Grant Agency (GAUK) research project no. 910319 *"Legal Paradigm of Medical Research: Civil Liability for Death and Bodily Harm"*.

The author would also like to express his sincere gratitude for the invaluable consultations to Mgr. et Mgr. Anna Nevečeřalová and JUDr. Petr Šustek, Ph.D.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

personal data are processed. One of the more sensitive areas is health care where health-related data (which represent a special category of protected data under GDPR) are processed on a large scale. Nevertheless, it was precisely for this apparent necessity for the protection of patients' privacy that the data processing in health care has already been subjected to a relatively complex regulation before 25 May 2018 when GDPR became fully applicable. As a result, it is not always clear what new changes GDPR requires from Czech health services providers and health professionals. The article identifies the most important of these changes and outlines several problematic areas of data protection both in clinical practice and medical research (primarily related to the functioning of biobanks).

2. Medical records under Czech law

Medical records contain several categories of personal data that are subjected to special protection under Article 9 (1) of GDPR. From their very nature, medical records represent sets of data concerning health. However, they can also encompass genetic or biometric data. In some cases, there might also be present data concerning a person's sex life or sexual orientation. The medical records can also contain data revealing the patient's racial or ethnic origin. This rich mixture of personal data makes medical records extremely sensitive, requiring a high level of protection.

Since the provider of health services is obliged to keep medical records, the processing of the relevant data is necessary for compliance with a legal obligation to which the provider as a controller is subjected (Article 6 (1) (c) of GDRP). However, this sole reason would not suffice to legalise the processing of the above-outlined special categories of personal data. The processing of these data is only allowed since it is necessary for health purposes listed in Article 9 (2) (h), especially for the provision of health care.

2.1. The influence of GDPR on clinical practice

GDPR did not bring about any crucial change for Czech clinical practice. The general principles of data protection have been known to Czech law for many years [2]. Before May 2018, the keeping of medical records had already

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).

[2] See for example J. NAVRÁTIL ET AL., *GDPR pro praxi [GDPR for Practice]* (Plzeň 2018), 66-67.

been regulated by Act No. 372/2011 Coll., on Health Services and Conditions of Their Provision (hereinafter "Act on Health Services") and by Decree No. 98/2012 Coll., on Medical Records. The privacy rights of patients have been adequately protected by these regulations [3]. The area in which GDPR might prove more innovative – and more demanding – for Czech providers of health services is the protection of personal data of their employees. Another change following the applicability of GDPR was the limitation of some of the time periods for which certain types of medical records must be stored [4]. While this move somewhat alleviates the administrative burden borne by the providers of health services, its suitability from the perspective of patients' interests is apparently open for a discussion.

It needs to be noted, though, that the relatively high quality of patients' data protection in Czech national law did not have a very long tradition in the country. On the one hand, medical professionals have always been thinking about the necessity to keep their patient's secrets [5]. In this sense, medicine has been ahead of most of other professions regarding what we now call personal data protection. On the other hand, medical paternalism often led physicians to believe they know the best when, how, and to whom to reveal the information about their patients. In the Czech Republic, the patients' access to their own medical records was uncertain until about 2005. The significant improvement followed the ratification of the Convention on Human Rights and Biomedicine (hereinafter "Convention") in 2001. Article 10 of the Convention sets two basic rights regarding personal data in health care: everyone has the right to respect for private life in relation to information about his or her health as well as the right to know any information collected about his or her health [6]. Even though the minimum standards set by the Convention were considered almost self-evident in Western Europe, they represented a significant challenge for Czech health law of the time.

---

[3] See L. ŠIROKÁ-P. ŠUSTEK, Zdravotnická dokumentace [Medical Records], P. ŠUSTEK-T. HOLČAPEK (eds.), *Zdravotnické právo [Health Law]* (Praha 2016), 162-196.

[4] For example, the required time of storage of medical records in case of long-term inpatient care was limited from 40 to 20 years. Appendix 3 to Decree No. 98/2012 Coll., on Medical Records.

[5] Even the oldest known version of the Hippocratic Oath contains the promise to keep confidentiality: *"And whatsoever I shall see or hear in the course of my profession, as well as outside my profession in my intercourse with men, if it be what should not be published abroad, I will never divulge, holding such things to be holy secrets."* Hippocrates of Cos, *The Oath* (Loeb Classical Library) available at <https://www.loebclassics.com/view/hippocrates_cos-oath/1923/pb_LCL147.299.xml;jsessionid=0D172B139B8933CBD47CC1A575EBB4FE> accessed 10 January 2020.

[6] Nevertheless, the exercise of the latter right may be restricted by the law in the interests of the patient (the so-called therapeutic privilege). See M. ŠOLC, *Therapeutic Privilege as the Last Bastion of Paternalism?* in *Riv. Resp. med.*, 2019, 3, 399-403.

The remaining paternalism – directly inherited from the Socialist law – was still relatively strong and incompatible with the Convention's requirements. Since 1992, the obligation to keep medical records was explicitly imposed by the law, but the regulation only applied to private health care providers. The obligations applicable to all the providers (including the public ones) were set by Act No. 20/1966 Coll., on the Care for the Health of the People that did not explicitly mention medical records until August 2001. Even several years later, there were cases where hospitals attempted to deny the patients access to their own medical records [7]. By the late 2000s, the providers learnt to comply with the new requirements. The Act No. 20/1966 Coll. was replaced by Act on Health Services in 2012 which in its Section 65 guarantees the right to access to medical records to several groups of persons, including the patients themselves, the deceased's patients close persons, or the employees of the provider of health services in a necessary scope for the fulfilment of their duties.

Nevertheless, there are several new obligations that GDPR imposes on the providers in the position of controllers. Since the providers' core activities [8] consist in the processing of a large scale of special categories of data pursuant to Article 9 (see Article 37 (1) (c) of GDPR), they are obliged to designate a data protection officer *(DPO)*. This might prove challenging since the DPO should have a good understanding of both the area of data protection and the provision of health care, often including medical research [9]. It might be one of the reasons for which a provider of health services might choose to designate a team that will fulfil the tasks of DPO – in this case, though, there must still be designated a particular responsible natural person [10].

---

[7] See P. Šustek, *Two Decades of the Convention on Biomedicine: Has It Been Any Good?* (2018) 9 *Czech Yearbook of Public & Private International Law*, 262.

[8] The fact that the processing of personal data is one of the core activities of hospitals is aptly explained by the WP29: "*(...)'core activities' should not be interpreted as excluding activities where the processing of data forms an inextricable part of the controller's or processor's activity. For example, the core activity of a hospital is to provide health care. However, a hospital could not provide healthcare safely and effectively without processing health data, such as patients' health records. Therefore, processing these data should be considered to be one of any hospital's core activities and hospitals must therefore designate DPOs.*" WP29, *Guidelines on Data Protection Officers ('DPOs')* (2016) 7.

[9] See J. Navratil et al. (fn 2), 63, 262-263; M. Nulicek-J. Donát-F. Nonnemann-B. Lichnovský-J. Tomíšek, *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář [GDPR. The General Data Protection Regulation. A Practical Commentary]* (Praha 2017), 339.

[10] See L. Suchánková, *Komentář k čl. 37 [Commentary to Article 37],* J. Pattynová-L. Suchánková-J. Černý et al., *Obecné nařízení o ochraně osobních údajů (GDPR). Data a soukromí v digitálním světe. Komentář [General Data Protection Regulation (GDPR). Data and Privacy in a Digital World. A Commentary]* (Plzeň 2018), 291-292.

For a similar reason – because the providers process on a large scale special categories of data referred to in Article 9 (1) (see Article 35 (3) (b) of GDPR) – they are also obliged to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data *(Data Protection Impact Assessment, DPIA)*. On a general level, the DPIA is only required when the relevant processing operations are "*likely to result in a high risk*" [11]. The seriousness of the risk is assessed by the controller who in case of the serious risk danger also carries out the DPIA. Nevertheless, given the sensitivity of health data as well as the vulnerability of patients as data subjects, the processing of these data will be a typical example of processing requiring the DPIA [12]. While a similar procedure was already known to several European jurisdictions before GDPR (we can recall the *Privacy Impact Assessment* under English or French law), it was not present in Czech law [13]. The obligation to carry out the DPIA, however, only applies to bigger providers. Therefore, most physicians in private practice are exempted from the obligation [14]. This exemption also applies to other individual health professionals or lawyers and arguably other similar professions that have a legal duty of confidentiality, given that they process the data of a limited number of clients [15]. In the Czech Republic, the threshold is seen to be around 5.000 patients the provider has in care, while the average number of patients of a general practitioner is approximately 1.600 [16].

---

[11] See Article 35 (1) and Recital 91 of GDPR.

[12] A hospital processing of its patients' genetic and health data in a hospital information system is explicitly stated as an example of processing likely to require DPIA by the Data Protection Working Party WP29 in WP29, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679* (2017), 11.

[13] See M. NULÍČEK-J. DONÁT-F. NONNEMANN-B. LICHNOVSKÝ-J. TOMÍŠEK (fn 9), 312.

[14] Recital 91 of GDPR: *"The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory."*

[15] See J. ČERNÝ, *Komentář k čl. 35 [Commentary to Article 35],* J. PATTYNOVÁ-L. SUCHÁNKOVÁ-J. ČERNÝ ET AL., *Obecné nařízení o ochraně osobních údajů (GDPR). Data a soukromí v digitálním světe. Komentář [General Data Protection Regulation (GDPR). Data and Privacy in a Digital World. A Commentary]* (Plzeň 2018), 273.

[16] See Appendix 2 to the draft document issued by the national authority data protection authority: Office for Personal Data Protection. "Data Protection Impact Assessment" Draft Version (2018) available at <https://www.uoou.cz/k-povinnosti-provadet-posouzeni-vlivu-na-ochranu-osobnich-udaju-dpia/d-28385> accessed 10 January 2020.

2.2. Problematic areas

The most problematic areas concerning the data protection in clinical practice rather consist in the access to medical records of certain persons other than the patients and the health professionals. For example, a problem arose when the National Contact Point for eHealth [17] was established in summer of 2018 [18]. Initially, the existence of this information system significantly broadened the scope of persons having access to medical records [19]. In spring 2019, this scope was narrowed to the health services providers from other EU states via the respective national contact point. Nevertheless, it might be argued that the regulation is still lacking adequate safeguards.

From a certain perspective, the access of insurance companies to medical records is problematic in the opposite way. Every provider of health services is obliged to have liability insurance [20]. For the purposes of the investigation of a loss event, the insurance company needs to work with the data concerning the injured person's health condition or the cause of her or his death. However, according to Section 2864 of Act No. 89/2012 Coll., the Civil Code (hereinafter "Civil Code"), the insurer is only allowed to ascertain such data if they have been granted consent to do so by the injured person or another person entitled to grant the consent. The same rule applies to access to medical records.

The injured party usually grants the consent – it is in their best interest to ensure that the insurance company will pay their compensation. Nevertheless, if the injured person refuses to grant the consent, the insurance company cannot investigate the case and cover the costs. For the insured provider of health services, this might be a very difficult situation: they have to compensate the injured person from their own sources without hope to have the costs covered by insurance. It is not very fortunate for insurance companies as well since they cannot really promise the insured persons their protection in all cases.

GDPR is of little help in this respect. Article 9 (2) does not provide the insurers with any legal basis for ascertaining health-related data of the injured persons. The only option is to ascertain and process the data for the defence against legal claims (Article 9 (2) (f) of GDPR). However, this is only applica-

[17] In Czech original: *Národní kontaktní místo pro elektronické zdravotnictví*.

[18] From the legislative perspective, it was established by adding the new Section 69a to Act on Health Services.

[19] See J. MACH-A. BURIÁNEK-D. ZÁLESKÁ-M. MÁCA-B. VRÁBLOVÁ, *Zákon o zdravotních službách. Zákon o specifických zdravotních službách. Praktický komentář. [Act on Health Services. And on Specific Health Services. A Practical Commentary]* (Praha 2018) 281-282; J. NAVRÁTIL ET AL. (fn 2) 163.

[20] See Section 45 (2) (n) of Act on Health Services.

ble if the litigation already started and the insurance company joined it as an intervenor. It does not help the insured providers with their uncertainty very much. Furthermore, it excludes the possibility of out of court settlement.

A somewhat related problem is connected to private health insurance. While there is a system of mandatory public health insurance in the Czech Republic, many foreigners are only insured privately. These patients can simply walk away from the health facility without paying, and it is virtually impossible for the provider to enforce the patient's duty to pay for the provided services since they have no legal basis for using the patient's personal data.

3. Medical research and biobanks

The processing of personal data for the purposes of medical research is rather complicated. It is necessary to find out whether there is any legal basis for this processing other than the data subject's consent. Furthermore, we will identify the conditions of further processing for scientific purposes if the data were collected for some other purpose. Then, we will focus on the special legal basis for the processing of health data. Finally, we will briefly analyse the contemporary situation of Czech biobanks.

3.1. Legal basis for the processing of personal data for scientific purposes

If personal data are to be processed without their subject's consent, there arises an important question of whether the medical research is a task carried out in the public interest in the sense of Article 6 (1) (e) of GDPR. If the answer were affirmative, the processing of data would be possible without consent given that it has a basis in Union or Member State law [21]. Nevertheless, this criterion is primarily applicable to public authorities [22]. In the context of health care, GDPR explicitly mentions the processing carried out with the purpose of public health protection or the management of health care services by subjects such as professional associations [23]. It is not clear whether the medical research carried out by research institutions – including the public ones – can reasonably fit into this category. This uncertainty is especially relevant with regard to clinical stud-

[21] See Recital 45 of GDPR.

[22] See M. NULÍČEK-J. DONÁT-F. NONNEMANN-B. LICHNOVSKÝ-J. TOMÍŠEK (fn 9) 130.

[23] Recital 45 of GDPR.

ies of new medicinal products or medical devices that might be understood as a mixture of public and private interest.

Alternatively, it is feasible that the processing for research purposes is necessary for the purposes of the legitimate interests pursued by the controller or by a third party according to Article 6 (1) (f) of GDPR. Under Directive 95/46/EC that was later repealed by GDPR, the Article 29 Working Party (WP29) had come to the conclusion that scientific or research purposes can constitute a legitimate interest [24]. While the legitimate interest is one of the most flexible of the legal grounds for data processing [25], it is not unlimited. It should not apply to the processing by public authorities in the performance of their tasks. In the case of other controllers, the legitimate interest can be given especially if "*there is a relevant and appropriate relationship between the data subject and the controller*" [26]. The practice would need to clarify under what circumstances the relationship between the provider of health services and the patient could be relevant and appropriate for this legal basis to be applied. Furthermore, the legitimate interests criterion always entails a balancing test since the processing is not allowed if the interests of the controller are overridden by the interests or fundamental rights and freedoms of the data subject. This could especially happen "*where personal data are processed in circumstances where data subjects do not reasonably expect further processing*" [27].

Therefore, the processing of personal data for research purposes without consent might be possible as constituting legitimate interest of the controller. However, the research institutions need to be very careful in each case [28]. It is commendable that the processing of personal data in research is based on consent. Even in that case, it remains to be clarified how specific the consent must be.

3.2. Further processing for scientific purposes

Another problem is the further processing of personal data for a purpose other than for which they were collected (see Article 6 (4) of GDPR). We can imagine a situation when the patient consented to the processing of his or her per-

[24] WP29, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (2014), 24-25.

[25] See M. NULÍČEK-J. DONÁT-F. NONNEMANN-B. LICHNOVSKÝ-J. TOMÍŠEK (fn 9) 131.

[26] Recital 47 of GDPR.

[27] *Ibidem*.

[28] See also G. MALDOFF, *How GDPR changes the rules for research?* (19 April 2016) *The International Association of Privacy Professionals* available at <https://iapp.org/news/a/how-gdpr-changes-the-rules-for-research/> accessed 27 January 2020.

sonal data in the context of the provision of health care, but the data are later used in health research. There are two possible legal bases for this processing. The first one is the additional consent granted before the processing of data for the new purpose. The second legal basis is the compatibility of the new and the original purposes. The compatibility shall be ascertained by the controller. They should take into account several aspects, for example, any link between the original and the new purposes, the context of the data collection, the stricter protection of the data pursuant Article 9 of GDPR, the possible consequences of the further processing, or the existence of appropriate safeguards (e.g. pseudonymisation).

Nevertheless, according to Article 5 (1) (b) of GDPR, *"further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes"*. Also, Recital 50 of GDPR states that the *"[f]urther processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations"*. For this reason, further processing for scientific purposes should be legal in most cases even without consent. However, it is still possible that sometimes the difference between the original and the new purpose will be so significant that the purposes will be considered incompatible. The controller should, therefore, carry out the test of compatibility, which is burdensome from the perspective of administrative costs.

3.3. Processing of health data

When health data are concerned, the processing also needs to have a legal basis under Article 9 of GDPR. Explicit consent of the data subject is, of course, one of these legal grounds. Another possibility is to be found in Article 9 (2) (j) on which the processing can be based if it is necessary for, inter alia, scientific research purposes, it is subject to safeguards set by Article 89 (1), and it is based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. This provision in conjunction with Article 6 (1) (f) arguably represents a sufficient legal basis for the processing of health data for scientific purposes without the consent of the data subject.

3.4. Biobanks in the Czech Republic

It is problematic that some of Czech health data registers are not regulated by any law or decree. However, there is also a broader question that threatens to undermine the processing of health data in the research context in the country. Under Czech law, the use of biological material for research purposes does not require the patient's consent if in the course of its use there are not used data that would make it possible to identify the patient or the deceased person (Section 81 (4) (a) of Act on Health Services). This requirement is crucial for biobanks (repositories that process, store, and distribute biospecimens and associated data for the use in research and clinical practice [29]). An important feature of biobanks is their ability to provide samples for a variety of future research purposes as opposed to traditional sample collections which have only been collecting each sample for a specific research need that was defined in advance [30].

Biobanks often provide samples to foreign researchers. The patient is known under a specific code to which the data are connected (clinical information, genetic data, lifestyle data, etc.). It is a usual practice that researchers ask for the information on the development of the patient's condition. This requires that the controller is still able to connect the code with the particular patient.

Anonymisation as a process represents the data processing, but the resulting anonymised data are not considered personal data and therefore are not protected by GDPR or national law. That is because anonymisation is irreversible; once the data are anonymised, the natural person cannot be directly or indirectly identified by the controller or by another person with the use of *"all the means reasonably likely to be used"* [31]. If it is still possible to identify the person by any reasonably foreseeable means, the data were not anonymised. And there is no doubt that as a rule, the data in biobanks can be used to identify the person. Therefore, these data are "merely" pseudonymised and cannot be considered anonymised.

The pseudonymisation of data would not necessarily be a problem if the data could simply be used under the legitimate interests clause (the above-analysed Article 6 (1) (f) of GDPR). From the sole perspective of GDPR, the data collected with the consent as a part of a research biobank can be used by the biobank administrators for other forms of scientific research without additional consent [32].

---

[29] See Y. G. De Souza-J. S. Greenspan, *Biobanking Past, Present and Future: Responsibilities and Benefits* (2013) 27 (3) *AIDS*, 303.

[30] See S. Biopankit, *What is a Biobank?* available at <https://www.biopankki.fi/en/what-is-a-biobank/> accessed 10 January 2020.

[31] Recital 26 of GDPR. See also WP29, *Opinion 05/2014 on Anonymisation Techniques* (2014) 5.

[32] See B.A. Simell-O. M. Törnwall-I. Hämäläinen-H.E. Wichmann-G. Anton-P. Bren-

However, the fact that biobanks contain health material means that the processing must be based on a Member State law as required by Article 9 (2) (j) of GDPR.

Therefore, the crucial question is whether the condition of the impossibility to identify the patient under Czech law means anonymisation or pseudonymisation. If Czech law required anonymisation, most of the activity of biobanks would not be possible since it would not be based on a Member State law. The specific purposes of future sample processing in a biobank cannot be foreseen in the time of the consent. For this reason, the consent can hardly be specific enough to meet the GDPR standard.

If interpreted extensively, anonymisation would not be possible in any human tissue since every tissue contains DNA. This is even more evident given that in their decision making, the controllers should take into account the possible future development of the possibilities of identification of persons [33]. Even the tissue samples that are relatively safe from identification today can be much more easily identified in the future with the development of science and the increasing popularity of commercial DNA testing. We believe that this fact only strengthens the argument for the pseudonymisation interpretation of the above-discussed Czech legal requirement.

4. Conclusion

Following the ratification of the Convention on Human Rights and Biomedicine in 2001, Czech health law made significant progress in securing the protection of patients' privacy. For this reason, GDPR did not bring about much change regarding the keeping of medical records. Nevertheless, it imposed several new obligations on the providers of health services such as the duty to designate a data protection officer or to carry out the data protection impact assessment. Furthermore, there remain several problematic areas, including the regulation of the access of insurance companies to medical records.

Processing of health data without consent for the purposes of medical research can be arguably based on Article 6 (1) (f) (legitimate interests) in conjunction with Article 9 (2) (j) (scientific research) of GDPR. Further processing

---

NAN-L. BOUVARD-N. SLIMANI-A. MOSKAL-M. GUNTER-K. ZATLOUKAL-J.T. MINION-S. SOINI-M.T. MAYRHOFER-M.J. MURTAGH-G.J. VAN OMMEN-M. JOHANSSON-M. PEROLA, *Transnational access to large prospective cohorts in Europe: Current trends and unmet needs* (2019) 49 *New Biotechnology*, 98-103 as cited in European Parliament. Panel for the Future of Science and Technology, "How the General Data Protection Regulation changes the rules for scientific research" available at <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634447/EPRS_STU(2019)634447_EN.pdf> accessed 26 January 2020.

