UNIFICATION OF PERSONAL DATA PROTECTION IN THE EUROPEAN UNION: CHALLENGES AND IMPLICATIONS

Unificación de la protección de datos personales en la Unión Europea: desafíos e implicaciones

Dolores-Fuensanta Martínez-Martínez

Nota: Este artículo se puede leer en español en:
http://www.elprofesionaldelainformacion.com/contenidos/2018/ene/17_esp.pdf

Dolores-Fuensanta Martínez-Martínez has a doctorate in Law from *Universidad Católica San Antonio* in Murcia, a master's degree in business management from the *Know How Business School* in Madrid, a degree in Law and Economics from *CEU San Pablo* in Madrid, and Criminology from *Universidad Europea* in Madrid. Professor of Company Law at the *Universidad de Murcia*, lawyer and substitute prosecutor of the *Tribunal Superior de Justicia de Madrid* (*TSJM*). Member of the R&D project work team *Mobile communication and personal information: Impact on the media industry, the advertising system and the perceptions of the users* (CSO2013-47394-R).
https://orcid.org/0000-0002-8149-828X

Universidad de Murcia, Facultad de Comunicación y Documentación
Campus de Espinardo. 30100 Murcia, Spain
dfmartinez@um.es

Abstract

The European Union faces the fourth industrial revolution and the digital single market with the unification of the legal status for personal data protection sought by the *General Data Protection Regulation (EU) 2016/679*. This legal unification is more theoretical than real, since formal aspects of the regulation and the content materials of the fundamental right to data protection make this process difficult. The entry into force of the *GDPR* in May 2018 provides the first legal reference framework for the implementation in companies of a true culture of privacy, and the protection of personal data and normative compliance in the EU.

Keywords

Digital economy; Digital single market; Fundamental rights; Protection of personal data; Privacy; *General data protection regulation*; *GDPR*.

Resumen

La Unión Europea afronta la cuarta revolución industrial y el mercado único digital con la unificación del régimen jurídico sobre protección de datos personales pretendida por el *Reglamento (UE) 2016/679 General de protección de datos*. Esta unificación es más teórica que real, toda vez que aspectos formales del reglamento y los materiales del contenido del derecho fundamental a la protección de datos dificultan este proceso. La entrada en vigor del *Reglamento* en mayo de 2018 proporcionará el primer marco legal de referencia para la implementación en las empresas de una verdadera cultura de la privacidad, de la protección de datos personales y el cumplimiento normativo en la UE.

Palabras clave

Economía digital; *Mercado único digital*; Derechos fundamentales; Protección de datos personales; Privacidad; Intimidad; *Reglamento general de protección de datos*; *RGPD*.

Martínez-Martínez, Dolores-Fuensanta (2018). "Unification of personal data protection in the European Union: Challenges and implications". *El profesional de la información*, v. 27, n. 1, pp. 185-194.

https://doi.org/10.3145/epi.2018.ene.17

Manuscript received on 09-09-2017
Accepted on 05-12-2017

1. Introduction

At the gates of the "fourth industrial revolution" (*CNMC Report*, 2016) a growing number of innovative technological solutions (3D printing, 5G, virtual and augmented reality, Internet of things, cloud computing, artificial intelligence, big data, etc.) are based on two essential pillars:

- the connectivity and interoperability of technologies (*Comisión Europea*, COM (2016) 587 final, p. 3); and
- the digitisation of data/information or information datification processes (**Santamaría**, 2016).

The information age embraces forms of "digital capitalism" (**Costas**, 2017) that include diverse socio-economic phenomena such as:

- the sharing economy,
- the free exchange of goods and services (gift economy),
- the barter economy, or
- economy on demand (gig economy),

all of them under the common umbrella of the "digital economy" or the concept of "information economy" (**Cohen**, 2017). This is characterised by the dematerialisation of traditional production factors of the market, to which is linked to a fourth key factor –personal data-, moving the traditional role of the market to digital platforms (**Cohen**, 2017). The "data" and "the information" represent the main production factor of a digital market still anchored to the economic theory of bilateral markets based on advertising. The treatment of information and data through profiling techniques (elaboration of users' online profiles) from "cookies" or other data collection techniques provides the segmentation required by online behavioural advertising, marketing one to one, or programmatic advertising (**Navas-Navarro**, 2015, p. 151; **Martínez-Martínez**; **Aguado**; **Boyekens**, 2017).