[33] See M. NULÍČEK-J. DONÁT-F. NONNEMANN-B. LICHNOVSKÝ-J. TOMÍŠEK (fn 9) 83-84.

needs to be subjected to the test of compatibility of the original and the new purposes of processing (even though the new purpose should be considered compatible if it consists in scientific research). It is primarily the national law that makes the legality of standard practices of health data processing in biobanks uncertain. According to national law, the patient's consent for the use of biological material for research purposes is not required only if it is not possible to identify the patient from the used data. As a rule, the data in the biobanks are pseudonymised but not anonymised. While the situation is far from clear, we argue for the interpretation of the said legal requirement in the sense of pseudonymisation, so the functioning of biobanks is not threatened.

THE COMPENSATION OF NON-PECUNIARY LOSS IN GDPR INFRINGEMENT CASES

Jonas Knetsch, University of Lyon
(Jean-Monnet-Faculty of Law Saint-Étienne)

Abstract:

Article 82 (1) of the General Data Protection Regulation (GDPR) provides that any 'person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered'. This paper aims to assess to what extent the compensation of 'non-material damage' can be an effective means to ensure legal protection in the field of data protection, despite persistent discrepancies between national civil liability rules.

Keywords: Non-pecuniary loss; compensation; GDPR infringement; assessment of damages

1. Introduction

As of 25 May 2018, the General Data Protection Regulation (GDPR) has replaced all national provisions enacted by the EU member states to transpose the Data Protection Directive 95/46/EC. From this date on, civil liability claims arising from data protection breaches have been given a new legal basis, article 82 (1) providing that any '*person who has suffered material or non-material damage as a result of an infringement of this Regulation*' has a right to receive compensation from the controller or processor for the damage suffered.

With the adoption of the GDPR in April 2016, significant legal research has been conducted on the civil liability issues related to data protection law [1], but

[1] In English, see E. O'DELL, *Compensation for Breach of the General Data Protection Regula-*

less attention has been given to the compensation of non-pecuniary loss in GDPR infringement cases. The reference to 'non-material damage' in article 82 (1) GDPR ties in with the current trend in several European jurisdictions to more and more broadly award monetary compensation for non-pecuniary loss [2].

2. The compensation of non-pecuniary loss under tort law in Europe

One of the many challenges of this issue is to find a way to frame the very concept of non-pecuniary or 'non-material' loss. At first sight, it seems to recover all those negative consequences of a harm which are not *per se* subject to an assessment in monetary terms. It is, indeed, difficult to find a way to describe this category of losses in a positive way, especially when you try to cover all of its facets. French lawyers use the phrase *souffrance morale*, that is moral suffering, but the word *suffering* is probably too strong and the term *moral* does not take into account that, in medical science, some kinds of *suffering* also have a physiological meaning [3]. One could say that non-economic loss refers to every kind of disturbance affecting the victim's feelings and not subject to a monetary assessment.

Given that the concept of non-economic loss is known today in all European tort law systems, it may seem rather intriguing that in every jurisdiction (even the most reluctant ones, such as Malta) [4], monetary damages are award-

tion (2017) 40 *Dublin University Law Journal*, 97; E. TRULI, *The General Data Protection Regulation and Civil Liability*, in M. BACKUM ET AL. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property: Towards a Holistic Approach* (Berlin 2018); AB MENEZES CORDEIRO, *Civil Liability for Processing of Personal Data in the GDPR* (2019) 5 *European Data Protection Law,* 492. In German, see C. BIEREKOVEN, *Schadensersatzansprüche bei der Verletzung von Datenschutzanforderungen nach der BDSG-Novelle* (2010) *Der IT-Rechtsberater*, 88; J. HARTUNG-L. BÜTTGEN, *Sanktionen und Haftungsrisiken nach der DSGVO* (2017) *Die Wirtschaftsprüfung*, 1152. See also, in Dutch, T. VALREE, *De vergoedbare schade bij de onrechtmatige verwerking van persoonsgegevens* (2017) *Weekblad voor Privaatrecht, Notariaat en Registratie*, 921.

[2] See, for example, WV HORTON ROGERS (eds.), *Damages for Non-Pecuniary Loss in a Comparative Perspective* (Berlin 2001); G. WAGNER, *Ersatz immaterieller Schäden: Bestandsaufnahme und europäische Perspektiven* (2004) *Juristen-Zeitung*, 319; J. KNETSCH, *Les limites de la réparation du préjudice extrapatrimonial en Europe*, P. BRUN-L. CLERC-RENAUD-C. QUEZEL-AMBRUNAZ (eds.), *Des spécificités de l'indemnisation du dommage corporel* (Bruxelles 2017). See also V. V. PALMER (eds.), *The Recovery of Non-Pecuniary Loss in European Contract Law* (Cambridge 2015).

[3] See, for example, F. BUZZI-M. VALDINI (eds.), *Medicina legale e sofferenza fisica e morale* (Milano 2010).

[4] On Maltese law, see C. MICALEF-GRIMAUD, *Article 1045 of the Maltese Civil Code: Is Compensation for Moral Damage Compatible Therewith?* (2011) 4 *Journal of Civil Law Studies,* 481. It was only through Act XIII of 2018 that a provision was added to article 1045 of the Maltese Civil Code, awarding damages for moral and psychological harm in cases of criminal offence.

ed for non-economic losses, although everyone agrees on the principle of incommensurability in this matter [5]. The classical methods for assessing the damage are, indeed, inadequate for pain and suffering damages, since a sum of money is fundamentally inappropriate to restore the *status quo ante*. In Germany, this mismatch between monetary damages and the mere idea of compensation is reflected in the case law where the term *Genugtuung* is used, sometimes with an idea of satisfaction or vindication for the infringement of the right [6]. In other jurisdictions, such as France, it seems that tort law scholars are following a sort of head-in-the-sand policy, pretending that awarding monetary damages for non-economic loss is a form of reparation like any other and that it does not raise any fundamental issues other than the precise assessment guidelines [7].

Throughout Europe, there are two contradictory trends in legislation and case law. On the one hand, there is a clear tendency towards a more systematic recognition of non-economic loss and lesser barriers to the recovery of monetary damages. Article 82 of the General Data Protection Regulation is just *one* illustration of the valorisation of human feelings in contemporary tort law. On the other hand, this 'boom' of *préjudice moral* is accompanied by an emerging reflection on the limits of this trend and, more generally, on where exactly the boundaries of modern tort law should be in our society:

- What are the disturbances that deserve a monetary compensation?
- Is it legitimate to take into account the seriousness of the tortfeasor's actions? Or do we have to assess damages on the sole basis of the victim's situation?
- What is the 'fair price' of human suffering?
- What place should the compensation of non-economic loss occupy in public discourse and discussions of legal policy?

---

[5] See, on this issue, M.J. RADIN, *Compensation and Commensurability* (1993) 43 *Duke Law Journal* 56 and C.R. SUNSTEIN, *Incommensurability and Valuation in Law* (1994) 92 *Michigan Law Review* 779. See also recently D. VON MAYENBURG, *Die Bemessung des Inkommensurablen* (Berlin 2012) and M. FABRE-MAGNAN, *Droit des obligations. Responsabilité civile et quasi-contrats* (Paris 2019), 4th ed., 146.

[6] From the German legal doctrine, see M. LEPA, *Die Wandlungen des Schmerzensgeldanspruchs und ihre Folgen*, in H.P. GREINER-N. GROSS-K. NEHM-A. SPICKHOFF (eds.), *Festschrift für Gerda Müller zum 65. Geburtstag am 26. Juni 2009* (Köln 2009) and D. VON MAYENBURG (fn 5) 37.

[7] For a critical assessment of the situation under French law, see J. KNETSCH, *La désintégration du préjudice moral* (2015) *Recueil Dalloz*, 443 and, most recently, H. GALI, *Le préjudice moral en droit de la responsabilité civile* (thesis, University Paris-Saclay 2019).

3. The right to compensation of 'non-material damage' under GDPR

One has to bear these questions in mind when it comes to damages for non-pecuniary loss in GDPR infringement cases. In cases of a breach of data protection regulation, the GDPR entitles the victim to claim compensation under the terms of article 82, which stipulates strict liability for the controller and, in certain cases, for the processor.

The right to compensation is specified in article 82 (1) GDPR that reads as follows: 'Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.' The wording of this provision is quite clear at first sight; it is presented as a statutory basis for a compensation claim [8]. There seems to be no need to invoke other provisions, national or European. Article 82 (1) provides directly for a claim to monetary compensation for 'material and non-material damage', that is pecuniary and non-pecuniary loss.

Indeed, regulations such as the GDPR have general application and are directly applicable in all EU countries. It is, therefore, logical that there be no need for the member states to take further action. Yet, in some member states (such as Ireland or the United Kingdom), there has been a debate about the necessity to incorporate some parts of the GDPR and, in particular, the right to compensation in case of an infringement of the GDPR provisions [9].

This debate might be surprising, but it can be explained by the specific place of civil liability in EU law [10]. Claims for compensation are typically provided for in directives rather than regulations, so article 82 (1) GDPR is rather unusual in that respect. A further aspect is that the formulation in article 82(1) is somehow ambiguous. It provides that a person who has suffered damage '*shall have* the right to receive compensation', which could indicate that it is not actually a *direct* basis for a compensation claim and that further steps must be taken by the EU or the member states before a plaintiff is entitled to claim compensation [11].

However, when you compare the wording of the different language versions of the GDPR, there can be no doubt that article 82 (1) is meant to give a direct right to compensation to the plaintiff without any detour via the national law.

---

[8] Under German law, one would say that the article is an *Anspruchsgrundlage*. On this issue, see E. O'DELL (fn 1) 111.

[9] See, in particular, E. O'DELL (fn 1) 121.

[10] See, *e.g.,* D. LECZYKIEWICZ, *Compensatory Remedies in EU Law: The Relationship Between EU Law and National Law*, in P. GILIKER (eds.), *Research Handbook on EU Tort Law* (Cheltenham 2017), 71.

[11] E. O'DELL (fn 1) 121.

This becomes even clearer when you compare article 82 (1) GDPR with another European legislation on data protection, the Police and Criminal Justice Authorities Directive of 2016 (PCJAD) [12]. In article 56, the PCJAD provides for the compensation of 'material or non-material damage' in case of the infringement of the data protection rules by the police or criminal justice authorities. The wording here is much more traditional as it reads that 'Member States *shall provide* for any person […] to have the right to receive compensation', which means that an implementation of this provision into national law is necessary.

The first conclusion is that article 82 (1) GDPR is a statutory basis for a claim to compensation in case of material and non-material damage caused by an infringement of EU data protection rules. Yet, one must admit that the vindication of that right cannot be as direct as other rights resulting from chapter III, such as information rights (right to access, right to erasure, etc.), which can be fulfilled directly by the controller. Article 82 (1) needs the intervention of the court or at least an out-of-court settlement to determine both whether the plaintiff has suffered the relevant 'material or non-material damage' and what the appropriate level of 'compensation' would be [13].

4. The assessment of 'non-material damage'

The GDPR does not give any guidelines about the assessment of damages which shall be awarded in order to compensate 'material or non-material damage'. In recital 146, the GDPR drafters stated that 'data subjects should receive full and effective compensation for the damage they have suffered'.

The clarification that the compensation should be 'full' refers to the principle of full compensation, which only means that the damages awarded to the plaintiff have to cover every head of the loss suffered and that there shall be no capping or limitation of damages.

As for the 'effective' nature of compensation, the significance is less clear. It might refer to the assessment of 'non-material damage', which is widely seen as a rather inaccurate science, leaving a certain margin of appreciation to the courts. In those member states which have a long tradition of awarding damages for non-pecuniary loss, the courts use more or less formal assessment guidelines, especially for pain and suffering and loss of amenities[14]. A UK tort lawyer would use the *Guidelines for the Assessment of General Damages in Personal*

[12] E. O'DELL (fn 1) 124.

[13] E. O'DELL (fn 1) 113.

[14] See, on this general issue, J. KNETSCH (fn 2) 23.

Injury Cases published by the Judicial College, which indicates the appropriate bracket of award for particular injuries on the basis of precedents [15]. In France, you will find similar ranges in a document issued by the board of Court of Appeal Judges, the *Référentiel Mornet* [16].

However, in cases of the infringement of personality rights, such as the right to privacy or the right to protect one's image or honour, assessment methods are often more flexible. It is not unusual for judges in these cases to take into account the satisfactory or even the punitive function of damages for non-pecuniary loss and refer at times to the malice of the tortfeasor, to the benefits he or she has taken from the situation or to the prominent public position of the claimant [17]. This is probably meant by recital 146 mentioning an '*effective* compensation'.

Yet, the assessment methods used by the national courts in those cases are very diverse and the issue is even more complex, since data protection tort law cases have arisen only recently, preventing courts from developing established practices.

There is a significant risk that GDPR infringement cases will give rise to a very differentiated court practice regarding the assessment of damages for non-pecuniary harm [18]. In the absence of European assessment guidelines, national courts are not to blame if they follow their own practice on the very moving ground of finding the right amount for the inconvenience caused by the infringement of GDPR rules. It is highly unlikely that the EU will enact precise assessment rules because the discrepancies between the level of damages awarded to plaintiffs also reflect the differences regarding the cost of living and the purchasing power in the member states.

5. Is there a need for a *De Minimis* Rule?

In some EU member states, such as France or Belgium, the simple suggestion of a *De Minimis* rule will be met with a sceptical frown, either because such

---

[15] JUDICIAL COLLEGE (eds.), *Guidelines for the Assessment of General Damages in Personal Injury Cases* (Oxford 2019) 15th ed.

[16] B. MORNET, *Indemnisation des préjudices en cas de blessures ou de décès* (2018) <http://www.ajdommagecorporel.fr/sites/www.ajdommagecorporel.fr/files/fichier_cv/RPC-BM-septembre%202018.pdf> accessed 10 January 2020.

[17] For the French law, see E. DREYER, *La faute lucrative des médias, prétexte à une réflexion sur la peine privée* (2008) 201 *La Semaine juridique. Edition générale* and S. CARVAL, *La responsabilité civile dans sa fonction de peine privée* (Paris 1995), 22.

[18] See, for example, B. KREßE, *DSGVO Art 82*, in G. SYDOW (eds.), *Europäische Datenschutzgrundverordnung* (Baden 2018) 2nd ed., 6.

a rule is widely unknown or because it is seen as a heresy to reject a compensation claim on the grounds that the loss has not reached a certain level of materiality [19]. This issue is of particular importance in the field of GDPR infringement cases since, before the RGPD came into force, the courts of several member states, such as Germany, held that the plaintiff had to establish a 'severe violation of a personality right' to be entitled to claim compensation [20].

We need to be asking to what extent the mere violation of GDPR data protection rules can give rise to a claim for compensation, even when the infringement has not had any serious impact on the everyday life of the plaintiff [21]. There are many cases in which a data breach only causes a slight inconvenience to the concerned person, for example, an avalanche of spam emails. Under the former case law, German courts did not allow any damages for non-pecuniary loss in those cases. But the practice could change under the influence of Article 82 (1) GDPR, which does not provide for such a strict gravity threshold.

It is too early to say if there will be any substantial changes in the national case law. A widely commented German district court judgement of November 2018 held that, although the threshold had been lowered significantly by the GDPR, the claimant still had to prove the existence of a 'non-material damage' [22]. For the district court judges, the sole breach of a GDPR provision is insufficient, *i.e.,* there has to be 'more' than the mere feeling of having been a victim of a breach of data protection rules. Subsequent judgments of other lower courts have confirmed this narrow approach to the right to compensation [23].

In the light of recital 146 and the aim of a 'full and effective compensation', this interpretation seems quite restrictive and may not be in full accordance to

---

[19] This issue has been given particular attention in German-speaking countries. See G. CHRISTANDL-D. HINGHOFER-SZALKAY, *Sinn und Funktion einer gesetzlichen Erheblichkeitsschwelle im Nichtvermögensschadensrecht* (2009) *Juristische Blätter*, 284 and D. VON MAYENBURG, *Nur Bagatellen? – Einige Bemerkungen zur Einführung von Schmerzensgeld bei Gefährdungshaftung im Regierungsentwurf eines Zweiten Gesetzes zur Änderung schadensersatzrechtlicher Vorschriften* (2002) *Zeitschrift für Versicherungsrecht*, 278. See also in French J. KNETSCH (fn 2) 36.

[20] On this fundamental difference between the former German case-law and article 82 (1) GPDR, see T. BECKER, Art 82 DSGVO, in KAI-UWE PLATH (eds.), *DSGVO/BDSG* (Köln 2018) 3rd ed., 4c (with further references).

[21] T. BECKER (fn 20); C. PILTZ, *Art 82*, in P. GOLA (eds.), *Datenschutz-Grundverordnung* (Munich 2017), 12.

[22] Case C 130/18, District Court Diez, 7.11.2018, *Zeitschrift für Datenschutz* (2019) 8, 85.

[23] Case U 760/19, Higher Regional Court Dresden, 11.06.2019, *Monatsschrift für Deutsches Recht* (2019) 4, 1193; Case C 485/18, District Court Bochum, 11.03.2019, *IT-Rechtsberater* (2020) 65, 11. On this case law, see also T. WYBITBUL, *Immaterieller Schadensersatz wegen Datenschutzverstößen – Erste Rechtsprechung der Instanzgerichte* (2019) *Neue Juristische Wochenschrift*, 3265.

the political rationale of the GDPR. Compensation claims, asserted via individual or class actions, have been designed as an instrument for the private enforcement of data protection rules, which calls for a wider interpretation of the concept of 'non-material damage'. Courts in Austria and the Netherlands have, therefore, opted for a wider approach, awarding damages on the sole ground of a data breach deemed to affect the individual's right to data protection [24].

Eventually, it will be up to the European Court of Justice to decide whether compensation claims for non-pecuniary loss will be an effective means to protect personal data or if the economic impact of a wide compensation system will act as a deterrent for such a wide understanding. The broader you interpret the concept of 'non-material damage', the more effective private enforcement of data protection rules will be. Both approaches seem defensible and, in the end, it is a political issue rather than a legal-technical one which the ECJ judges will have to address.

6. Conclusions

As the 21st century is entering its third decade, there is a consensus among tort lawyers that the increasing value of immaterial interests has to be taken into account and that a sufficient protection of personality rights would not be possible without the monetary compensation of non-pecuniary loss. By referring to 'material' and 'non-material damage', article 82 (1) GDPR ascertains this trend in the field of data protection law, yet without providing any guidance on the delimitation of cases eligible for a compensation of non-pecuniary loss and the assessment of damages. At a time when cases of data breach cut across jurisdictional frontiers, it would be of great concern if the national court practice revealed significant discrepancies regarding the principle of compensation and, especially, the amounts awarded for similar cases.

[24] Case Cg 30/19b, Regional Court Feldkirch, 7.8.2019, *Computer Law Review International* (2019) 57, 147; Case no 7560515 CV EXPL 19-4611, Court Amsterdam, 2.9.2019, *Jurisprudentie Arbeidsrecht* (2019), 241.

ART. 82 GDPR: STRICT LIABILITY OR LIABILITY BASED ON FAULT? *

Radosław Strugała, University of Wrocław

Abstract:

In its article 82 the GDPR expressly deals with damages for the infringement of the regulation. From the mere wording of the article it is not clear, whether the right to compensate is dependent on fault. Policy arguments suggest that the liability spelled out in the article 82 should be interpreted as strict. Strict liability although full and effective, in some instances may turn out to be excessive for the torfeasors and thus result in overdeternce. The aim of the article is both to verify the hypothesis of the liability at stake being strict and, in case of its affirmation, to propose to remedy some adverse effects.

Keywords: Data Protection Law, fault, strict kiability, multiple tortfeasors, recourse claim

Summary: 1. Preconditions to Liability provided in art. 82. – 2. The relevance of fault. – 3. Too burdensome liability of controlers? – 4. Towards fair allocation of risk. – 5. Concluding remarks.

1. Preconditions to Liability provided in art. 82

According to the article 82 of the General Data Protection Regulation (GDPR) any person who has suffered material or non-material damage as a result of an infringement of this regulation shall have the right to receive compensation from the controller or processor for the damage suffered. The compensatory liability spelled out in this provision of the GDPR may be viewed as an additional incentive for data controllers and processors to abide the rules on data

* The work was supported by the National Science Centre, Poland, under research project *"Sprawiedliwość prawa deliktów w XXI w. Funkcje odpowiedzialności deliktowej w świecie nowych technologii"*, no UMO-*2017/27/B/HS5/0089*.

processing. This compensatory scheme may thus operate alongside the public punishment with the aim to increase the effectiveness of the GDPR (or – in other words – to constitute the tool of its „private enforcement"). Looked at from this perspective the liability spelled out in the article 82 seems to be designed to play a preventive role. In fact, the preventive function (deterrence) of damages is familiar to European private law tradition [1]. What is however the main purpose of damages is compensation [2]. Therefore the liability at stake should in the first place grant any single data holder the compensation for losses incurred as a result of data breach. The preamble of the GDPR leaves no doubt that compensation constitutes a main aim of the liability at hand (see recital 146).

Whether the goal of compensation can be achieved under article 82 depends on the interpretation that will be employed in respect to the conditions to liability provided therein. When talking about preconditions to liability in damages traditionally three are pointed out, namely: a loss (be it monetary, non-monetary or both kinds of losses), an event defined in the piece of legislation imposing liability (the event that may trigger liability if it constitutes a cause of loss) and the causal link between this event and the items of loss incurred by the victim seeking compensation.

As far as the loss is concerned the GDPR provides a clear definition explaining that the term embraces two principle heads of losses, that is pecuniary and non-pecuniary losses. Although it is not expressly said in the GDPR it is quite clear that the first category composes both actual loss and lost future profits [3]. Some doubts may arise as to the scope of the term „non-monetary losses" used in the article 82. One may ask whether it only stands for pain and suffering or means loss of amenity as well. This doubt could well be avoided by the proper wording of the article at stake, especially that the EU legislation is aware of the potentiality of interpretative problems and can handle it successfully as shown in the article 2 of the CESL where "loss" is expressly defined as economic loss and non-economic loss in the form of pain and suffering, excluding other forms of non-economic loss such as impairment of the quality of life and loss of enjoyment. It seems however, that the problem is rather of minor importance and can easily be tackled by the future CJEU case law.

---

[1] P.H. OSBORNE, *The Law of Torts* (Toronto 2011), 14; G.T. SCHWARTZ, *Reality in the Economic Analysis of Tort Law: Does Tort Law ReallyDeter?* (1994) 42 *UCLA Law Review*, 377, 425-427.

[2] C. VAN DAM, *European Tort Law* (Oxford 2013), 347; H. KOZIOL, *Comparative Conclusions in Helmut Koziol* (ed.) *Basic Questions of Tort Law from a Comparative Perspective* (Wien 2015), 746.

[3] See Opinion of A.G. CAPOTORTI in Case C-238/78, Ireks-Arkady GmbH v Council and Commission, ECR, 4.10.1979, 2955.

The same holds true for the way the GDRR handles causality. Despite the lack of any suggestion of how it should be ascertained when applying the article 82 it is quite obvious that it should be understood as based on the assumption commonly shared in European private law systems, that the liability arises only where the loss is sufficiently close (proximate cause) or adequate to the event[4].

2. The relevance of fault

Much more problematic is the formulation of the third condition to liability being the event causing loss of the data holder. It is not clear from the wording of the provision whether the mere breach of rules concerning data processing constitutes an event giving rise to liability on its own. Possible interpretation involves additional requirements of intention or negligence being necessary to trigger liability. In other words, it is not certain if the liability is based on fault or is purely objective, which would entail that the liability may be established irrespectively of any kind of fault on the controller's or processor's side. Doubts are even more apparent if one takes into account the discrepancies in different language versions of the GDPR. The above-mentioned discrepancies concern the condition to escape liability described in the 3th paragraph of the article 82. Whereas the majority of the language versions use the formula, according to which the controller and processor may be exempt from liability if they prove that they are „not in any way responsible for the event giving rise to the damage", the Polish version dictates that the exemption comes into play where the controller or processor prove not to be at fault.

Doubts as to the principle of liability (that is doubts concerning fault being or not being precondition to it) have serious bearing on data holders chances to claim compensation successfully. A restrictive interpretation demanding fault would entail that in great number of cases they could not be awarded damages. The mere fact of breaching the GDPR rules will not trigger liability if the controller's negligence cannot be established, for instance where the controller is not capable of guilt (of being held liable based on fault) because of mental illness. The liability of controller would not arise either if the breach of the GDPR can be ascribed to the processor and there is no negligence (or other type of fault) on the side of a controller. Where the processor turns out to be insolvent and incapable of paying damages, the victims remain uncompensated.

In my view, to establish whether the liability for losses stemming from data

[4] See Case T-149/96, Coldiretti and 110 Farmers v Council and Commission, EU, 30.9.1998, 228.

breach is dependent on fault two main arguments should be taken into account. The first argument speaking in favor of no fault liability interpretation is anchored in the wording of the GDPR's predecessor – the Directive 95/46/WE [5], which has been replaced by the GDPR in 2018. The directive not only used the same formula enabling the exemption from liability where the controller proves "not to be responsible" for breach of rules on data processing that the GDPR repeats in the article 82. It also listed in the preamble (recital 55) an exemplary circumstances the occurrence of which makes it possible to escape liability. These circumstances are: force majeure (*vis maior*) and fault on the part of the data holder. Both exemplary circumstances cannot be viewed as exculpatory in the traditional sense of the word as they do not entail the lack of fault defined as intention or negligence. The recital 55 of the preamble of the Directive made it clear that the possibility of escaping liability is exceptional and limited to very narrow matrix of facts which is a characteristic feature of strict liability scheme. The latter should not be confused with absolute liability. In contrast to it, within the strict liability scheme the tortfeasor can be exempted from liability in the case of successful exoneration. Exoneration is different from exculpation in that the former is possible only where one of certain exhaustively listed exoneration circumstances occurs and the tortfesor successfully proves to be so whereas the latter takes place where there is no intention or negligence on tortfeasor's side. Thus the liability provided in the Directive was not based on fault but a strict liability [6]. No suggestion can be traced down in the GDPR that it was intended to change the approach taken in the Directive.

Also it is necessary to bear in mind the requirement that the compensation be full and effective which is expressed in the preamble (recital 146) of the GDPR. In my view the need to decline fault as a precondition to liability at hand is a consequence of this requirement. As a matter of fact there is a great number of judgments, where the CJEU (ECJ) suggests or even expressly states that fault as a precondition to liability in the form of monetary compensation constitutes a serious obstacle for the victims and thus undermines the requirement of the compensation being effective.

This is the case of judgments concerning compensation for loss suffered through a breach of the competition rules (issued before the directive 2014/104

[5] 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.

[6] See M.A. BÜLLESBACH (eds.), *Concise European IT Law* (Praha 2010), 109; B. VAN ALSENOY, *Liability under EU Data Protection Law From Directive 95/46 to the General Data Protection Regulation* (2016) 7 *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 273.

EU on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union was in place). For instance in the "*Manfredi*" case [7] the Court of Justice stated that any individual can claim compensation for the harm suffered as a consequence of the breach of the competition rules and underlined that a causal nexus between an infringement of the competition rules and the harm thereby caused is sufficient to ground a claim in damages. This follows that in general no relevance should be given to whether the rules have been infringed intentionally or by negligence. In the course of preparatory work on the future directive the Commission later referred to this suggestion in the so called Green Paper and the so called White Paper. It was held that any fault requirements under national law would have to be limited for they hamper the effectiveness of compensation. The Commission saw no reasons to relieve infringers from liability on grounds of absence of fault other than in cases where the infringer made an excusable error (an error would be excusable if a reasonable person applying a high standard of care could not have been aware that the conduct restricted competition) [8]. Thus the Commission accepted that fault requirement would have to be limited to very exceptional situations.

Similar conclusions are to be drawn from the case law regarding private procurement law. For example in the judgments C-275/03 [9] and T-33/09 [10] the ECJ found the national law to be incompatible with the EU law (namely Council Directive 89/665/EEC on the coordination of the laws, regulations and administrative provisions relating to the application of review procedures to the award of public supply and public works contracts, currently replaced by 2014/24/EU on public procurement and repealing Directive 2004/18/EC) as it makes the tenderer's right to damages for breach of the private procurement procedure conditional on the prove of fault on the side of the contracting authority. Moreover, in the judgment C-314/09 when answering the Austrian's supreme Court preliminary ruling question the CJEU held that restricting access to compensation by the requirement that the contracting authority be at fault would be contrary to the wording, context and objective of the Directive even if the fault is presumed [11]. It was underlined that the Directive (Article 1(1), Article 2(1), (5) and

[7] Case C-295/04, Manfredi v Lloyd Adriatico Assicurazioni S.p.A., ECR, 13.7.2006, I-6619.

[8] G. CUMMING-M. FREUDENTHAL, *Civil Procedure in EU Competition Cases Before the English and Dutch Courts* (Praha 2010), 123; White Paper on Damages actions for breach of the EC antitrust rules 6.

[9] Case C- 275/03, Commission v Portugal, ECR, 2004, I-00000.

[10] Case T-127, Commission v Portugal, ECJ, 29.3.2011.

[11] Case C-314/09, Stadt Graz v Strabag AG, ECR, 30.9.2010, I-8769.

(6), and the sixth recital in the preamble) establishes the right to damages but makes no mention that the infringement of the public procurement legislation to give rise to a right to damages should have specific features, such as being connected to fault – proved or presumed [12].

3. Too burdensome liability of controlers?

The above-mentioned case law strongly supports the conclusion that no fault requirement should be added in the course of interpretation to the text that does not express such a requirement. This is true even if fault were presumed for it would still leave room for potential exculpation by the defendant which in turn undermines the effectiveness of compensation. Since the requirement of compensation being full and effective stands for the GDPR (recital 146 of the Preamble), the line of reasoning employed by the CJEU (ECJ) in the above-described judgement is to be shared in the course of interpretation of the article 82 of the GDPR. Thus the proper way of reading article 82 of the GDPR seems to be the interpretation according to which the liability is triggered by the mere breach of rules regarding data processing. In case of processors the breach may concern only these rules that are specifically directed to processors or may take the form of acting outside or contrary to lawful instructions of the controller. As far as the controllers are concerned the liability may be triggered by the breach committed by the controllers themselves or by processors acting on their behalf even if the controller did not commit any breach [13]. Consequently the possibility of the controller or processor being exempted from liability if they prove that they are not in any way responsible for the event giving rise to the damage should be limited to exceptional cases other than a simple lack of fault (that is exoneration reasons similar to these listed in the Directive 95/46). As such the liability at hand can be seen as strict liability [14]. This is especially true for the liability of controllers may be held liable even where they did not commit any wrongful, illegal act (any data breach).

Article 82 of the GDPR definitely provides for a high level of incentive to

[12] See also B. WINIGER-E. KARNER-K. OLIPHANT (eds.), *Essential Cases on Misconduct* (Berlin 2018), 188.

[13] See article 82(2) according to which any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

[14] B. VAN ALSENOY (fn 6) 283.

comply with data processing standards. While interpreted as not dependent on fault it also effectively grants compensation to any data holder who suffers loss as a result of a breach of these standards. However, a question may arise at this point whether the liability spelled out in the article 82 of the GDPR is not too excessive.

The question seems especially justified in respect to the liability of controllers for losses directly caused by the processors acting on their behalf as it appears to be far more burdensome than the traditional vicarious liability scheme. In contrast to vicarious liability (as known in the majority of legal systems), under article 82 of the GDPR the controller cannot escape liability by proving that the processor while processing data on their behalf acted outside their control and consent. This may result in judgments analogous to *Morissons data leak* case issued in the UK before the GDPR was in place (and thus decided on Data Protection Act 1998, DPA). The *Morrisons* supermarket chain has been found (both by High Court and Court of Appeal) liable for a personal data breach carried out by an employee, a senior internal auditor at the supermarket's, who deliberately leaked the details of staff members (information about staff salaries, bank details and national insurance numbers) to take revenge on the employer for disciplinary punishment. The High Court dismissed the primary claims as *Morrisons* had not authorized misuse of information and had appropriate measures in place that were intended to prevent misuse of personal data by *Morrisons* employees. In spite of this *Morrisons* was held vicariously liable – thus the liability was purely objective (strict) and the claim against *Morrisons* was based simply on the fact that the information entrusted to the defended were misused by their employee.

4. Towards fair allocation of risk

The burden of liability of controllers reflected in the *Morrisons* case results in a potential risk that should be of comparable concern to employers as the public punishments provided in the GDPR. The same is true for damages under article 82 of the GDPR if the no fault interpretation is accepted. Whether such a burden is just rises a serious question. It is true that the GDPR should work both as preventive and compensative tool. At the same time too high level of risk of liability may result in overdeterrence leading to the lowering of activity which puts entrepreneurs (data controllers) at risk of liability. There are at least two potential options to avoid this scenario in cases similar to *Morissons*.

On one hand it seems reasonable to read article 82 paragraph 4 and 5 [15] so that where a controller (or processor) who was not at fault has paid full compensation for the damage suffered, that controller (or processor) shall be entitled to claim back from other controllers or processors involved in the same processing who were at fault (especially where they committed breach intentionally or by gross negligence) the whole of the compensation paid so far. This interpretation would not hinder the compensative effect of liability as the compensation has already been paid (the compensation would remain full and effective). At the same time it would grant fair allocation of liability. It is controversial, however, if this interpretation can be accepted in the light of the wording of article 82. Although the article 82 is commonly said to be inspired by the Principles of European Tort Law (PETL), its wording differs significantly from the rules of solidary and several liability contained in the Principles. The latter rules expressly provide that a person subject to solidary liability (joint and several liability) may recover a contribution from any other person liable to the victim and that the amount of the contribution shall be what is considered just in the light of their respective degrees of fault (see article 9:102 of PETL). Whereas the GDPR mentions the possibility of claiming back the part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2. As said above, these conditions render the liability strict.

The alternative solution is to render it possible for the controllers in cases like *Morissons* to escape liability *vis-a-vis* the data holder. At the first glance it seems not to be excluded as the intention or gross negligence of the processor may appear to be exceptional event constituting the proof of the controller who is not at fault of him being „not in any way responsible for the event giving rise to the damage" in the meaning of article 82. This interpretation rises significant doubts though. First of all, it seems to seriously undermine the main purpose of the liability at stake as it may jeopardize compensation in cases where the processor happens to be insolvent. Moreover if the EU legislator had the intention of freeing controllers from liability in such circumstances they would have expressly deal with it in the article 28 of the GDPR. Its current wording speaks

[15] Article 82 (4): Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject. Article 82 (5): Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

against this interpretation. The article states that if a processor infringes the GDPR by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing. The article underlines however that this is „without prejudice to articles 82" which follows that the processor becomes co-controller alongside the main controller who still remains liable under the article 82.

5. Concluding remarks

The wording of the GDPR rules on civil liability is vague and leaves room for manifold interpretation. As shown above the risks that this shortcoming of the GDPR may bring about is as serious as the risks bound to the public punishments provided in the Regulation. This should enhance academics to focus not only on public enforcement questions but to give more attention to private enforcement tools of the GDPR. By doing so this paper aimed at establishing whether the liability provided in the article 82 of the GDPR is based on fault or can be viewed as strict. The conclusion that the liability at hand is strict calls for an interpretation of the article 82 that would render the liability of controllers less burdensome in these situations where the damage of data holder was directly caused intentionally or negligently by a processor acting on behalf of the controller who was not at fault. In my view the interpretation should be accepted, according to which article 82 paragraph 4 and 5 enables the controller who was not at fault and has compensated the victim (a data holder who suffered damage) to claim back from the processor at fault (especially where they committed breach intentionally or by gross negligence) the whole of the compensation paid so far. Despite the fact that the wording of the provisions at hand leaves doubts as to whether this interpretation is legitimate, their *ratio legis* seems to speak in favor of this interpretation.

LIABILITY FOR THE UNAUTHORISED USE OF PERSONAL DATA IN SOCIAL NETWORKS: THE CASE FOR COLLECTIVE REDRESS [*]

Albert Ruda-González, University of Girona (Spain)

Abstract:

This paper analyses liability for the unauthorised use of personal data in social networks such as Facebook. In particular, it presents and shortly comments upon one initiative in Spain to obtain collective redress for damage caused as a result of the so-called Facebook-Cambridge Analytica scandal.

Keyword: Facebook, Cambridge Analytica, data protection, collective redress

1. Introduction

It is already a common thing to hear that the world's most valuable resource is no longer oil, but data. The amount of published information or data is growing so rapidly that it is often talked of as a 'data explosion'. The effects of this abundance are felt in many ways, and inevitably some conflicts arise.

Data value usually increases when data is big. Big data provides a plethora of new opportunities and makes things which were previously unthinkable, possible. For instance, big data makes it possible to profile a person starting from the scat-

[*] This paper has been written in the framework of the research project DER2016-77229-R (Spanish Ministry of Economy and Competitiveness) of which the author is one of the co-directors. It was presented at a conference held in Bergamo (Italy) in October 3-4, 2019, under the title 'Private Enforcement of General Data Protection: Regulation New Chances, New Challenges'. The event was organised by Prof. Massimo Foglia (Bergamo).

tered pieces of personal information which the same person has been leaving through the Internet. Personal profiling in its turn makes it possible to offer that person personalised offers of products or services, including medical treatments or the like. Knowing the potential addressee of advertising better profers the obvious advantage that the person in question will be in a better position to receive information about commercial offers which may be to their interest.

However all this comes at a price, since personal profiling entails risks as well. Many Internet users have fallen for the idea that services like Facebook are 'free', when in fact they are not.

This paper explores one of the scenarios where personal profiling leads to harm caused to the individual whose information is used by another person. In particular, a violation of the rights to privacy and data protection may occur whenever someone gains access to another's personal data without authorisation. This is essentially what happened in the so-called 'Facebook-Cambridge Analytica scandal', where it is said that a private company was able to create personal profiles of thousands, if not millions, of people around the world, without their consent, by means of the Facebook social network. Whenever these kind of scenarios take place, it may be asked whether or not there is the possibility of some kind of redress for the affected data subjects, and if so, which.

Thus this paper analyses liability for the unauthorised use of personal data on social networks. In particular, it presents and briefly comments upon one initiative in Spain to obtain collective redress for damage caused from the social network under discussion.

2. Promethean fire

As is well known, the Facebook–Cambridge Analytica scandal was a major controversy in 2018, where the latter company allegedly harvested the personal data of millions of people's Facebook profiles without their authorisation to use it for political advertising. Cambridge Analytica, a company which had been created in 2013, managed to get access to a massive amount of personal data without the consent of the data subjects at issue. Although both companies involved basically denied any wrongdoing, it is alleged that around 50 million personal profiles were mined for data. The scandal attracted a great deal of public attention, in part because it was alleged that Donald Trumps' election victory as well as the Brexit vote may have profited from such a data misuse.

Access to personal data seems to have been gained through the use of a mobile application (or 'app') called 'thisisyourdigitallife'. The app was created by an academic called Aleksandr Kogan and his company Global Science

Research in 2004 [1]. Users downloaded the app from the Internet and were paid to take a psychological test. However this company not only gathered personal data from the users themselves but also from their Facebook friends by means of the app in question [2]. Kogan then shared the data with Cambridge Analytica, which developed software to help influence choices in elections, according to a the company's mastermind-turned-whistle-blower [3] Christopher Wylie.

According to Wylie, his job as a 'director in research' with Cambridge Analytica – where he served for one year and a half – consisted in designing psychological profiles to influence both the Brexit vote and the 2016 presidential election. The conservative strategist Steve Bannon –who later worked in President Trump's White House– was Wylie's boss [4]. Such influence was achieved by means of disinformation campaigns, which were microtargeted at people considered to be more prone to conspiratorial thinking, according to a book written by Wylie [5]. Following this account, 'Facebook's data was weaponised by the firm' and 'left millions of Americans vulnerable to the propaganda operations of hostile foreign states' [6]. From the whistle-blower's perspective, Cambridge Analytica was able to take a large amount of data and use it to design and deliver targeted content capable of moving public opinion on a large scale, and that was because Facebook's loosely supervised permissioning procedures made it surprisingly easy to do it [7]. In fact, it seems hard to imagine how such a data misuse would have been possible without a data set as large as the one managed by Facebook in the very first place. As one scholar has aptly put it, Facebook was at the time 'like the data set of the gods' [8]. Thus, Kogan

[1] Kogan was a psychologist who had earned an appointment as a lecturer at Cambridge University in 2012. See J.C. WONG-P. LEWIS-H. DAVIES, *How academic at centre of Facebook scandal tried – and failed – to spin personal data into gold* (2018) *Guardian*, available at https://www.theguardian.com/news/2018/apr/24/aleksandr-kogan-cambridge-analytica-facebook-data-business-ventures (accessed 1 May 2020).

[2] See Channel 4 News, *Here's everything you need to know about the Cambridge Analytica scandal* (2018), available at https://www.cnbc.com/2018/03/21/facebook-cambridge-analytica-scandal-everything-you-need-to-know.html (accessed 1 May 2020).

[3] As S. ZUBOFF, *The Age of Surveillance Capitalism* (London 2019), 278, calls him.

[4] See Forbes, *Christopher Wylie* (2020), available at https://www.forbes.com/profile/christopher-wylie/#6b36729f7f47 (accessed 1 May 2020).

[5] See C. WYLIE, *Mindf*ck. Inside Cambridge Analytica's Plot to Break the World* (London 2019), 5 ff. As Wylie explains, in the practice of microtargeting 'machine learning algorithms ingest large amounts of voter data to divide the electorate into narrow segments and predict which *individual voters* are the best targets to persuade or turn out in an election (*ibidem* 22).

[6] *Ibidem* 5 and 66.

[7] *Ibidem* 95.

[8] See S. LEVY, *Facebook. The Inside Story* (London 2020), 406. According to the same author, even if Facebook had always set its terms so that information could not be retained, transferred, or

acted as a sort of Prometheus by stealing the divine fire and making it possible for Cambridge Analytica to misuse it.

3. The case for collective redress

As seems obvious, in a case like the one described above the number of persons affected by the data misuse is very large. Not only was personal information gathered from the app's direct users, but also their Facebook friends. Data provided by themselves to Facebook was used to create psychological profiles with which to categorise them. Those who seemed more vulnerable to psychological manipulation were targeted by Cambridge Analytica so their vote could be changed if needed. In essence, it is not only the right to privacy that is at stake here – in those legal systems where such a right is protected – but also the right to data protection. Facebook failed to prevent the misappropriation of data from happening. Moreover, it failed to timely inform the affected users. What is worse, once it looked into the matter, it discovered hundreds of other developers who had violated its rules, and suspended 69,000 apps, including 10,000 which may have misused Facebook user data[9]. That in itself proves that Facebook could have done better in the past.

When considered in an isolated way, harm is very small indeed. Therefore, from an economic perspective each individual affected has little incentives to litigate. However, when considered from a collective or macro perspective, harm is considerable. Furthermore, the nature of harm sustained by the victims is homogenous. When these conditions concur, there are good reasons from a procedural economy perspective to put all the single claims together and let a single court decide them all as a whole. Such a collective claim also avoids the risk of the contradicting court decisions, which could be issued if each victim filed a separate claim on their own. If one bears all this in mind, it cannot come as a surprise that since the scandal there have been several collective claims running in parallel in different countries –as will be shown below.

4. Spain is different

In the case of Spain, there are two separate initiatives in connection with the scandal mentioned above which are worth mentioning.

---

sold, it had done very little to enforce those rules, and it still had no way of actually knowing what happened to data after it left Facebook (*ibidem* 410).

[9] *Ibidem* 430.

The first is a complaint filed by a consumer association called FACUA-Consumers in Action [10] before the Spanish Agency on Data Protection (*Agencia Española de Protección de Datos* or AEPD for short) [11]. The AEPD is a public administration independent agency which is entrusted with the protection of personal data in Spain. In accordance with the administrative nature of the agency, it does not settle private law matters and does not thus award compensation to the victims, however it may fine the liable parties. This is in line with the general stance adopted by Spanish law, whereby public authorities may impose fines on the infringers but are generally not allowed to decide on damage compensation to private parties [12]. The latter can nevertheless file a claim before the court. The scope and functioning of the Agency is provided for by domestic legislation, namely the Organic Act on Personal Data Protection and the Safeguard of Digital Rights 2018 [13].

The second initiative, which will be elaborated on further in this paper, is the claim filed by a different consumer protection association, called Organización de Consumidores y Usuarios (OCU) [14]. It is a consumer organisation in the form of a private law association created in 1975 and thus created non for profit. It currently has about 300,000 members.

The OCU claim is more interesting than the one mentioned above for several reasons. To start with, the claim is filed against Facebook in connection with the scandal referred to before. According to the claimant association, the problem is not only the violation of data protection but also the business model adopted by the defendant company. The claim was filed in October 2018 before the Commercial Court No 5 of Madrid. In July 2019, the claim was allowed for further study by the court, thus it was not rejected on preliminary

---

[10] FACUA stands for "Federación de Asociaciones de Consumidores y Usuarios de Andalucía". Currently the association has extended its radius of operation beyond the region of Andalusia to which it was initially devoted and is one of the major consumer protection associations in the country. See the association's website at www.facua.org/english (accessed 1 May 2020).

[11] See the Agency's website (available in Spanish only) at www.aepd.es/es (accessed 1 May 2020).

[12] See E.C. LOBATO, *La liquidación de daños entre particulares en el procedimiento administrativo* (2003) 2 (1) *InDret*, 2.

[13] *Ley Orgánica* 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (Official Gazette, *Boletín Oficial del Estado,* BOE, no 294, 6 December 2018). Available at www.boe.es/eli/es/lo/2018/12/05/3 (accessed 1 May 2020). In legal scholarship generally see M. A. ARENAS RAMIRO – A. ORTEGA GIMÉNEZ (eds.), Protección de datos. Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD (Madrid 2019), with further references.

[14] Its webpage can be found at www.ocu.org/ (accessed 1 May 2020).

grounds [15]. The text of the claim itself has not been published [16].

Pursuant to what the claimant has explained in press notes and the media, the claim is based on the lack of the users' consent to use their data for political profiling. Facebook users were not even informed about what the aim for using their data was. According to OCU, data can be the object of a property right, and thus it belongs to the user only. Therefore, each user alone is entitled to decide about data use. Leaving aside for now whether such a proprietary approach is statutorily correct or even theoretically sound, the claim further relies on the fundamental right to personal data (enshrined in the Spanish Constitution, art 18.4) [17]. According to OCU, this is an instance where it becomes necessary to protect an interest of a diffuse nature (*intereses colectivos difusos*) [18].

The claimant requests several things from the court. First, a declaration that the standard terms on which data gathering from Facebook was made possible are illegal and therefore void. Second, cessation and abstention in the future, so further violations are prevented from occurring. And third, and perhaps most interestingly, OCU claims compensation for harm caused to each Spanish Facebook user. The compensation award requested is established at 'at least' 200 € per person. Bearing in mind that in Spain there were around 23 million users at the time when the events took place, that would entail one of the highest compensation sums ever to be awarded by a Spanish court, should the claim succeed [19].

The previous is both noteworthy and astonishing. To start with, it may strike the reader that the compensation sum requested is of 'at least' 200 € [20]. This is in contrast with the general provisions of Spanish procedural law, according to

---

[15] According to information provided by OCU, Admitida a trámite la demanda colectiva de OCU contra Facebook, 9 July 2019, available at https://www.ocu.org/organizacion/prensa/notas-de-prensa/2019/admision-demanda-facebook.

[16] A request from the author to obtain a copy was rejected by an OCU official on the basis of intellectual property protection.

[17] An official English translation by the Spanish Official Gazette can be found online under BOE, The Spanish Constitution, available at www.boe.es/legislacion/documentos/ConstitucionINGLES.pdf (accessed 1 May 2020).

[18] See Radio Televisión Española, *La OCU demanda a Facebook por la cesión irregular de datos de sus usuarios españoles*, 11 October 2018, www.rtve.es/noticias/20181011/ocu-demanda-facebook-cesion-irregular-datos-usuarios-espanoles/1817367.shtml (accessed 1 May 2020).

[19] The number of Facebook users in Spain has declined since then. According to data provided by Statista, Facebook has lost approx. 2 million users in this country in the last two years. See Statista, *Número de usuarios de Facebook en España de 2014 a 2019* (2020), available at https://es.statista.com/estadisticas/518719/usuarios-de-facebook-en-espana/ (accessed 1 May 2020).

[20] See OCU, *OCU presenta una demanda colectiva contra Facebook por cesión irregular de datos*, 11 October 2018, available at www.ocu.org/organizacion/prensa/notas-de-prensa/2018/demandafacebook111018 (accessed 1 May 2020).

which the object of the claim has to be 'precise and clear' (pursuant to art 399.1 of the Civil Procedure Act or *Ley de Enjuiciamiento Civil*, hereinafter LEC)[21]. From a practical perspective, it is worth mentioning that under Spanish law a court is prevented from awarding the claimant more than the latter has claimed (art 218.1 LEC).

Moreover, this is actually a very low amount, at least if one compares the same with the one asked for in similar claims filed in other countries. For instance, in the Austrian case *Max Schrems v Facebook* (pending before Austrian Supreme Court at the time of sending this paper to press), the compensation sum requested was 500 € per user[22]. And in a class action filed in the US the claim was 1,000 USD per user (totaling approx. € 5,200 million to the change)[23].

5. #MyDataIsMine

As has been said, OCU filed its claim in October 11th, 2018 before a commercial court in Madrid. This is not an isolated case since there have been sister claims in other countries as well. The alleged purpose of the claim is 'to compensate all users who could be the victims of data misuse'. According to Facebook, the number of victims of Cambridge Analytica in Spain is approx. 137,000[24].

When OCU received notice of the case, it started a campaign in the media called '#MisDatosSonMios'[25] (#MyDataIsMine, in the English translation) and invited the affected parties to support the claim. OCU has not made clear what kind of support it was seeking, in particular whether it was merely begging for

---

[21] See *Ley* 1/2000, de 7 de enero, de Enjuiciamiento Civil (BOE no 7, 8 January 2000), available at www.boe.es/buscar/act.php?id=BOE-A-2000-323 (accessed 1 May 2020).

[22] Mr. Schrems filed further claims afterwards when the General Data Protection Regulation was passed. See D. SCALLY, *Max Schrems files first cases under GDPR against Facebook and Google* (2018) *The Irish Times*, available at https://www.irishtimes.com/business/technology/max-schrems-files-first-cases-under-gdpr-against-facebook-and-google-1.3508177 (accessed 1 May 2020).

[23] See O. BOWCOTT - A. HERN, *Facebook and Cambridge Analytica face class action* lawsuit (2018) *The Guardian*, available at https://www.theguardian.com/news/2018/apr/10/cambridge-analytica-and-facebook-face-class-action-lawsuit (accessed 1 May 2020).

[24] To be more precise, exactly 136,985 Facebook users downloaded the app. See L.J. SÁNCHEZ, *Un año después de Cambridge Analytica, los expertos creen que un escándalo similar podría ser posible en nuestro país* (2019) *Confilegal*, available at https://confilegal.com/20190320-un-ano-despues-de-cambridge-analytica-los-expertos-creen-que-un-escandalo-similar-podria-ser-posible-en-nuestro-pais/ (accessed 1 May 2020).

[25] See the webpage by OCU, *Mis datos son míos, Mr. Facebook*, available at https://www.ocu.org/especiales/misdatossonmios/ (accessed 1 May 2020).

funds to continue the claim, merely moral support, or legally joining other claimants to the civil procedure. According to the press, OCU is going to 'represent all Facebook users in Spain'. However, the form used in the OCU website asks the supporter to indicate whether she is a Facebook user or not. This suggests that a non-user can thus 'support' the campaign but not necessarily join the court proceedings or even count as a victim. At the time of sending this paper to the editor, 47,328 persons have joined the campaign. This is a notably small amount, if one takes the total number of Facebook users in Spain into consideration, as referred to above. Nonetheless, it seems a huge amount even for collective claims under Spanish law.

The OCU claim must be read against the background of a 'My Data is Mine Declaration', i.e. some sort of manifesto signed by OCU itself together with several foreign consumer organisations, namely Altroconsumo, Deco-Proteste, Proteste and Test-Aankoop/Test-Achats [26]. The declaration starts from the basis that the new data economy is a game-changer, it stresses the emergence of 'predictive profiling' and the Internet of Things (IoT) and that users should be recognised as data 'owners'. According to the same, '[w]e cannot relinquish our autonomy and freedom in exchange for our comfort'. Moreover, the signatory parties state that complying with legislation is not enough. As their text goes, '[a]lmost fully account' for added value should be provided to the user (benefits should be shared on a fair basis between data controllers and data subjects). Moreover, it continues, '[c]onsumers are crucial catalysts of a more sustainable and responsible digital value chain to make the data economy flourish'.

6. A matter of class

Although it is obviously too early to make any prognostic judgement about the prospective future (or lack of it) of the claim, it may be interesting to consider for a while the basis on which it is grounded, on which logically most of its strengths or weaknesses depend. The claim starts from the fact that there has been a data leak, since data which was controlled by Facebook ended up in the hands of another company without the users consenting or even knowing. Moreover, OCU stresses that Facebook has failed to provide a satisfactory explanation. In fact, there is no evidence that Facebook has adopted any steps to prevent something similar from happening again [27]. Pursuant to the claim, Face-

[26] Available at https://www.mydataismine.com/manifest (accessed 1 May 2020).

[27] See J.C. WONG, *The Cambridge Analytica scandal changed the world – but it didn't change Facebook* (2019) *The Guardian*, available at https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook (accessed 1 May 2020).

book behaviour compromised several legally protected interests, namely privacy, data protection, users autonomy (#NoSomosMarionetas [We are not puppets]), and data ownership (#MisDatosSonMios).

In its turn, Facebook has replied that there is actually no proof of data sharing and that data obtained was from people who downloaded the app, meaning there was no violation whatsoever [28].

The claim's basis is similar to the one of other claims in foreign countries. The Cambridge Analytica scandal has given rise to more than thirty class actions internationally, and according to an opinion this could be just the tip of the iceberg [29]. A UK organisation called Fair Vote [30] has prepared a claim along the lines of the one filed by OCU in Spain. Facebook has actually been brought to court not only because of the Cambridge Analytica app but because of other third-party apps as well. Among others, it has been sued in the in the US District Court Northern District of California because of a data hacking which affected 50 million users (e.g. *Carla Echavarria and Derrick Walker v Facebook, Inc.*) [31]. Another claim – coincidentally, filed before the very same court as the previous one – was based on misconduct on Facebook's part because of users' location tracking when location had been deactivated (*Brett Heeger v Facebook*) [32]. In a different case, the claimant complained of Facebook logging of text messages and phone calls through its smartphone app (*John Condelles III v Facebook*) [33]; the claimant seeks at least USD 5 million and to turn the suit into

---

[28] See S. SALINAS, *Zuckerberg on Cambridge Analytica: "We have a responsibility to protect your data, and if we can't then we don't deserve to serve you"* (2018) *CNBC*, available at https://www.cnbc.com/2018/03/21/zuckerberg-statement-on-cambridge-analytica.html (accessed 1 May 2020).

[29] See J.J. ROBERTS, *Facebook Has Been Hit by Dozens of Data Lawsuits. And This Could Be Just the Beginning* (2018) *Fortune*, available at https://fortune.com/2018/04/30/facebook-data-lawsuits/ (accessed 1 May 2020).

[30] See the campaign webpage under https://fairvote.uk/home/facebook-claim/ (accessed 1 May 2020).

[31] *Carla Echavarria and Derrick Walker v Facebook, Inc*., no. 5:18-cv-05982 (N.D. Cal. Sept. 28, 2018). On which see E. MELAMPY-A. LIU, *Echavarria v Facebook: Class Action Complaint Seeks Damages for the Massive Facebook Data Breach* (2018) *JOLT Digest*, available at https://jolt.law.harvard.edu/digest/echavarria-v-facebook-class-action-complaint-seeks-damages-for-the-massive-facebook-data-breach (accessed 1 May 2020).

[32] C-3:18-cv-06399, Heeger v Facebook, California Northern Court, 11.10.2018. The complaint can be found at https://www.classaction.org/media/heeger-v-facebook-inc.pdf (accessed 1 May 2020). On which see M.C. KELLY - J. FISHMAN, *Class Action Suits Challenge Facebook, Google Over Location* Tracking (2018), *JOLT Digest* available at https://jolt.law.harvard.edu/digest/class-action-suits-challenge-facebook-google-over-location-tracking (accessed 1 May 2020).

[33] C- 3:18-cv-02727, Condelles III v Facebook*,* District Court, N.D. California, 9.5.2018. See the

a class action across the US [34]. Just to provide another example, Facebook was also sued because of incidents of scanning of private messages without consent (*Campbell v Facebook*) [35]. In a settlement agreement, Facebook agreed to cessation of scanning, among other practices [36].

7. What is next

The OCU claim, commented upon earlier, is extremely interesting for several reasons. To understand these, it is important to provide some context on the general framework under Spanish law. Spanish law does not have a 'class action' strictly speaking, and therefore the case under comment is no true class action. Accordingly, a single individual cannot file a class action under Spanish civil procedural law. Rather, legal scholarship describes the existing collective claim, which can indeed be filed, as a sort of 'collective compensatory action' which is not entirely equivalent to the US class action [37]. At any rate, in this paper the traditional terminology of 'class action' will be used for the sake of clarity and brevity.

Spanish legal scholars generally agree that the statutory framework on the Spanish class actions is confusing. As a civil law jurisdiction, substantive rules are provided in a Civil Code (*Código Civil*) [38], which dates from 1889 but has been amended many times. Consumer law has grown outside the Code in several separate statutes, the principal one being a consolidated Consumer Protection

---

case file at https://www.pacermonitor.com/public/case/24465744/Condelles_III_v_Facebook,_Inc (accessed 1 May 2020).

[34] See S. GIBBS, *Facebook hit with class action lawsuit over collection of texts and call logs* (2018) *The Guardian,* available at https://www.theguardian.com/technology/2018/may/11/facebook-class-action-lawsuit-collection-texts-call-logs (accessed 1 May 2020).

[35] C-13-5996 (WL 3581179), Campbell v Facebook, District Court, N.D. California, 18.8.2017, appeal docketed C-17-16873, 9.9.2015. The complaint is available at https://digitalcommons.law.scu.edu/historical/603/ (accessed 1 May 2020).

[36] See A. BHARATKUMAR-L. REMBAR, *Campbell v Facebook: California District Judge Approves Final Class Action Settlement Over Facebook's Use of URL Data* (2018) *JOLT Digest*, available at https://jolt.law.harvard.edu/digest/campbell-v-facebook-california-district-judge-approves-final-class-action-settlement-over-facebooks-use-of-url-data (accessed 1 May 2020).

[37] See J.J. MARÍN LÓPEZ, *Las acciones de clase en el derecho español* (2001) 1 (3) *InDret*, 3, available at https://indret.com/wp-content/themes/indret/pdf/057_es.pdf (accessed 1 May 2020).

[38] *Real Decreto* de 24 de julio de 1889 por el que se publica el Código Civil (Madrid Gazette, *Gaceta de Madrid*, 206, 25 July 1889). An official translation into English has been published by the Spanish Ministry of Justice (Ministerio de Justicia), *Spanish Civil Code,* Madrid, BOE, 2013. It can be found under http://derechocivil-ugr.es/attachments/article/45/spanish-civil-code.pdf (accessed 1 May 2020).

Act from 2007[39]. Private procedure is basically provided for in the Civil Procedure Act (LEC), mentioned above.

The procedural rules on class actions are indeed far from being clear because of deficient legal drafting. The LEC, mentioned above, provides the general rule on the standing of consumer associations to sue. Pursuant to art 11.3, *When those harmed by a harmful act are an indeterminate or difficult to determine plurality of consumers or users, the standing to sue in defense of these diffuse interests will correspond exclusively to the consumer and user associations that, according to the law, are representative*[40]. However, it is doubtful whether in the case at stake it is correct to talk of 'diffuse interests' (*intereses difusos*). As has been seen above, the interests harmed by Facebook in the context of the Cambridge Analytica scandal seem to be not of a truly diffuse nature, but in fact they are rather individual and homogeneous interests, namely, those of many consumers which can be very easy to determine. The relevant question is merely whether they were Facebook users when the facts occurred.

The previous comments lead to the conclusion that neither OCU, nor any other consumer protection association, has an exclusive standing to sue in this case. Rather, since those harmed are 'perfectly determined' or 'easily determinable', as the LEC provides (in art 11.2), those associations do indeed have standing to sue, but so do the groups of affected persons.

It remains to be seen whether the claim will be allowed or not. At any rate, the judge will call any interested parties to the court (pursuant to art 15 LEC). Thereby, any individual consumer who may have been harmed by the data misuse may have the opportunity to take part in the proceedings (art 15.1 para 1 LEC). The complaint will be eventually published by the court secretary. The Public Prosecutor, who has a more active role in private law cases under Spanish law than under other jurisdictions, may also be a party in the proceedings whenever it is considered that the social interest of the case so requires (art 15.1 para 2 LEC). Since, as has been noted, in this case the potential victims are easily identifiable, OCU may be deemed to have already complied with the statutory requirement (pursuant to art 15.2 LEC) that it notify all the interested parties about the intention to file a claim – given that it already campaigned as de-

[39] *Real Decreto Legislativo* 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (BOE 287, 30 November 2007), available at https://www.boe.es/buscar/act.php?id=BOE-A-2007-20555 (accessed 1 May 2020).

[40] Translation by the author. The original Spanish text reads as follows: *Cuando los perjudicados por un hecho dañoso sean una pluralidad de consumidores o usuarios indeterminada o de difícil determinación, la legitimación para demandar en juicio la defensa de estos intereses difusos corresponderá exclusivamente a las asociaciones de consumidores y usuarios que, conforme a la Ley, sean representativas.*

scribed above. If the court considers instead that it is too difficult for the claimant association to determine who the interested parties are, the proceedings will be suspended for a time period not exceeding two months, after which it will carry on with the consumers who have come to the court (pursuant to art 15.3 LEC). Any other consumers will not be allowed to join the case. However, should the claim prevail, they court may individually determine which consumers may benefit from the compensation award (art 221.1 and 519 LEC).

One of the more controversial issues in the case may be that of damage sustained by the parties. It does not seem entirely clear how the 200 € amount was established. OCU states that this should be compensating non-pecuniary loss (*daño moral*) sustained by the victims. However, damage assessment in the case of this kind of damage is obviously not as clear-cut as in the case of patrimonial damage (*daño patrimonial*, as it is called in Spanish). Spanish courts tend to be quite generous with regard to non-pecuniary loss compensation, although the criteria on which the precise award is based are not always apparent [41].

At any rate, the present case may pave the way for other claims in the future, or not, depending on the outcome. The case may be a success anyway (in terms of publicity for the claimant organisation), which seems to have won some additional notoriety because of the claim.

8. Conclusions

The Facebook-Cambridge Analytica scandal is an excellent example of the risks posed by big data. Although it has attracted a lot of attention it does not seem to be an isolated case, but merely a symptom of the way in which capitalism operates in the digital realm [42]. In this particular case, personal data of millions of Facebook users was misused for political advertising without the data subjects' consent or even their being aware of it. It seems clear that Facebook negligently failed to adopt the steps required to prevent such a data misappropriation from taking place. Thus this is a clear case for a compensation claim based on the failure to secure the data and avoid such leaks. Even when Facebook requested that Cambridge Analytica and Wylie erase the data, Facebook never followed the request up and performed no due diligence [43]. It is no sur-

[41] A scholarly opinion even complained that the Spanish courts munificence to that regard was in itself a scandal. See L.M. DÍEZ-PICAZO, *El escándalo del daño moral* (Madrid 2008).

[42] According to S. ZUBOFF (fn 3) 280, Cambridge Analytica 'merely reoriented the surveillance capitalist machinery from commercial markets in behavioral futures toward guaranteed outcomes in the political sphere'.

[43] As explained by another whistle-blower, see B. KAISER, *Targeted. My Inside Story of*

prise, then, that several class action suits have been filed in different countries.

In Spain, the class action filed by the OCU, a major consumer protection association, has taken the lead and has attracted a great deal of public attention. However the huge number of potential victims, the lack of clarity as to how the damages are assessed, and a deficient statutory framework cast some doubts as to the outcome of the case now before the courts. In the meantime, it seems that Facebook is making use of every resource it can avail itself of to delay the court proceedings – including challenging the jurisdiction of the Spanish courts or requesting every document to be translated [44]. Whereas it is unclear whether Facebook has changed enough as to avoid anything similar from happening again, it could be said that the OCU has already won the case, at least in terms of notoriety. At any rate, it remains now for the Spanish court to show if – and how much – privacy and data protection matter under Spanish law.

Cambridge Analytica and How Trump, Brexit and Facebook Broke Democracy (New York 2019), 317.

[44] Pursuant to a press note by OCU, *Caso Facebook: un nuevo paso hacia la compensación para todos los afectados* (2020), available at https://www.ocu.org/organizacion/prensa/notas-de-prensa/2020/facebookresolucionitaliana130120 (accessed 1 May 2020).

PROCESSING PERSONAL DATA AND THE ROLE OF CONSENT

Shaira Thobani, University of Torino

Abstract:

Consent of the data subject is one of the leading bases to process personal data. However, its role and importance are strongly limited not only by other provisions of data protection law, but also by consumer protection rules. The essay will therefore focus on these limitations, which lead to some more general reflections on the interests at stake in data processing and on the legitimacy of a market of personal data.

Keywords: Personal data, Consent, Tying practices, Consumer law

1. Introduction

It is well known that most people, when asked, do seriously care about their data. However, it is also recognised that those same people, when required to take action to protect their data, do almost nothing in that respect. This discrepancy between attitude and behaviour when it comes to privacy is usually referred to as the 'privacy paradox' [1]. The explanations given to this phenomenon

[1] A. ACQUISTI-J. GROSSKLAGS, *Privacy and Rationality in individual Decision Making* (2005) 3(1) *IEEE Security & Privacy*, 26; S. KOKOLAKIS, *Privacy Attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon* (2017) 64 *Computers & Security*, 122; L. GATT-R. MONTANARI-I.A. CAGGIANO, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali* (2018) *European Journal of Privacy Law & Technologies*, <http://www.ejplt.tatodpr.eu/Article/Archive/index_html?idn=2&ida=29&idi=-1&idu=-1> accessed 17 February 2020; N. GERBER-P. GERBER-M. VOLKAMER, *Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior* (2018) 77 *Computers & Security*, 226.

are mainly related to the lack of information and cognitive biases of data subjects who, on the one hand, do not have access to all the relevant information regarding their data that would allow them to take an informed decision and, on the other hand, do not have the means to process the information they are given [2]. Moreover, the data subjects who consent to the processing of their information usually lack a clear perception of the value of such data and do not suffer from negative consequences that they can easily trace back to the processing. As a consequence, an individual confronted with the decision either to click on "I consent" or to read the privacy policy of a website will mostly prefer the former.

Notwithstanding this empirical evidence, the consent of data subjects is one of the main bases for processing personal data. Under the General Data Protection Regulation 679/2016 (as under previous directive 95/46/EC) processing is lawful if, among other conditions, "the data subject has given consent to the processing of his or her personal data for one or more specific purposes". Consent is not the only basis to lawfully process data. It is, however, the broadest one, as the other conditions require the processing to be undertaken for specific reasons while consent can be asked to process data for any purposes. Indeed, the widespread practice of requesting consent also seems to suggest that consent is one of the most commonly used bases for processing personal data. In practice, this may be related to the uncertainty surrounding some of the other bases for processing data, such as the legitimate interest clause: as this clause is not clear as to what amounts and what does not amount to a legitimate interest, controllers tend to ask for consent to ensure that the processing is lawful.

In spite of the importance attributed to consent, there are however other provisions that downsize its role. As we shall see in the following paragraphs, some of these limits stem from data protection law itself and others from consumer protection law. The role of consent shall therefore be assessed bearing in mind these restrictions.

2. The role of consent under data protection law

The GDPR itself, while putting consent in a prominent position on the one hand, does not seem to fully trust its suitability to protect the interests involved in data protection on the other. In the first place, it compels the controller to put in place certain measures to protect the interests affected by data processing even if the data subject has consented to the processing. In the second place, it

[2] D.J. SOLOVE, *Privacy Self-Management and the Consent Dilemma* (2013) 126 *Harvard Law Review*, 1880.

strictly regulates consent, prescribing it to meet stringent requirements. Finally, it excludes that in some cases the processing can be based on individual consent.

Firstly, in any case, even if the data subject has lawfully consented to the processing, the controller must not only put in place adequate security measures to preserve the integrity of the collected data, but he is also required to limit the risks deriving from the processing. The controller must indeed evaluate those risks and in certain cases perform a data protection impact assessment (art. 35 GDPR); if risks are serious and cannot be minimised, the controller shall stop *tout court* the processing. This clearly demonstrates that the processing, even if it has been consented to, may still be harmful: not only because individual consent is not completely reliable considering the cognitive biases affecting data subjects, but also because the risks in question concern not only the individual, but society more in general. As is well known, data protection regulation was born to address the risks stemming from technological development regarding, for instance, social control, discrimination, surveillance, social conformity, segregation and exclusion of minorities. These risks have a collective dimension and therefore cannot be tackled by individual consent only [3]. Therefore, consent does not exempt controllers from evaluating and minimising those risks.

As regards the requirements of consent, consent must be "freely given, specific, informed and unambiguous" (art. 4, lett. 11). Leaving aside for now the requirement of freedom of consent, the aim of the other requirements is doublefold. Firstly, it is to promote awareness of the existence and of the scope of the processing by the data subject: the data subject shall be aware that they are consenting to the processing (consent must be unambiguous) and they shall be aware of what they are consenting to (consent must be informed). The second aim is to limit what controllers can do with the data: even if the data subject consents, their consent shall not be too broad but must be referred to a specific purpose (consent must be specific).

Finally, consent cannot always be used as a legitimate basis for processing personal data: more precisely, consent cannot be invoked if the circumstances prevent it from being freely expressed. It is therefore necessary to examine the requirement that consent is *freely* given, as provided for by the GDPR. According to the Art. 29 Working Party, freedom of consent "implies real choice and control for data subjects", in the sense that "if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not

[3] A. MANTELERO, *Personal data for decisional purposes in the age of analytics: From and individual perspective to a collective dimension of data protection* (2016) 32 *Computer Law & Security review*, 238.

consent, then consent will not be valid"[4]. Therefore, for consent to be free, the data subject must have a real choice whether to give it or not. What does it mean to have a *real choice*?

In the first place, the choice is not *real* if there is a qualified imbalance of power between the controller and the processor[5]. This is the case, for instance, of public authorities or employers, who cannot rely on consent to process personal data of citizens or employees if they take advantage of their position to obtain consent. Therefore, an employer cannot ask its employees to consent to the processing of their personal data as a condition to continue being employed (provided, of course that those data are not necessary to perform the job, e.g. the work telephone number to call the employee when he is on duty: in this case the employer is entitled to process the data without the employee's consent). Another example could be that of hospitals or other healthcare facilities, which cannot ask patients to consent to the processing of their data as a condition to provide health care (here as well, provided that the data are not necessary to that end).

In the second place, the choice is not real if the data subject is forced to give consent in the sense that they do not have an alternative in order to have access to a good or service[6]. This is the issue of the so called *tying* practices, in which someone who provides a good or service makes the performance conditional on the users' consent to the processing of their personal data that are not necessary for the performance of the required service. Tying practices are at the core of the pervading business model of offering services for free (in the sense that no monetary price is asked in return) but upon request of personal data. Especially (but not only) in the online world, many services are offered provided that the users communicate some of their personal data when registering to the service and accept that the data generated while using the service are tracked and used by the service provider or by third parties.

Are tying practices prohibited by data protection legislation? The GDPR gives a nuanced answer, providing that "[w]hen assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of a contract" (art. 7, para. 4). Thus the GDPR does not prescribe a blanket prohibition, but states that tying consent to the processing to the performance of a contract shall be taken in "utmost account" when assessing the validity of con-

[4] Article 29 Working Party, *Guidelines on consent under Regulation 2016/679* adopted on 28 November 2017 as revised on 10 April 2018, WP259 rev.01, 5.

[5] *Ibidem* 6-7.

[6] *Ibidem* 8-10.

sent. To understand what this means it is useful to go back to the recommendations of the Art. 29 Working Party that the data subjects have a real choice. As said, there is no real choice if the data subject does not have an alternative to access a good or service without consenting to the processing of their personal data.

An alternative surely exists if the service provider offers two versions of the same service, one for free but asking users to consent to the processing of their data, and the other one without asking for consent [7]. In the latter case, the service provider can ask for a fee to use the service, provided, of course, that the price is reasonable: if the price were disproportionate to the service, users would not have a real choice not to consent to the processing.

The problematic question is whether an alternative exists if an equivalent service is offered on the market by another provider, who does not ask for consent to data processing. The Art. 29 Working Party denies this possibility [8] and some data protection authorities across Europe have taken a similar position as well [9]. The wording of art. 7 GDPR (which, as said, does not prescribe a blanket prohibition) suggests however a more flexible interpretation. Indeed, it seems reasonable to argue that if users are able to access an equivalent service without having to consent to the processing of their personal data, they do have a real choice [10]. Of course, the service must be equivalent: this excludes that those who offer a service in a quasi-monopolistic position (such as, e.g., Facebook and Google) can legitimately ask users to consent to the processing as a condition to use the service.

To summarise, data protection law restricts the role of consent by compel-

---

[7] *Ibidem* 9.

[8] *Ibidem* 9-10.

[9] See, e.g., the position of the Italian data protection authority (*Garante per la protezione dei dati personali*) in *Linee Guida in materia di attività promozionale e contrasto allo spam*, decision 4.7.2013, 330 and of the French authority (*Commission nationale informatique & libertés*), in *Projet de recommandation sur les modalités pratiques de recueil du consentement prévu par l'article 82 de la loi du 6 janvier 1978 modifiée, concernant les opérations d'accès ou d'inscription d'informations dans le terminal d'un utilisateur (recommandation «cookies et autres traceurs»)* 14.1.2020, art. 3. Instead, the British Information Commissioner's Office has taken a more nuanced position: while it recommends "that organisations do not make consent to marketing a condition of subscribing to a service unless they can clearly demonstrate how consent to marketing is necessary for the service and why consent cannot be sought separately", it also stresses that it must be considered "whether there is a choice of other services and how fair it is to couple consent to marketing with subscribing to the service"; (*Direct marketing guidance*, version 2.3 of 6 March 2018, para. 66).

[10] This is the position taken by the first Italian court decision on the issue: Cass. 2.7.2018, 17278, in *Giur. It*., 2019, 3, 530, according to which tying practices are banned only when the service has no equivalents and is indispensable.

ling the controller to protect otherwise the rights and interests affected by the processing, by prescribing strict consent requirements and by excluding that in certain cases the processing of personal data can be based on consent. It is important to underline that it is one thing to provide for strict consent requirements, asking for consent to be unambiguous, informed and specific, and another thing to require that consent is free in the sense of limiting the possibility to base the processing on consent. In the first case, consent can be used as a legitimate basis for processing (and, therefore, data can be processed) provided that all information is given, that the data subject is aware of the processing and that the processing is limited to specific purposes. In the second case, the only way to abide by the requirement of freedom of consent is not to ask for it: as a consequence, in the absence of other conditions for the processing, data cannot be processed. The requirement of freedom of consent is therefore used as a way to limit the collection of personal data.

3. The role of consent under consumer law

In the previous paragraph we considered the limits to the role of consent from a data protection perspective. However, as consent to the processing of personal data is often asked for when offering a good or service, data subjects are at the same time consumers taking part in economic transactions and, as such, the role of their consent should also be evaluated from a consumer protection law perspective. There is no doubt that these are economic transactions, notwithstanding that in many cases the services in question are offered "for free": the economic value of personal data is well known and these services are offered without charging a fee precisely because there is an economic advantage deriving from the data collected when providing the service [11].

The European Commission has taken a stance on the issue, clarifying that data processing, together with advertising, often constitutes the main source of revenues of "data-driven business structures", as "[p]ersonal data, consumer preferences and other user generated content, have a 'de facto' economic value and are being sold to third parties". As a consequence, "if the trader does not inform a consumer that the data he is required to provide to the trader in order to access the service will be used for commercial purposes, this could be consid-

[11] While it is undisputed that personal data have economic value, doubts have arisen on how to measure it: see, eg, Organisation for Economic Co-Operation and Development, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value* (2013) *OECD Digital Economic Papers*, 220; G. MALGIERI-B. CUSTERS, *Priving privacy - the right to know the value of your personal data* (2017) 34 *Computer Law & Security Review*, 289, 294-297.

ered a misleading omission of material information" under directive 2005/29/EC (Unfair Commercial Practices Directive), especially under art. 7, para. 2 concerning misleading omissions [12]. The issue is one of transparency: traders cannot advertise their services as free if they ask for personal data in return for using the service. In order to abide by consumer protection law, it is therefore necessary to openly disclose the purposes for which consent to personal data protection is required and to make it clear to consumers that such purposes have an economic nature.

Transparency requirements under consumer protection law lead to a result that is partially similar to what is achieved applying data protection law [13]. The GDPR requires consent to be informed: this amounts to saying that service providers must be transparent to users on the use they make of the collected data. From a consumer protection point of view, the commercial practices shall be transparent while, from a data protection perspective, the data subjects' consent shall be informed: the result is the same, i.e. to clearly inform consumers/data subjects on the purposes and scope of the processing.

Consumer protection law also takes into consideration consent to data processing from another point of view. As said, providing a service asking not for a monetary price but for the consent to process personal data amounts to an economic transaction. Therefore, if consumers are involved, they deserve the protections provided for by consumer law for economic transactions. This aspect has been clarified by the European legislator in the recent Directive (EU) 2019/779 on certain aspects concerning contracts for the supply of digital content and digital services, which applies not only when the consumer "pays or

---

[12] European Commission, *Guidance on the implementation/application of Directive 2005/29/EC on unfair commercial practices* SWD (2016) 163 final, 25.5.2016, 23-25. See also Case AT.39740, Google Search (Shopping), European Commission, 2017, 4444 final, decision of 27.6.2017, para. 158. The Italian competition authority has sanctioned this practices as unfair commercial practices: see, lastly, Case Facebook - condivisione dati con terzi, Autorità garante della concorrenza e del mercato, 29.11.2018, 27432 (the decision was later partially reversed by TAR Lazio, 10.1.2020, 260, that, however, confirmed that traders shall be transparent on the economic value of the consumers' data they collect).

[13] On the intertwines between personal data and consumer protection law see M. ROHEN, *Beyond consent: improving data protection through consumer protection law* (2016) 5(1) *Internet Policy Review*, <https://policyreview.info/node/404/pdf> accessed 17 february 2020; A. DE FRANCESCHI, *La circolazione dei dati personali tra* privacy *e contratto* (Napoli 2017), 101 ff.; N. VAN EIJK-C.J. HOOFNAGLE-E. KANNEKENS, *Unfair Commercial Practices: A Complementary Approach to Privacy Protection* (2017) 3 *European Data Protection Law Review,* 325; M. GRAZIADEI, *Collusioni transatlantiche: consenso e contratto nel trattamento dei dati personali*, in F. DI CIOMMO-O. TROIANO (eds.), *Giurisprudenza e autorità indipendenti nell'epoca del diritto liquido. Studi in onore di Roberto Pardolesi* (Piacenza 2018), 367; C. GOANTA-S. MULDERS, *Move Fast and Break Things: Unfair Commercial Practices and Consent on Social Media* (2019) 8(4) *Journal of European Consumer and Market Law*, 136.

undertakes to pay a price", but also when the consumer "provides or undertakes to provide personal data to the trader, except where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content or digital service" (art. 3) [14]. In both cases, consumers are entitled to the rights and remedies provided for in the Directive. The European legislator is careful to specify that this does not amount to considering personal data as a commodity that can be traded in return for a service [15] (instead, the extent to which this is legitimate is regulated, as we have seen, by data protection law), but only prescribes that, if in practice it happens that data are used for that purpose, then consumers shall be protected as if they had paid a price.

Summarising, consumer law tells us that, when consent to the processing of personal data is asked in the context of economic transactions, then consent shall be asked in a transparent way and data subjects are entitled to consumer protection. But consumer protection law cannot go beyond ensuring transparency and fairness in the processing. If the terms and conditions are clear enough and if consent is not acquired with unfair commercial practices, then consumers' consent to data processing can be legitimately asked. Instead, as we have seen, data protection law goes further in limiting the role of consent, excluding that under certain circumstances consent can be used as a legitimate basis to process data. Consumer law cannot go that far because, as it has developed in Europe, it cannot interfere with the economic content of market transactions: provided that the terms and conditions are clear and that consumers' choices have not been unduly influenced by unfair commercial practices, the "adequacy of the price and remuneration" is not subject to scrutiny (art. 4, para 2, Directive 93/13/EEC on unfair terms in consumer contracts). As we have seen, consumer law itself qualifies consent to the processing of personal data as a *de facto* remuneration, in order to protect consumers by ensuring the transparency of tying practices and by granting them remedies. By qualifying consent as a remuneration, and thus recognising its direct relevance for the economic content of the contract, it is excluded from scrutiny under consumer protection law. Instead, it is the task of data protection law to limit the role of consent and to prescribe when it can or cannot be used to collect data.

If consumer protection law does not allow a scrutiny on the economic conditions of the transactions in which personal data are involved, some doubts have

[14] On the issues raised by the Directive see A. DE FRANCESCHI (ed.), *European Contract Law and the Digital Single Market* (Cambridge 2016).

[15] Whereas 24 of the Directive. This clarification follows the concerns raised by the European Data protection Supervisor on the use of personal data as counter-performance: *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, 14.3.2017, 6-11.

been raised on whether it is possible to perform such a scrutiny under competition law. The question has emerged as an issue of abuse of dominant position: can a company with market dominance ask its users to consent to the processing of their personal data as a condition to access the service? [16] Here, once again, the answer seems to be negative, at least as argued by the German court, that for first in Europe addressed this specific issue [17]. Indeed, even if it is taken for granted that a dominant undertaking cannot ask for consent because consent would not be free (as users as have no other option to access an equivalent service without consenting to the processing) under data protection law, this does not imply that this conduct impairs competition and therefore needs to be sanctioned under competition law as well. Firstly, such sanction only applies if it is demonstrated that the business model of asking for data in return for a service would not be adopted in a competitive market: it is fully possible that such a business model is so widespread because of the cognitive limitations of data subjects and has nothing to do with the abuse of a dominant position. Secondly, because it needs to be demonstrated that this conduct has a negative effect on competition: if, on the one hand, users are not prevented from using other services as a result of the request to consent to the processing of their data and, on the other hand, other businesses are not prevented from collecting personal data themselves, then this does not seem to be the case. In other words, if a dominant undertaking infringes the law, this infringement will be relevant under the body of law in question, but it will not necessarily amount to a competition problem. It remains to be seen how the issue will be addressed by other European authorities and judges.

4. Conclusions

Having briefly seen the limits to the role of consent stemming from different sources, we can return to some general remarks on the role of consent to the processing of personal data.

---

[16] The question was given a positive answer by the German competition authority: Case B6-22/16, Bundeskartellamt, 6.2.2019. However the decision was later reversed by Case VI-Kart 1/19 (V), OLG Düsseldorf, 26.8.2019. The case regarded Facebook's data policy, which the Bundeskartellamt found abusive in the part that made the use of the social network conditional upon users' extensive consent to process the personal data generated while using external services.

[17] Case VI-Kart 1/19 (V), OLG Düsseldorf, 26.8.2019. On the matter see R. PODSZUN, *Regulatory Mishmash? Competition Law, Facebook and Consumer Protection* (2019) 2 *Journal of European Consumer and Market Law*, 50; G. COLANGELO, *Facebook and the Bundeskartellamt's Winter of Discontent* (2019) *Competition Policy International*, <https://www.competitionpolicyinternational.com/facebook-and-bundeskartellamts-winter-of-discontent/> last accessed 17 February 2020.

Firstly, why, in spite of the aforementioned limits, does the European legislator still give it such a prominent role? A possible reason of the importance attributed to consent may lie in the way data protection has evolved in Europe. The right to the protection of personal data has been developed in the fundamental rights scenario and has been framed as a fundamental right by the UE charter of fundamental rights (art. 8)[18]. The European legislator has therefore shaped data protection as the subject of an individual right, thus drawing it to the realm of personality rights, which are, indeed, rights of the individual person. The underlying assumption is that data pertain to the individual they refer to and, therefore, individual consent is needed to process them. In other words, even without adopting an outright proprietary model with regard to personal data, if the protection of personal data is the subject of an individual right, then the consent of the right's holder is necessary for intrusions to be legitimate and, therefore, for the data to be processed.

Secondly, as we have seen, in spite of this importance, the European legislator is well aware of the weak effectiveness of consent to protect the interests involved in data processing and thus sets forth strict limits to the role of consent. What are the reasons of these limitations? At first sight, the reason lies in the protection of the individual data subject or consumer. This can be read as a response to the privacy paradox: as data subjects have limited rationality when it comes to protecting their data, the law steps in to protect the individual, both by providing for conditions of transparency and, in some cases, by limiting *tout court* the processing. Under this perspective, consent is not adequate because the individuals are not in the condition to give a fully aware consent. However, there is also another reason why consent is limited, which has to do, not with the protection of the individual, but with the protection of society. As we have seen, in some cases consent (even if it is fully informed, specific and there is no qualified power imbalance) cannot constitute a legitimate basis for processing, meaning that data cannot be processed: this is the case when there is no alternative to access an equivalent good or service. This leads to a direct limitation to consent, but indirectly it limits the possibility to process data in itself. The purpose of such a limitation is not only the protection of the individual (who is usually not directly affected by the processing of big data), but is the protection of society from the risks that the mass processing of personal data poses to the community: as mentioned, these are indeed the main risks that data protection

[18] S. RODOTÀ, *Data Protection as a Fundamental Right*, in S. GUTWIRTH-Y. POULLET-P. DE HERT-C. DE TERWANGNE-S. NOUWT (eds.), *Reinventing Data Protection* (Berlin 2009), 77; M. TZANOU, *Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right* (2013) 3(2) *International Data Privacy Law*, 88; G. GONZALEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Berlin 2014).

regulation at first intended to address. Under this perspective, consent (even if it is given by someone who is perfectly aware of what they are doing) should have no role as the interests at stake are not those of the individual. Individual consent is just not the right tool to address these issues because under this perspective the aim is to limit the collection of data in order to protect society more in general.

It can be doubted, however, that limiting personal data processing under data protection law is always the right tool to address all of these problems. Taking the example of discrimination (which is one of the main risks associated with data protection), if we fear that data processing could lead to discriminate parts of society, it is clear that the decisions regarding the processing cannot be left to the consent of individual data subjects. However, it can be doubted that data protection law is the right tool to address the issue. If the aim is to prevent discrimination, it is necessary in the first place to specify what the discriminatory results to forbid are: however, this is the domain of anti-discrimination law, not of data protection law. Put another way, if the aim is to prevent discrimination, using data protection law to limit the collection of personal data risks to lead to a blanket prohibition to the processing and prevents a transparent discussion on what are the discriminatory results to forbid. Therefore not only the role of consent, but also the role of data protection law should be reassessed considering whether other bodies of law are better suited to address the risks stemming from data processing.

This leads to a final conclusion. When assessing the role of consent, it should always be borne in mind what the protected interests are and what the final results that the limits to the role of consent lead to. The debate on the role of consent often focuses on whether it amounts or not to a contract and, therefore, on whether data can be considered as a tradeable commodity that can circulate by means of the data subjects' consent [19]. Due to reasons that regard not only the protection of individuals, but the protection of society more in general, the legislator can decide to forbid the "trade" of personal data by limiting the role of consent and prohibiting tying practices. This prohibition can be read as a means to protect the fundamental right to data protection. Under this perspective there is no space for consumer and competition law, which need a market to

[19] On the issue of using personal data as counter-performance see C. LANGHANKE-M. SCHMIDT-KESSEL, *Consumer data as consideration* (2015) 6 *Journal of European Consumer and Market Law*, 218; A. DE FRANCESCHI, *La circolazione dei dati* (fn 13) 67 ff.; A. METZGER, *Data as Counter-Performance: What Rights and Duties do Parties Have?* (2017) 8 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 1; G. RESTA-V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. e proc. civ*., 2018, 411, 436 ff.; V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno,* in *Il diritto dell'informazione e dell'informatica*, 2018, 4-5, 689.

regulate, as, simply put it, there is not market (as a market of personal data is forbidden). However, data protection law aims at protecting not only the fundamental right to data protection, but also the free movement of personal data (art. 1, GDPR): excluding from this protection the processing of data for economic purposes (and, therefore, the possibility to develop a market of personal data) would mean to exclude a significant part of the interests that the free movement of personal data refers to. Indeed, the GDPR does not clearly forbid tying practices (art. 7, para 4) and this is not by chance: the rule in question was widely discussed during the preparatory works and a previous proposal providing for a blanket prohibition was discarded [20]. Therefore, as data can be traded (even though under the limits that we have previously seen), consumer and competition protection problems do arise and cannot be ignored: it is for the benefit of data subjects/consumers to acknowledge this openly and to put in place the necessary safeguards. Instead of denying the existence of a market which the law does not forbid, it is better to regulate it using all the available and relevant tools.

[20] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Draft Report 17 December 2012, 2012/0011(COD), amendment no 107, where the Parliament proposed to add the following para. to art. 7: "The execution of a contract or the prevision of a service may not be made conditional on the consent to the processing or use of data that is not necessary for the execution of the contract or the provision of the service pursuant to Article 6(1)(b)". The position expressed in this work is not however commonly accepted at the European level: the Art. 29 Working Party firmly excludes that data can be used as a counter-performance to access a good or service: *Guidelines on consent* (fn 4) 8. See also, in the same direction as the Working Party, J.P. ALBRECHT, *The EU's New Data Protection Law - How a Directive Evolved Into a Regulation* (2016) 17(2) *Computer Law Review International*, 33, 36.

GDPR AND THE RIGHT TO BE FORGOTTEN

Marco Rizzuti, University of Florence

Abstract:

The paper deals with the EU case-law about the right to be forgotten, enshrined also in article 17 of the GDPR, and compares its developments with some trends at domestic level.

Keywords: Oblivion, Balancing, Information.

1. Historical Remarks

Forgetting, or in more learned words oblivion, has always been something of great anthropological importance. The wish to forget traumatic events has always been a powerful driver of human behaviour at both the individual and the societal level, since the most remote antiquity [1]. In the Greek mythology Oblivion was even a goddess, the famous *Λήθη* [2].

[1] We know about ceremonies performed in primitive societies in order to establish a collective forgetting: see D. BATTAGLIA, *At Play in the Fields (and Borders) of the Imaginary: Melanesian Transformations of Forgetting* (1993) *Cultural Anthropology*, 430-442. With regard to the philosophical and anthropological aspects of memory and forgetting see A. ASSMANN, *Formen des Vergessens* (Göttingen 2016) and F. CIMATTI, *La fabbrica del ricordo* (Bologna 2020).

[2] According to T. HESIOD, *Theogony*, (Harmondsworth 1973) 225-226, Lethe was one of the dreadful daughters of Eris (the personification of Strife), and so a granddaughter of Night and Chaos. Lethe was also the name of one of the underworld rivers, and the shades of the dead drank its waters in order to forget their earthly life and so to be ready for reincarnation (PLATO, *Politeia* (Leiden 1989), 621; VIRGIL, *Aeneid* VI (London 1906), 713-715), or, in the later Christian versions, to be ready for Paradise (D. ALIGHIERI, *Purgatory*, XXVIII, 126-130). See also H. WEINRICH, *Lethe: Kunst und Kritik des Vergessens* (München 1997).

More specifically, humans have always tried to govern through legal instruments the unpleasant consequences of new technologies that seemed to render possible a perpetual survival of some information that could be unwelcome to those in power, or anyway destabilizing for the society. Therefore, ancient legislators ordered the systematic destruction of monuments, when the new potentially dangerous techniques were sculpture and engraved inscriptions [3], and then ordered the burning of books, when press played such a role in its turn [4].

In other interesting cases through the centuries, provisions that forbade to remember recent events were enacted in order to extinguish past hates at the end of civil wars [5], or in the attempt to avoid new conflicts [6], and with the aim to grant a peaceful transition from dictatorship to democracy [7].

---

[3] Many relevant cases are reported by J. ASSMANN, *Das kulturelle Gedächtnis: Schrift, Erinnerung und politische Identität in frühen Hochkulturen* (München 1992) and N.N. MAY (ed.), *Iconoclasm and Text Destruction in the Ancient Near East and Beyond* (Chicago 2012), including the Egyptian attempts to destroy any memory of Hatshepsut, the woman who dared to proclaim herself Pharaoh, and then of Akhenaton, the heretic monotheist Pharaoh. E. VARNER, *Mutilation and Transformation: Damnatio Memoriae and Roman Imperial Portraiture* (Boston 2004), shows that also in Rome the destruction of imperial monuments was usually ordered after the deposition of an emperor or of a dynasty, but sometimes the same monuments were also restored after new changes of circumstances. Similar practices went on during the Middle Ages against the monuments of antipopes and of excommunicated sovereigns; see L. SANFILIPPO-A. RIGON (eds.), *Condannare all'oblio: pratiche della Damnatio Memoriae nel Medioevo* (Ascoli Piceno 2010).

[4] The historical examples are innumerable, from the Savonarola's *Falò delle vanità* to the Inquisition's *Index librorum prohibitorum* or the Nazi *Bücherverbrennungen*, and so on: see, also for other references, R. KNUTH, *Burning Books and Leveling Libraries: Extremist Violence and Cultural Destruction* (Westport 2006); L.X. POLASTRON, *Livres en feu. Histoire de la destruction sans fin des bibliothèques* (Paris 2004); P. BATTISTA, *Libri al rogo. La cultura e la guerra all'intolleranza* (Milan 2019).

[5] In 403 BC, after the civil war between the followers of the democratic leader Thrasybulus and those of the oligarchy of the Thirty Tyrants, an agreement was reached in Athens and death penalty was imposed on people who dared to "*μνησικακεῖν*" the strife of the recent past (ARISTOTELES, *De Republica Atheniensium*, 39.6 and 40.2). After a couple of millennia, in 1598 AD, the French Wars of Religion were ended by King Henry IV of Bourbon with the Edict of Nantes that contained a specific prohibition to "*renouveler la mèmoire*" of what had happened. Both cases are discussed by S. RODOTÀ, *Il diritto di avere diritti* (Bari 2012).

[6] In 44 BC a few days after the death of Caesar in Rome, his followers leaded by Marc Anthony and the conspirers defended by Cicero reached a compromise: the acts of the assassinated dictator would have remained valid, but his murderers would have been protected by a "*αμνηστία*", whose Greek literal meaning is precisely the denial of memory (see S. MAZZARINO, *L'impero romano* (Bari 1998), I, 40-41). But the agreement did not last, and the final outcome was inspired by a totally different approach to memory: Octavianus chased for years the killers of his divinized adoptive father all over the ecumene, and then dedicated the temple built in his new Forum to *Mars Ultor*, the Avenger God.

[7] In Spain all political parties accepted the so called *Pacto del Olvido* (meaning: "agreement of oblivion") after the end of the Francoist dictatorship in 1975. Only after the approval of the *Ley de Memoria Històrica* of 26 December 2007, the situation has changed.

Today internet and search engines are the new technologies that promise a (seemingly) permanent preservation of information [8], while each and every single individual is now considered as a sovereign on his/her own personal data.

Therefore, people ask for, and often judges do order, the cancellation of information that are not defamatory nor false [9], neither reserved [10], but true and originally published in a fully legal manner, because such data are now considered as not consistent with the current personal identity of the concerned individual. This is, indeed, the exact legal rationale of the right to be forgotten, as a right pertaining to the fundamental value of free self-identification [11].

At the European level the existence of such a right has been recognized by the Court of Justice in the well-known decision on the Google Spain case [12], has then been elaborated in specific Guidelines [13], and is now enshrined in article 17 of the General Data Protection Regulation [14].

---

[8] Indeed, it could be just an illusion, given that the obsolescence of electronic supports is much faster than that of the more traditional ones: see L. RUSSO, *La rivoluzione dimenticata* (Milan 2001), 433. In fact, today we are still able to read ancient manuscripts in the libraries and engraved inscriptions in the monuments of our historical cities, but everyone has experienced that it is practically impossible to accede the information stored in floppy disks and CD-ROMs of a few years ago, or saved with a software version that is not compatible with the last updated one.

[9] Legal protection of the rights to honour and reputation against defamatory information dates back, at least, to Roman times, and defamation is considered as a crime in modern legal systems. But today private law remedies, such as civil liability, are provided also to protect the right to personal identity against the circulation of merely false information, given that "*The false light need not necessarily be a defamatory one*" (W.L. PROSSER, *Privacy* (1960) *California Law Review*, 383-423 and in particular 398).

[10] The protection of privacy as the "*right to be let alone*" dates back to S. WARREN - L. BRANDEIS, *The Right to Privacy* (1890) *Harvard Law Review*, 193-220. In the European framework it found a legal basis in article 8 of the Convention on Human Rights of 1950: e.g., its first recognition in the Italian Supreme Court case-law was grounded by Cass. 27.5.1975, 2129, the famous Soraya case, precisely on a direct application of article 8 to the domestic legal system. Today, the protection of personal data has been strongly enhanced by recent, European as well as internal, statutory acts, including, last but not least, our GDPR.

[11] See, for further references from different countries, F. WERRO (ed.), *The Right To Be Forgotten. A Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas, and Asia* (Cham 2020).

[12] We refer to the Case C-131/12, Google Spain v Google, ECJ, 13.5.2014. See, also for other references, S. PIETROPAOLI, *La rete non dimentica. Una riflessione sul diritto all'oblio*, in *Ars interpretandi*, 2017, 1, 67-80.

[13] The Guidelines were elaborated by the Article 29 Data Protection Working Party, composed by the Data Protection Authorities of all EU Member States, and were adopted on 26 November 2014.

[14] We refer to EU Regulation 2016/679 of 27 April 2016, in force since 25 May 2018. Its article 17 states that: "*1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the*

2. EU Law Impact on Domestic (Italian) Law

If we look at such developments from an Italian Law point of view [15], we have to notice that, quite interestingly, the most relevant European impact on the internal legal system has concerned not the recognition of the right to be forgotten, already admitted by domestic case-law, but the recognition of its limits, with particular regard to the respect for the competing rights to free information and to free historical research. Indeed, in a first moment internal judges had almost neglected such issues, but the European interventions sensitized them to consider the need for a balance with these other fundamental rights.

In fact, in the recent past, some famous Italian judicial decisions had recognized right to oblivion in a wide sense to a known politician under investigation

---

obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1). 2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data. 3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: (a) for exercising the right of freedom of expression and information; (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3); (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or (e) for the establishment, exercise or defence of legal claims".

[15] About the Italian perspective on article 17 of GDPR see, also for other references: D. BARBIERATO, *Osservazioni sul diritto all'oblio e la (mancata) novità del regolamento UE 2016/679 sulla protezione dei dati personali*, in *Responsabilità civile e previdenza*, 2017, 6, 2100; A. THIENE, *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio*, in *Nuove leggi civili commentate*, 2017, 2, 410; R. SENIGAGLIA, *Reg. UE 2016/679 e diritto all'oblio nella comunicazione telematica. identità, informazione e trasparenza nell'ordine della dignità personale*, in *Nuove leggi civili commentate*, 2017, 5, 1023; F. DI CIOMMO, *Diritto alla cancellazione, diritto di limitazione del trattamento e diritto all'oblìo*, in V. CUFFARO - R. D'ORAZIO - V. RICCIUTO (eds.), *I dati personali nel diritto europeo* (Turin 2019), 353-396.

for corruption [16] and to a former terrorist [17]. But soon after Google Spain in quite similar cases a right to be forgotten has been denied, because of the public function exercised by the applicant [18] or because of the historical relevance of the concerned events [19]. Indeed, we could say that, thanks to the European influence, these later judgements have rediscovered some important limits on the right to be forgotten [20], that are indeed granted also by the fundamental principles of the internal legal system, both at the constitutional level [21] and in important developments of ordinary legislation [22].

---

[16] Cass. 5.4.2012, 5525, in *Guida al diritto*, 5, 44: a former socialist politician, who had been under investigation for corruption during the famous "*Tangentopoli*" (meaning something like "Bribesville") scandal and had been acquitted, was trying to restart a new political career but the news concerning the investigations were still online in the informatic archive of "*Corriere della Sera*", a prominent Italian newspaper; therefore, he obtained a judicial injunction ordering the newspaper to modify the archive, with a link to the updated news concerning the successive acquittal.

[17] Cass. 26.6.2013, 16111, in *Foro italiano*, 2013, 9, I, 2442: a former far left extremist, who had been a member of the terroristic organization "*Prima Linea*" and had already served his sentence in jail, obtained compensation against a local newspaper that had republished news concerning his troubled past.

[18] First Instance Tribunal of Rome, 3.12.2015, in *Il Quotidiano giuridico*: the applicant asked de-indexation with regard to his involvement in a criminal law proceeding, where he had never been sentenced, but the judge rejected the application also because the applicant, being a practicing lawyer enrolled in a public register, has no right to be forgotten in accordance with criterion n. 2 of the above-mentioned Guidelines of the Article 29 Data Protection Working Party, which excludes all persons who "*play a role in public life*". The difference with the case of 2012 is evident: the role in public life played by a politician involved in a corruption scandal is indeed much more relevant!

[19] Italian Authority for Data Protection, 31.3.1998, 152: a former far right extremist who had committed crimes of terrorism and had already served his sentence in jail, asked for de-indexation with regard to his troubled past, but the Authority rejected his application because, also in the light of criterion n. 13 of the Guidelines of the Article 29 Data Protection Working Party, the public interest to access information about his serious crimes, connected to a very relevant page of Italian recent history, has to prevail. Of course, we cannot accept to ground the distinction between this case and that of 2013 on a different evaluation of far right and far left terrorism, and so we have to recognize again a relevant impact of the European limits on the exercise of the right to be forgotten. See M. RIZZUTI, *Il diritto e l'oblio*, in *Corriere giuridico*, 2016, 8/9, 1077-1082, also for further references to Italian legal literature at these regards.

[20] The mentioned decisions still made reference to the Guidelines of the Article 29 Data Protection Working Party, but also the new article 17 of GDPR expressly confirms that right to be forgotten is limited by both freedom of information (paragraph 3, letter a) and historical research (paragraph 3, letter d). In fact, more recent Italian decisions, such as Cass. 27.3.2020, 7559, and Cass. 19.5.2020, 9147, have directly grounded on article 17 of GDPR the need to balance the right to oblivion with the competing rights to memory and to free press.

[21] In the Italian Republican Constitution of 1948 free press and freedom of information are protected by article 21, while the freedom of scientific research is protected by article 33.

[22] In the last years many legislative interventions have been enacted in Italy aiming at protecting against oblivion the historical memory of relevant tragic events, such as: the *Shoah* (with the Act of

We need to distinguish different legal aspects: if a politician has been acquitted from charges of corruption, he/she must be free to restart a political career but the public must be free to know about his/her past involvement in scandals; if a person involved in tragic historical events has already served his/her sentence, he/she must be free from any other sanction but historians must be free to do research and the descendants of the victims must be free to preserve their memory [23].

In a quite similar way, a need for distinction and for a reasonable balance is emerging with regard to parental anonymity (that is something analogous to oblivion): if, in order to disincentivize abortion, the biological mother is allowed to obtain anonymity after childbirth, this means that the child has no right to establish a legal parental relationship nor to claim for maintenance and inheritance, but it must not imply also the denial of any possibility to access to information about genetic ancestry for health-related reasons or for other relevant reasons [24].

---

20 July 2000, 211), the Istrian-Dalmatian Exodus (with the Act of 30 March 2004, 92), and precisely Terrorism (with the Act of 4 May 2007, 56). The trend is going on with the legislation against the crime of negationism (Act of 16 June 2016, 115), and with other interventions to protect the memory of the victims of migration (Act of 21 March 2016, 45) and of mafia (Act of 8 March 2017, 20). Moreover such a trend is not isolated and similar initiatives can be reported also in other legal systems, with regard to the memory of: the *Holodomor* (with the EU Parliament Resolution of 23 October 2008) and other crimes of Communism (with the EU Parliament Resolution of 19 September 2019), the Slave Trade (with the French Act of 21 May 2001, 434), the *Medz Yeghern* (with the French Act of 29 January, 2001, 70, and the German *Bundestag* Resolution of 2 June 2016), the Native American Genocide (with, e.g., the Venezuelan Decree of 10 October 2002, 2028), the *Seyfo* and the *Katastrophè* (with the Swedish *Riksdag* Motion of 11 March 2010, that considered them together with *Medz Yeghern*), the *Sürgünlik* (with the Ukrainian *Rada* Resolution of 12 November 2015), the Ethnic Cleansing of Circassians (with the Georgian Parliament Resolution of 21 May 2011). In many cases the concerned events are still quite controversial and provoke harsh debates, the so called "memory wars", with international tensions (e.g. between Turkey and France about *Medz Yeghern*) or internal contradictions (e.g. France also approved the Act of 23 February 2005, 158, to recognize the positive role of French colonialism). At these regards see, from different perspectives, D. RIEFF, *In Praise of Forgetting: Historical Memory and Its Ironies* (New Haven 2016); E. SJÖBERG, *The Making of the Greek Genocide: Contested Memories of the Ottoman Greek Catastrophe* (New York 2017); M. BIANCA (ed.), *Memoria versus oblio* (Turin 2019); V. PISANTY, *I guardiani della memoria e il ritorno delle destre xenofobe* (Florence-Milan 2020); M. FLORES, *Cattiva memoria. Perché è difficile fare i conti con la storia* (Bologna 2020).

[23] In some interesting cases, the national appeasement after regime changes has been pursued through an exchange between a criminal law immunity for the perpetrators of serious delicts linked to the past regime, on the one hand, and the preservation of truth and memory for the victims, on the other hand. The most renown example is represented by the Truth and Reconciliation Commission instituted in South Africa after the end of Apartheid by N. Mandela, but other relevant examples can be found in other countries of Africa, Oceania and the Americas: see, also for other references, P.B. HAYNER, *Unspeakable Truths: Facing Challenge of Truth Commissions* (New York 2010). On the other hand, in the Italian historical experience such a moment is missed, because the post-war amnesty implied also a general amnesia: see, also for other references, P. CAROLI, *Il potere di non punire. Uno studio sull'amnistia Togliatti* (Naples 2020).

[24] Case C-33783/09, Godelli, European Court of Human Rights, 25.9.2012, deemed the Italian

3. Recent Judicial Developments

The above-mentioned European trend towards a careful limitation of the right to be forgotten is confirmed also by the most recent case-law of the European Court of Justice. First of all, with reference precisely to an Italian case, the CJEU has specified that there is no room for the right to oblivion when public registers are concerned [25].

Moreover, according to recent CJEU decisions "*the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced against other fundamental rights*", so that "*there is no obligation under EU law, for a search engine operator who grants a request for de-referencing made by a data subject… to carry out such a de-referencing on all the versions of its search engine*" [26]. Interestingly, in the same days a totally different approach has been adopted by the Court with regard to the illegal publication of defamatory content, with the recognition of a judicial power to block access to that information worldwide [27]. It is therefore quite evident that, according to EU justices, the right to be forgotten has a lower rank in comparison with the protection against defamation.

On the other hand, recent domestic case-law sometimes turns out to be less convincing. In a recent case decided by the Italian Supreme Court, with regard to a journalistic reconstruction of a murder dating back to twenty-seven years ago, the justices opined that this kind of historical research is not protected by art. 21 of the

---

legislation on maternal anonymity not acceptable, because it was totally unbalanced against the child's right to information. In *obiter dictum* the Italian Constitutional Court of 10.6.2014, 162, declared that the same legal reasoning has to apply also to the anonymity of gametes' donors with regard to assisted reproductive technologies. On the other hand, Cass. 17.2.2020, 3877, has recognized an unlimited right to be forgotten with regard to the freedom of a transsexual person to choose a new name, precisely because in this case there no competing rights to be balanced.

[25] Case C-398/15, Camera di Commercio Industria Artigianato e Agricoltura di Lecce v Salvatore Manni, ECJ 9.3.2017, issued such a decision with specific regard to data archived in the Public Register of Enterprises run by the Chamber of Commerce of Lecce (Italy). See the comment to the judgement by A. VERDESCA, I. STELLATO, *Diritto all'oblio e pubblicità commerciale: un bilanciamento invertito*, in *Corriere giuridico*, 2018, 8-9, 1125, also for other references to Italian legal literature at these regards.

[26] The twin judgments with regard to the controversies between Google and the French Authority for Data Protection are: Case C-507/17, Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), ECJ, 24.9.2019, and Case C-136/17, GC e a. v Commission nationale de l'informatique et des libertés (CNIL), ECJ, 24.9.2019. For a critical perspective see M. ASTONE, *Il diritto all'oblio on line alla prova dei limiti territoriali*, in *Europa e Diritto Privato*, 2020, 1, 223 et seq.

[27] We refer to the Case C-18/18, Eva Glawischnig-Piesczek v Facebook Ireland Limited, ECJ, 3.10.2019, regarding the controversy between the Austrian politician E. Glawischnig-Piesczek and Facebook.

Constitution, recognizing the freedom of the press, and, as a consequence, that the right to be forgotten should prevail: therefore, the decision imposed the anonymization of the data of the involved persons [28].

Indeed, the recourse to anonymization can even be approved as a sort of judicious compromise solution, but we have to critically discuss the quite surprising motivations used by the justices: in fact, in the Italian legal system, historical research, and scientific research in more general terms, enjoys of the protection of art. 33 of the Constitution, that is stronger than that of the said art. 21 [29].

Therefore, coming back to our starting point, we would like to conclude that the right to *ἀλήθεια* has to prevail against *Λήθη* [30].

[28] Cass. 22.7.2019, 19681, in *Foro it*., 2019, 10, I, 3071. See the comment to the judgement by V. CUFFARO, *Una decisione assennata sul diritto all'oblio*, in *Corriere giuridico*, 2019, 10, 1189, also for other references to Italian legal literature at these regards.

[29] More specifically, according to article 21 of the Italian Constitution press is free but with the limit of common decency, whilst according to article 33 research is *tout court* free without such a limit nor other comparable limits at all.

[30] The ancient Greek word for truth was *ἀλήθεια* and interestingly its literal meaning is "denial of oblivion" (privative alpha + *Λήθη*), and so disclosure of information. Moreover, we should remember that the opposite of Lethe, as personification of oblivion, was Mnemosyne, as personification of memory (*Μνήμη* in Greek), and that the latter was also the mother of the Muses (*Μοῦσαι* derives from *Μόνσαι* and contains the same root μεν-μαν of their mother's name, and of Latin words such as *mens* = mind or *meminisse* = remember), including precisely Clio, the Muse of historical research (HESIOD, *Theogony*, 53-79). About the "rights to truth" today see F. D'AGOSTINI-M. FERRERA, *La verità al potere. Sei diritti aletici* (Turin 2019).

ADVANCEMENT OF THE RIGHT TO BE FORGOTTEN – ANALYSIS OF THE JUDGMENT OF THE COURT OF JUSTICE OF THE EUROPEAN UNION OF 24 SEPTEMBER 2019 IN THE CASE OF GOOGLE LLC VERSUS COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL) – C-507/17

Wojciech Lamik, University of Wrocław

Abstract:

The analyzed judgment of the Court of Justice of the European Union dated 24th of September 2019 concerning the case Google LLC versus Commission nationale de l'informatique et des libertés (CNIL) – C-507/17, is another judgment that explains the application of the right to be forgotten by the Internet search engine operators. In the judgment, the CJEU focused on analyzing the territorial scope of the application of the abovementioned right. It was important to answer the question whether the right to be forgotten can be used for search engine versions with extensions for countries outside the European Union, assuming that the data subject lives in the EU. In other words, is it possible to use this institution globally and not only within the EU? The author of this article analyzes the judgment in the abovementioned scope, and at the same time compares the decision to other judgments of the CJEU (including in cases C-136/17 and C-18/18), but also the judgment of the European Court of Human Rights in the case of M.L. and W.W. against Germany. The author focuses on the potential effects of the decision of the CJEU and its impact on the further functioning of the right to be forgotten in relation to Internet search engine operators.

Keywords: personal data, right to be forgotten, data protection, privacy, GDPR, Internet search engine, territorial scope, right to freedom of information.

Summary: 1. Introduction. – 2. Factual circumstances. – 3. Ruling. – 4. Analysis of the ruling. – 5. The Court's position in the case of Eva Glawischnig-Piesczek versus Facebook Ireland Limited. – 6. Two stages of exercising the right to be forgotten? – 7. Conclusion.

1. Introduction

The foundations of the right to be forgotten were laid by the judgment of the Court of Justice of the European Union of 13 May 2014 in the case of Google Spain SL and Google Inc. versus *Agencia Española de Protección de Datos* (AEPD) and *Mario Costeja González* [1] and by Art. 17 of Regulation (EU) 2016/679 of the European Parliament and of 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) [2]. The above-mentioned judgment of the CJEU introduced this institution into the EU law, while the GDPR led to its codification and – at the same time – to extending its application beyond Internet search engines.

In the following years, the right to be forgotten was addressed on the basis of subsequent CJEU rulings, such as in the judgment of 9 March 2017 in the case of *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce* versus *Salvatore Manni* [3], which limited the possibility of removing personal data of a member of a body of a limited company consisting of information being processed in the register of business entities, even though sufficient amount of time has passed since the company's existence ceased.

24 September 2019 brought further rulings regarding the subject of protection of personal data in the context of the operation of search engines. The first one was issued in the case of GC and Others versus *Commission nationale de l'informatique et des libertés* (CNIL) [4]. The second one concerns the case of *Google LLC* versus *Commission nationale de l'informatique et des libertés* (CNIL) [5]. The French supervisory authority was party to the proceedings before the Court in both cases. Despite the fact that Directive 95/46/EC [6] was still in

[1] Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, ECJ, 13.4.2014, hereinafter referred to as the "judgment in the case of Google Spain".

[2] OJEU L 119, p. 1, hereinafter referred to as the GDPR.

[3] Case C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce contro Salvatore Manni, ECJ, 9.3.2017.

[4] Case C-136/17, GC and Others v Commission nationale de l'informatique et des libertés (CNIL), 10.1.2019.

[5] Case C-507/17, Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), 24.9.2019, hereinafter referred to as the "judgment in the case of Google LLC".

[6] Directive 95/46/ EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, (1995) OJEU L 281, 31–50.

force at the time when these proceedings started, the CJEU also cited the GDPR regulations which were applicable during the ruling period.

The case of Google LLC regulates the territorial scope of application of the right to be forgotten in the context of the operation of an Internet search engine. In turn, the judgment in the case of GC and Others raised the issue of processing specific categories of data by Internet search engines, such as medical data or data concerning offences. The subject-matter of this article is primarily to discuss the issue of the territorial scope of the right to be forgotten under judgment C-507/17. However, in further parts of the article the author will consider judgment C-136/17.

2. Factual circumstances

In this case, the chairwoman of CNIL requested from Google LLC to take a global approach to exercising the right to be forgotten. In a situation where a natural person would request removal of links to websites that appeared in the search results when the name of that person was entered, the removal should be carried out for all domain extensions of this search engine. In other words, it would not be sufficient to remove links from the google.fr search list; they would have to be removed from all the extensions. Contrary to the CNIL's request, Google LLC removed only the links that appeared in search results of Google search engine domains corresponding to EU Member States. In addition, Google proposed CNIL to apply "geo-blocking" to other domain extensions, which would prevent the display of links in search results carried out in France, regardless of the search engine domain used (i.e. also the ones corresponding to non-EU countries).

However, CNIL stated that Google LLC did not comply with its request and, as a result, by the resolution of 10 March 2016 imposed a fine of EUR 100,000 on the company. The controller lodged a complaint with Conseil d'État - the Council of State. Having doubts regarding the application of Art. 12(b) and Art. 14(a) of Directive 95/46/EC being in force at the time, the Council asked the following questions to the Court of Justice of the European Union:

1) Must the "right to de-referencing", as established by the Court of Justice of the European Union in its judgment of 13 May 2014 on the basis of the provisions of Articles 12(b) and 14(a) of Directive [95/46/EC] of 24 October 1995, be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, to deploy the de-referencing to all of the domain names used by its search engine so that the links at issue no longer appear, irrespective of the place from where the search initiated on the basis of the re-

quester's name is conducted, and even if it is conducted from a place outside the territorial scope of Directive [95/46/EC] of 24 October 1995?

2) In the event that Question 1 is answered in the negative, must the "right to de-referencing", as established by the Court of Justice of the European Union in the judgment cited above, be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, only to remove the links at issue from the results displayed following a search conducted on the basis of the requester's name on the domain name corresponding to the State in which the request is deemed to have been made or, more generally, on the domain names distinguished by the national extensions used by that search engine for all of the Member States of the European Union?

3) Moreover, in addition to the obligation mentioned in Question 2, must the "right to de-referencing", as established by the Court of Justice of the European Union in its judgment cited above, be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, to remove the results at issue, by using the "geo-blocking" technique, from searches conducted on the basis of the requester's name from an IP address deemed to be located in the State of residence of the person benefiting from the 'right to de-referencing', or even, more generally, from an IP address deemed to be located in one of the Member States subject to Directive [95/46/EC] of 24 October 1995, regardless of the domain name used by the internet user conducting the search?

3. Ruling

In this case the Court ruled that "where a search engine operator grants a request for de-referencing pursuant to those provisions, that operator is not required to carry out that de-referencing on all versions of its search engine, but on the versions of that search engine corresponding to all the Member States, using, where necessary, measures which, while meeting the legal requirements, effectively prevent or, at the very least, seriously discourage an internet user conducting a search from one of the Member States on the basis of a data subject's name from gaining access, via the list of results displayed following that search, to the links which are the subject of that request".

The Court's line of reasoning is based on the assumption that numerous third States do not recognise the right to be forgotten (in this case – the right to de-referencing) or have a different approach to that right[7]. The right to the protection of personal data alone is not an absolute right, but must be balanced against

[7] Judgment C-507/17 (fn 5) para 59.

other fundamental rights, in accordance with the principle of proportionality. The CJEU emphasised that the balance between the right to privacy and the protection of personal data and the freedom of information of internet users is not uniform, and is likely to vary significantly around the world [8]. According to the Court, the problem of uniformity in balancing the above-mentioned values also occurs between Member States themselves, which is caused, among others, by the GDPR itself [9]. For example, according to Art. 85(1) of this regulation, the Member States shall by law reconcile the right to the protection of personal data pursuant to the general regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

In the light of the above, in order to develop common standards for balancing between the rights of data subjects and freedom of information, supervisory authorities of Member States should cooperate with each other under Chapter 4 Section 2 of the GDPR as part of cohesion policy [10]. The joint decision obtained that way would be binding for the supervisory authorities and would be observed by the data controller in the aspect of processing personal data in all its facilities within the EU [11].

4. Analysis of the ruling

The judgment discussed here was considered a great victory for Google LLC in protecting global freedom of expression and flow of information. According to *Article 19*, an organisation working for freedom of expression, courts or data regulators in the UK, France or Germany should not be able to determine the search results obtained by the Internet users in America, India or Argentina [12].

Where does the title of this article come from then? In its judgment the Court indicated that although the EU law does not require the exercise of the right to de-referencing in all versions of a search engine, it also does not prohibit such activities. Thanks to this, a judicial or supervisory authority of a Member State

[8] Judgment C-507/17 (fn 5) para 60.

[9] Judgment C-507/17 (fn 5) para 67.

[10] At the time of writing this article, there are consultations underway on the guidelines for the right to be forgotten in search engines. The deadline for submitting comments expires on 5 February 2020; details available on the page https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-52019-criteria-right-be-forgotten-search_pl.

[11] Judgment C-507/17 (fn 5) para 68.

[12] https://www.article19.org/resources/google-win-in-right-to-be-forgotten-case-is-victory-for-global-freedom-of-expression/.

– guided by national standards of protection of fundamental rights – remains competent to weigh up the two disputed values. On the one hand there is a data subject's right to privacy and the protection of personal data concerning them. On the other one there is the right to freedom of information. After weighing those rights against each other, a judicial or supervisory authority of a Member State shall be able to order the operator of that search engine to carry out a de-referencing concerning all versions of that search engine [13].

The above is demonstrated by the CNIL statement of 24 September 2019, where the content of the CJEU judgment was acknowledged. Despite the fact that the Court did not base its decision on the position of the French supervisory authority, CNIL still has the right to demand from the search engine operator to remove search results from all versions of the search engine if the protection of data subjects' rights is justified [14].

Due to this, the Court's judgment indicated the territorial scope of the right to be forgotten, in principle limiting it to the Member States of the European Union. However, it established a kind of a "loophole" for further expansion of the institutions from Art. 17 of the GDPR outside the EU. This "loophole" applies to a situation where the rights of the data subject, i.e. the right to privacy and protection of personal data exceeds the right to freedom of information.

In the presented case, the Court has not indicated any criteria to be followed by judicial or supervisory authorities which should be applied when balancing the values cited above. This may cause significant interpretation problems in the future. As pointed out by *O. J. Gstrein*, one of the interpretations that the Court may have used in the presented judgment would be that the right to be forgotten is not based on one's belief in the importance of privacy or freedom of expression. Its purpose, however, is to determine where the power of informational self-determination of individuals ends in the digital domain, and at the same time – how to guarantee the legitimate need of society to access information [15].

The content of judgment C-136/17, which was announced on the same day as the judgment analysed in this article, may provide a clue as to the above scope in relation to a specific category of personal data. In this judgment, the CJEU states that in determining whether to remove links to websites where outdated information on criminal proceedings against a data subject is published, one should consider such factors as:

1) the nature and seriousness of the offence in question;

---

[13] Judgment C-507/17 (fn 5) para 72.

[14] https://www.cnil.fr/en/right-be-forgotten-cjeu-ruled-issue.

[15] O.J. GSTREIN, *The Judgment That Will Be Forgotten: How the ECJ Missed an Opportunity*, in *Google vs CNIL* (C-507/17) (2019) VerfBlog, available on https://verfassungsblog.de/the-judgment-that-will-be-forgotten/ - DOI: https://doi.org/10.17176/20190925-232711-0.

2) the progress and the outcome of the proceedings;
3) the time elapsed from ending the proceedings;
4) the part played by the data subject in public life;
5) the data subject's past conduct;
6) the public's interest at the time of the de-referencing request;
7) the content and form of the publication in question;
8) the consequences of the publication for the data subject [16].

In the author's opinion, items 4-8 apply not only to the data related to criminal proceedings, but also to a much wider range of publications on the Internet.

Interestingly, in a situation where the operator of an Internet search engine finds that the continued existence of a link to an outdated article is necessary for reconciling the data subject's rights to privacy and protection of personal data with the freedom of information, it is necessary to adjust the search results list in such a way that it reflects the current legal situation of the data subject. Thus, the results list should start with links to pages containing current articles. Such a search update should occur at the time of requesting a removal of the disputed links links at the latest [17].

Another clue can be found in the judicial decisions of the European Court of Human Rights concerning Art. 6 section 2 of the Treaty on European Union [18]. In the judgment of 28 June 2018 in the case of M.L. and W.W. versus Germany [19], the ECtHR pointed out a number of criteria regarding the application of the right to be forgotten in relation to press publications on the Internet, although in most cases they can also be used in relation to search engines. It is important that the judicial or supervisory authority examines the following factors concerning the publication:

1) the contribution to a debate of public interest;
2) the degree to which the person concerned is well-known, and the subject of the report;
3) the prior conduct of the person concerned with regard to the media;
4) the content, form and consequences of the publication;
5) the circumstances in which the photos were taken (if applicable).

It should be emphasised that some views on the global removal of links from the search results list have been already presented before, also outside the European Union. In the controversial judgment of 29 June 2017, in the case of *Google* versus *Equustek*, the Supreme Court of Canada upheld the injunction

[16] Judgment C-136/17 (fn 4) para 77.

[17] Judgment C-136/17 (fn 4) para 78.

[18] See C 326/13 on Official Journal of the European Union, 26.10.2012.

[19] Applications 60798/10 and 65599/10, M.L. and W.W. v Germany, HUDOC, 28.6.2018, available on https://hudoc.echr.coe.int/eng/#{%22itemid%22:[%22001-184438%22]}.

for global removal of search results. "The problem in this case is occurring online and globally. The Internet has no borders – its natural habitat is global. The only way to ensure that the interlocutory injunction attained its objective was to have it apply where Google operates – globally"[20].

The Court's view that it is for Member States to develop their own standards in balancing data subject's rights and freedom of information can also be problematic for search engine operators. A scenario in which each Member State, despite the cohesion mechanism provided for in Art. 63 et seq. of the GDPR, will establish criteria that will present a different approach to the territorial scope of the right to be forgotten in terms of operation of search engines is not at all unlikely. In country A – the prevailing position will be that de-referencing should be global, in country B – the scope of the law will be narrowed down to the UE territory, and in country C – de-referencing covering the search engine for the domain corresponding to the extension for that Member State will suffice. The institution of the right to be forgotten would then be fragmented, which in turn would have impact on the effectiveness of its implementation. Such a state of affairs would also not be beneficial for the Internet search engine operator, which would have to adapt to the regulations of every Member State in this respect[21].

The issue of geo-blocking is another aspect that has not been fully resolved by the Court. The Court decided to generalise this issue, stating only that "it is for the search engine operator to take, if necessary, sufficiently effective measures to ensure the effective protection of the data subject's fundamental rights. Those measures must themselves meet all the legal requirements and have the effect of preventing or, at the very least, seriously discouraging internet users in the Member States from gaining access to the links in question using a search conducted on the basis of that data subject's name[22]". The CJEU has developed virtually no criteria for search engine operators in this regard. Thus, this problem was entirely passed on to operators, who in the event of a potential dispute will have to prove that their technological solutions are fully sufficient to prevent access to incriminated information by Internet users. On the other hand, however, one can understand the Court's position on such a general guideline, as the rapid development of search engine technology is likely to make the current solutions proposed by Google LLC insufficient over time. Setting the above minimum framework for operators by the CJEU may prove to be more beneficial then, especially for persons executing their right to de-referencing.

---

[20] Case C-36602, Google Inc. v Equustek Solutions Inc., SCC Canada 34, 28.6.2017, available on https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16701/index.do.

[21] Cf. O.J. GSTREIN (fn 15).

[22] Judgment C-507/17 (fn 5) para 70.

5. The Court's position in the case of Eva Glawischnig-Piesczek versus Facebook Ireland Limited

Interestingly, the CJEU in its judgment of 3 October 2019 (i.e. just a few days after the announcement of the judgment concerning the case C-507/17) in the case of Eva Glawischnig-Piesczek versus Facebook Ireland Limited [23], was settling a dispute quite similar to the one presented in this article. The basis for the Court's ruling was Art. 15 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce) [24]. This provision pertains to the monitoring being carried out by service providers, concerning the content that is being posted on their websites by their users. Referring to recital 52 of Directive 2000/31/EC, the CJEU pointed out that the damage that may arise in connection with information society services is characterised both by its rapidity and by its geographical extent [25]. The directive itself does not provide for any geographical restrictions concerning the use of prescriptive measures [26]. Thus, it is possible to order the hosting service provider to remove or block access to information worldwide, provided the EU regulations comply with the international law framework.

According to *L. Woods*, the balancing test in case C-18/18 differs from the one in judgment C-507/17 [27]. In the case of Google LLC, the Court pointed out that the right to freedom of information stands opposite to the rights of the data subject (i.e. the right to privacy and protection of personal data). However, in the case of Eva Glawischnig-Piesczek, opposite to the rights of the data subject stands the need of not imposing an excessive burden on the hosting service provider within the scope of supervision and searching for unlawful content. Nevertheless, it should be noted that the presented subject-matter is very similar and is likely to be raised by advocates of global de-referencing.

---

[23] Case C-18/18, Eva Glawischnig-Piesczek contro Facebook Ireland Limited, ECJ, 3.10.2019.

[24] OJEU L of 17 July 2000.

[25] Judgment C-18/18 (fn 23) para 28.

[26] Judgment C-18/18 (fn 23) paras 49 and 50.

[27] L. WOODS, *Facebook's liability for defamatory posts: the CJEU interprets the e-commerce Directive* (2019) *EU Law Analysis*, available on http://eulawanalysis.blogspot.com/search?q=507%2F17.

6. Two stages of exercising the right to be forgotten?

It should be noted that the judgments in the case of Google Spain and in the case of Google LLC actually introduce the need for search engine operators to implement two stages of verifying whether specific links should be removed from the search results list. The first one, introduced on the basis of the judgment in the case of Google Spain – in accordance with paragraph 4 of the judgment, requires the operator to check whether the rights of the data subject prevail in the specific situation over the economic interest of the operator or the interest of recipients in finding said information as part of conducting a search based on the first and last name of this person (although the Court itself states that the data subject's rights prevail over those two opposite values). In addition, the operator must determine whether in the particular case there are special reasons why it is not possible to remove the links in question (e.g. the role that the person plays in public life).

If the search engine operator concludes that it is necessary to remove specific search results, it will be required to move to the second stage, i.e. to decide on the extent of the territorial right to be forgotten in connection with the judgment in the case of Google LLC. The operator must then balance the values of the data subject, i.e. the right to privacy and protection of personal data, against the right to freedom of information. If the controller considers that the Internet users' (including those outside the EU) access to disputed links about a person whose main centre of interest lies within the EU will have immediate and significant consequences for that person in the EU itself, it will be advisable to remove these links from search results lists for every search engine extension. However, if the operator does not believe the above situation to take place, the links removal (or at least the application of measures that would considerably discourage users from gaining access to those links) should be limited only to the territory of the Member States of the Union.

7. Conclusion

To sum up, it should be concluded that the judgment in the case of Google LLC will not stop the initiation of further proceedings regarding de-referencing on all versions of search engines, not only those corresponding to the extensions to the Member States of the European Union. The Court allowed the possibility of formulating such requests in special situations, which means that subsequent court and administrative cases, which will be conducted in the courts of the Member States to the indicated extent, will simultaneously create a catalogue of cases in which such protection should be granted to data subjects. At the same

time, it cannot be ruled out that further requests for preliminary rulings in this respect will be issued to the CJEU.

Unlike countries, the Internet is not limited by any borders. This fact becomes problematic in the perspective of effective application of the right to be forgotten. There seem to be two solutions to this state of affairs. The first one is extraterritorial application of the above institution based on EU regulations, which would necessarily result in a conflict with other legal regulations in this respect (e.g. with American law and its distinctive approach to the relationship between the right to privacy and protection of personal data, and the freedom of information). The second potential solution, although certainly requiring some time in terms of its implementation, is an attempt to standardise legal regulations in the aspect of applying the right to be forgotten. This, of course, is associated with the need to reconcile many legal systems and their solutions provided for Internet search engines [28]. It seems appropriate to opt for the second solution in the long run. After all, global problems require global solutions.

[28] It should also be noted that the right to be forgotten has been addressed in some legislations or court orders (the case of Virginia da Cunha v Yahoo and Google, see E.L. CARTER, *Argentina's Right to be Forgotten* (2013) *Emory International Law Review*, available on http://law.emory.edu/eilr/content/volume-27/issue-1/recent-developments/argentinas-right-to-be-forgotten.html) even before the ruling in the case of Google Spain. More and more legal regulations outside the European Union provide for the ability of removing one's own personal data. Cf. D. ERDOS-K. GARSTKA, *The 'Right to be Forgotten' Online within G20 Statutory Data Protection Frameworks* (2019) 31 *University of Cambridge Faculty of Law Research Paper*.

NEW DATA PROTECTION REGULATION IMPACT ON EUROPEAN INSTITUTIONS [*]

Pelopidas Donos, Data Protection Officer (DPO)
of the European Investment Bank (EIB)

Abstract:

Purpose of the paper is: a) to briefly present the main changes introduced by the New Data Protection Regulation applicable to all EU Institutions and bodies, b) to present the main actions undertaken in order to ensure compliance with the legal framework and c) to describe some differences regarding the application of the legal framework in comparison with private entities and public authorities in the EU Member States.
European Institutions and Bodies were under extreme time pressure in order to implement compliance actions with their data protection Regulation because there was no transition period between the adoption and the entering into force of the new legal framework. The new "accountability" model enhances the responsibilities of the institutions and requires a change of data protection culture not only for the institutions but also for the Supervisor. On the other hand, European Institutions, because of their robust data protection regime can substantially contribute to the development and establishment of future "Best Data Protection Practices".

Keywords: New Regulation for EUIs, Accountability model

1. Introduction

In April 2016 the comprehensive Data Protection Reform was approved. It includes (1) the General Data Protection Regulation (GDPR replacing Directive

[*] Although the activities of the DPOs and the legal obligations of the EUIs are similar, this Article is based only on the experience of the EIB's DPO and reflects his personal opinion.

95/46) establishing a single legal regime over the Members States, (2) a Data Protection Directive on the Police and Criminal Justice sector harmonizing laws in order to facilitate cross border cooperation in the fight against crime and terrorism. These two instruments entered into force in May 2018.

Through those legal acts important changes have been introduced: (a) the idea "one continent/one law" which, together with the "one stop shop" (leading of a single supervisory authority) will facilitate procedures and clarify responsibilities for many companies, businesses and European citizens, (b) the idea "European rules on European soil" (a new territorial scope in order to include EU third countries companies offering services in the EU), (c) major responsibility for Controllers (privacy by design and by default, data protection impact assessments), (d) a major control of data subjects over their own data (right to be forgotten and portability, right to be informed about serious incidents on data protection), (f) increased accountability and enforcement (significant fines can be applied for breach of data protection rules).

The third act of the reform, the Regulation (hereinafter New Regulation) dedicated to European Union Institutions and Bodies (hereinafter EUIs), which aligns the data protection provisions with the provisions of the GDPR, entered into force on 11 December 2018 [1]. The main difference with regard to the EUIs was that other than the GDPR, the New Regulation entered into force without a transition period, which means that the EUIs had less time to prepare and implement the necessary changes. During 2018, the EUIs activities in this particular field have therefore continued to be governed by the previous Regulation (EC) No 45/2001, until the entering into force of the new one on 11 December 2018. That means that complaints (also to the European Data Protection Supervisor) and other cases having started before the date of entry into force were handled, and continued to be handled until they were finalised, under the provisions of the previous Regulation.

On the other hand, the EUIs were for several years closely supervised by the EDPS and under the guidance of the Supervisor had initiated several preparatory actions in order to ensure compliance with the New Regulation [2]. That means that for the EUIs the new data protection provisions and their implementation constitute an evolution rather than a revolution. Nevertheless, there is no doubt that the new legislation indeed introduces a new model of Supervision, enhanc-

[1] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

[2] EDPS Accountability on the Ground, part. 1, part. 2, available on https://edps.europa.eu/data-protection/our-work/publications/guidelines/accountability-ground-provisional-guidance_en.

ing the accountability of the EUIs with regard to their compliance with their legal obligations.

In practical terms, the most important changes introduced by the New Regulation, concern the enhanced obligations of the EUIs and the responsible Controllers and Processors inside the institutions. Furthermore, they concern the conducting of Data Protection Impact Assessments (DPIAs), the obligation to consider in advance the data protection requirements, whenever new information systems or automatized processing operations are introduced (data protection by design and by default), or the obligation to report data protection breaches. Finally yet importantly, the New Regulation provides the data subjects with more rights and enhances the powers of the EDPS, including the power to impose fines.

2. Model change in Data Protection Supervision and new powers for the EDPS

The new "Accountability model" indicates a shift of responsibilities for both the EUIs and the Supervisor (EDPS). Under the previous system, the EUIs (DPOs and Controllers inside the EUIs) had to invest more time and resources in order to notify the most risky processing operations to the EDPS to be prior checked (prior notification model). After the operations have been prior checked, the EUIs had to implement the recommendations but on the other hand, they had at their disposal a kind of "compass and roadmap" with regard to the necessary actions ensuring compliance. Accountability goes beyond "passively" ensuring compliance, in the sense that the EUIs shall be in the position to "actively" demonstrate at any time their compliance with the Regulation vis-à-vis the data subjects or/and the EDPS. That means that the EUIs and consequently the DPOs have to introduce a "risk based approach" in order to be able to identify the data protection risks inside the institutions and to take all necessary measures to ensure, document and demonstrate compliance. Furthermore, the DPOs have to develop enhanced monitoring actions, enabling the follow up of the risk mitigating actions. This risk-based approach together with the reinforcement of the responsibility of the Controllers requires a new data protection culture within the EUIs. More awareness sessions, policies, and procedures that are more detailed can be the outcome of a gap analysis conducted by the DPOs.

The accountability model requires also a shift of activities also from the side of the Supervisor. Besides the consultation provided to the EUIs, it is expected that the EDPS will invest more time in the future for ex post compliance checks, audits and inspections, conducted either "on site" or remotely. This development coincides with the enhanced powers of the EDPS introduced by the New

Regulation, consisting mainly of: a) the possibility to impose a definite limitation, including a ban on processing, b) suspending data flows to a recipient, c) being informed about security breaches, and ordering the notification of the affected persons, and d) imposing administrative fines in cases of non-compliance of 25.000 to 250.000 EUR.

3. New obligations for the institutions

The main new obligations for the EUIs and their controllers are presented in the following four areas:

a) Register

The Register is the data protection "mirror" of the EUIs, containing a detailed description of all processing operations. The Register has an important function not only for Controllers and DPOs but also for the data subjects, which they can find there all information about the way their personal data are processed by the EUIs.

Also under the previous Regulation, all personal data processing operations should be prior notified to the DPO by the Controller and a publicly accessible Register containing all notifications should be also kept. Nevertheless, there was a distinction between "simple" notifications and those related to more sensitive cases, which should subsequently be notified by the DPO to the EDPS. After the 11th of December 2018, the prior check obligation to the EDPS ceased to exist. The text of the New Regulation foresees the replacement of the DPO Register by records kept by the Controllers. Nevertheless, and upon the strong recommendation of the EDPS, the EIB together with the vast majority of the EUIs will continue to have those records kept centrally by the DPO. This solution ensures business continuity and enhances the overall visibility of the processing operations. In addition, the DPOs have to ensure that the Register is publicly accessible also outside the institutions.

b) Data Protection Impact Assessments (DPIAs)

Under the New Regulation, the Controllers responsible for a processing operation of personal data have the obligation to conduct a DPIA whenever the operation is likely to create a high risk for the rights and freedoms of data subjects. This is the case especially for new automated systems containing sensitive data on a large scale.

In practice, the DPIA looks like a set of questions, which allows Controllers to conduct a precise evaluation of the process' risks and to envisage concrete measures to address them. The New Regulation foresees an obligatory consulta-

tion of the DPO during the DPIA. Only in cases where the risks cannot be mitigated will the EDPS be consulted.

In order to prepare the organisations for this important obligation, the EIB's DPO has conducted a threshold inventory to identify the processing operations that could be subject to a DPIA. The inventory was based on a questionnaire proposed by the European Data Protection Supervisor (EDPS) after consultation with the DPOs of the European Institutions and bodies. The inventory was also used in order to identify sensitive processing operations which had not been sent to the EDPS for prior checking under the previous regime. Ideally, the EUIs have to develop a methodology for conducting the DPIAs and a related procedure including the monitoring of the implementation of the risk mitigating measures.

c) Adjustment of Data Protection clauses (DP) in Procurement Rules and Contractual Clauses

One of the most challenging issues, especially for the big institutions like the EIB, was the adjustment of Data Protection clauses (DP) in Procurement Rules and Contractual Clauses to the requirements of the New Regulation. The new responsibilities of the processors, the obligations related to the security breaches and to the conducting of DPIAs had to be reflected and translated in the contractual clauses and in the calls for tenders. In 2018, the EDPS addressed two letters to all European institutions and bodies describing the necessary changes and adjustments required by the New Regulation in the matter of procurement rules and contractual clauses, especially those related to outsourcing activities. The adjustment of the provisions is of upmost importance in order to meet also the requirements of privacy by "design and by default" as reflected in Article 27 of the New Regulation. Especially for new systems and applications, the EUIs will have the opportunity to describe the relevant data protection requirements from the very beginning namely during the procurement phase.

The EIB DPO prepared a questionnaire and conducted an extensive survey within the Bank to establish an inventory of all EIB Data Protection (DP) clauses used in outsourcing activities. The exercise has identified three types of DP clauses that would need to be adjusted: Procurement rules and templates (1), Contractual DP clauses (2) and Service Level Agreements (SLA) (3). The exercise identified approximately 500 objects being subject to the adjustments.

Given the big amount of contracts, one important question was whether it would be necessary to also adjust existing contracts, and if yes, which ones. A dedicated Working Group composed of DPOs and the EDPS has been established in order to discuss all parameters of the matter and initiate the setting up of Standard Contractual Clauses for outsourcing activities.

As a follow up of the relevant discussions, the EDPS proposed to the institu-

tions to conduct a risk assessment for all categories of contracts in order to identify them under the following categories: No risk, Low risk and High risk. For those identified as High risk contracts, the EUIs shall, on their own initiative, address the contractual counterparties and propose to amend the contracts by using the standard contractual clauses prepared by the EDPS and the European Commission. The EDPS finally communicated the Standard Contractual Clauses shortly before the entering into force of the New Regulation.

Furthermore, the EIB DPO together with the other DPOs (OLAF, Commission and EIF) took the initiative to consult the EDPS on the way the EUIs have to proceed in cases where contractual parties ask for changes because of their GDPR obligations. The result of the consultation was a model letter prepared by the EDPS to be used by the institutions in those cases.

d) New rights for the data subjects

With regard to the rights of the data subjects, the New Regulation introduces additional safeguards related to the validity of the consent of the data subject. Consent is valid only via an "affirmative action" of the data subject (opt-in) and EUIs have the obligation to always document and demonstrate that consent has been provided. Nevertheless, the processing operations where the consent of the data subjects is legally required, is limited to those cases where the data subjects have a real choice to provide the information or not (like e.g. in the EIB for staff members having their pictures published in the intranet or for travelers and visitors providing their diatery preferences to the organisation). In the vast majority of the cases in the EUIs, the legal basis for the specific processing operations derives from a contractual relationship (e.g contract of employment) or represents a legal obligation of the institution.

New is also the right to "data portability" (Article 22 of the New Regulation) entitling data subjects to receive their personal data in a structured machine-readable format, and ask to transfer the data to another Controller. Taking into consideration that this Article is copied from the GDPR and applies mostly to the private sector e.g. whenever a customer changes the service provider, it is expected that the impact to the EUIs will be rather limited. The famous "right to be forgotten" has been also included in the Regulation as an extension of the already applicable right to ask for an erasure (deletion) of the data. The additional obligation of the Controller not only to erase the data but also to inform other Controllers about the request, if the data have been made public, will have probably a limited impact to the EUIs taking into consideration that this provison is also copied by the GDPR and it is more related to Internet or social media providers (Big data companies like e.g. Google or Facebook).

One of the most urgent issues following the entering into force of the New Regulation was to prepare and adopt internal rules allowing the restriction of

data protection rights (Article 25 of the New Regulation). Taking into consideration that the possibility to restrict rights on an ad hoc basis (Article 20 of the previous Regulation 45/2001), (e.g. during investigations and administrative inquiries), has been removed from the final text of the New Regulation, internal rules had to be prepared allowing the respective services to fulfil their tasks without hindrance. Those rules have to be published also to the Official Journal of the European Union. Therefore, and due to the time constrains, the DPOs and the EUIs were under extreme time pressure in order to prepare adopt and publish the rules. The EIB has published e.g. two sets of internal rules, one set governing the conducting of investigations and administrative inquiries [3] and one set related to similar activities of the Personnel Department.

e) Adjustment of policies, procedures and "Privacy Notices"

Another important topic was the adjustment of the Data Protection Statements (Privacy Notices) to the requirements of the new legal framework. The DPOs in cooperation with the services concerned had to identify and accordingly amend the most important Privacy Notices, especially those accessible via Internet. It goes without saying that also internal procedures, policies and guidelines had to be also amended or initiated based on a conducted gap analysis.

Although there were no substantial changes with regard to international data transfers, the EUIs have to pay attention in order to carefully document and supervise transfers outside the European Economic Area and especially for those applications based on cloud solutions.

4. Status of the Data Protection Officer

The Data Protection Officers (DPOs) of the EUIs (Section 6 of the New Regulation) are integrated in a European framework of data protection entities, headed by the European Data Protection Supervisor (EDPS) located in Brussels (with substantial competences and supervisory powers - Art. 52 of New Regula-

[3] Internal rules concerning the processing of personal data by the Fraud Investigations Division within the Inspectorate General and the Office of the Chief Compliance Officer of the European Investment Bank in relation to the provision of information to data subjects and the restriction of certain of their rights, available on https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2019_065_I_0001&from=EN. Internal rules concerning the processing of personal data by the Personnel Directorate of the European Investment Bank in relation to the provision of information to data subjects and the restriction of certain of their rights, available on https://www.eib.org/attachments/documents/eib_decision_on_the_processing_of_personal_data_en.pdf.

tion), and completed at national level by national Data Protection Authorities (DPAs) and at EUIs level by the DPOs.

In all EUIs the DPO is an independent function. The functional independence of the DPO is enshrined in the New Regulation and complemented by the implementing rules of each institution. The DPOs have the following main tasks:

a) to inform and advise the Controller or the Processor and the employees who carry out processing operations of their obligations,

(b) to ensure in an independent manner the internal application of the Regulation; and to monitor compliance, including the assignment of responsibilities, the raising of awareness and training of staff involved in processing operations, and the related audits,

c) to provide advice where requested as regards the necessity for a notification or a communication of a personal data breach,

d) to provide advice where requested as regards the data protection impact assessment,

e) to consult the European Data Protection Supervisor in different occasions,

f) to respond to requests from the European Data Protection Supervisor, cooperate and consult with the European Data Protection Supervisor at the latter's request or on his or her own initiative,

g) to ensure that the rights and freedoms of data subjects are not adversely affected by processing operations,

(h) to investigate matters and occurrences that directly relate to the DPO's responsibilities,

(i) to cooperate with the DPOs of the other institutions,

(k) to represent the institution with regard to all data protection issues.

The DPO of the EIB e.g. has data protection oversight over all Departments and can use significant investigative powers. In particular, the DPO has access to all premises and to all information systems and applications, may propose administrative measures and issue general recommendations, draw attention to any failure by a staff member to comply with the Regulation, propose an administrative inquiry, and request an opinion from the relevant areas of the Bank on any associated issue. The internal application of data protection rules (Art. 43, 44, 45 of the New Regulation) should be ensured with autonomy, and the DPO should plan his activity in an independent way.

In addition, and under the New Regulation, the EU Institutions have to ensure that the DPO reports directly to the highest management level and that the DPO will be involved in all cases of data protection breaches and of Data Protection Impact Assessments. The contact details of the DPO shall be also made public. Furthermore, the DPOs should be allocated the resources necessary for the performance of her/his duties. The new legal framework provides the EUIs

with the possibility to use external DPOs and to "share" the DPO by appointing one DPO for more EUIs.

Under the new "Accountability model", the responsibilities and the importance of the position of the DPO will increase. Like in the private and public sector of the Member States, the DPOs have to play a central role [4] by preparing the EUIs in the best possible way in order to ensure compliance with the new legal framework. Although the liability lays mainly with the Controllers, remains the main responsibility of the DPO to create awareness for controllers and data subjects, to update about the legal and technical developments, to communicate with the Supervisor and coordinate the actions of all data protection stakeholders.

5. Conclusion

The new data protection framework introduces the new model of "Accountability" for the European Institutions and Bodies. This model means more responsibilities for Controllers inside the institutions and for the Data Protection Officers in order to ensure document and demonstrate compliance. Nevertheless, the new model represents rather an "evolution" than a "revolution" for the data protection regime taking into consideration that the EUIs were under many years under the close supervision of the EDPS. Although the EUIs had less time to introduce and implement the necessary changes they can serve as a "laboratory" of best data protection practices, taking into consideration that they concentrate in a more "controlled environment" all kinds of processing operations, like e.g. staff related operations, business related operations upon personal data, international data transfers and contractual relationships with public and private stakeholders. The EDPS can use this experience in order to further develop and establish those "Best Data Protection Practices" in their proposals, consultations and guidelines.

[4] B. RASLE, *Pour une Désignation 'Idéale' du DPO* (2019) *Le Journal du Management*, 38.

HAVE COLLABORATED TO THIS ISSUE OF THE *EJPLT*

PELOPIDAS DONOS – Data Protection Officer (DPO), European Investment Bank (EIB)

MASSIMO FOGLIA – Researcher of Private law, Department of Law, University of Bergamo

LUCILLA GATT – Full Professor of Private law, Department of Law, University Suor Orsola Benincasa of Naples; Director of the Research Centre of European Private Law (ReCEPL)

AGNIESZKA GUZEWICZ – Assistant Professor of Civil law, Faculty of Law, Administration and Economics, University of Wrocław

JONAS KNETSCH – Professor of Civil and Comparative Law, Faculty of Law, Jean-Monnet University of Saint-Étienne

WOJCIECH LAMIK – PhD Student in Civil Law, Faculty of Law, Administration and Economics, University of Wrocław

DULCE LOPES – Assistant Professor of European Union and Private International Law, Faculty of Law, University of Coimbra; Researcher at the University of Coimbra Legal Research Institute

FEDERICA PERSANO – Assistant Professor of International law, Faculty of Law, University of Bergamo

MARCO RIZZUTI – Researcher of Private Law, Department of Legal Sciences, University of Florence

ALBERT RUDA-GONZÁLEZ – Associate Professor of Private Law, University of Girona, Dean of the Faculty of Law

MARTIN ŠOLC – Researcher at the Centre for Medical Law and doctoral student at the Department of Civil Law, Faculty of Law, Charles University

RADOSŁAW STRUGAŁA – Assistant Professor in Civil law, Faculty of Law, Administration and Economics, University of Wrocław

SHAIRA THOBANI – Research Fellow with grant in Private law, Faculty of Law, University of Turin