> New technological solutions pose complex challenges related to the collection and use of personal information in very different areas and, at the same time, interrelated subjects

In this context, it is not risky to agree with **Gómez-Barroso** and **Feijóo-González** (2013) in stating that personal data is the new currency of the digital economy, by enabling not only personalised advertising (one-to-one advertising) as a business model of the "big data", but also the ubiquity of information with mobile internet (**Martínez-Martínez**; **Aguado**; **Boeykens**, 2017, **Martí-Parreño**; **Cabrera-García-Ochoa**; **Aldás-Manzano**, 2012). Perhaps the most paradigmatic case of the relevance of personal data is that of social network platforms and services. It has been said that the users are not customers but products, since the essence of the social network business is found in the data and information that users provide and make public in their profiles (**Alonso-García**, 2015, p. 23).

New technological solutions pose complex challenges related to the collection and use of personal information in very different areas and, at the same time, interrelated to subjects such as the economy, telecommunications, health, sectoral policies or law. From a legal perspective, online personal data and information have always faced the challenge of guaranteeing consumer-users the same protection and legal security as in a physical market. An efficient electronic commerce requires the free cross-border circulation of data (personal or not) and information, but also a reliable and uniform legal reference framework that guarantees the rights of companies and consumers. But the biggest challenge of a digital society is to guarantee the rights and freedoms of citizens/online users in the face of threats of malicious use or treatment of our trail or digital fingerprint (information and personal data that we leave behind when interacting with electronic supports, surfing the internet or accessing social networks), which could lead to crimes of various types of cyber-harassment: cyberbullying, happy slapping, grooming or computer scams such as phishing using malware or malicious code (**Alonso-García**, 2015, p. 35; **Hernández-Guerrero**, 2013).

The first European legal framework for the Information Society was *Directive 2000/31/EC*, of the *European Parliament* and the *Council*, of June 8th, regarding certain aspects of Information Society services (*Unión Europea*, 2000). Focused on electronic commerce in the domestic market (directive on electronic commerce) it is incorporated into Spanish *Law 34/2002*, of July 11th, of *Information Society services and electronic commerce* (*Lssic*). This Law resolves the legal uncertainties generated by the Internet and ICT by providing legal status to services and electronic contracting, regulating:

- obligations of the service providers including intermediaries for the transmission of content over telecommunication networks;
- electronic commercial communications;
- information before and after the conclusion of electronic contracts;
- conditions related to its validity and effectiveness; and
- sanctioning status applicable to service providers of the Information Society (Article 1 *Lssic*).

The regulation, despite its reforms (2003, 2007, 2011, 2012 and 2014), includes a broad concept of "Information Society services" that includes practically all current activities, only limited to "representing for the provider an economic activity" so allowing the inclusion in the concept future services or activities yet unknown. The providers of online platforms developed from web 2.0 such as social networks or collaborative economy platforms (*Blablacar*, *AirBnb*...) are subject to the scope of the *Lssic* and are considered services of the Information Society –in spite of the users-consumers themselves being the generators of content and information through their interaction in the network (**Agustinoy-Guilayn**; **Monclús-Ruiz**, 2016, p. 25)-, because they constitute an economic activity, they provide electronic information remotely and they are offered at the request of the user (**Ortiz-López**, 2013, p. 31).

The communication *A strategy for the Digital Single Market of Europe*, COM 2015 192 final, Brussels, 6/5/2015) (*Comi-*

sión Europea, 2015) marks the beginning of a new community legislative policy of the digital economy. The harmonising mechanisms are abandoned in favour of the unifiers as the community regulation, giving support on the promotion of ICT as a horizontal European policy that affects all economic sectors and the public sector. The Union's strategy is ambitious with 22 short-term actions based on the principle of legislating better and three basic pillars:

- ensure the accessibility of consumers and businesses to online goods and services by eliminating European cross-border barriers;
- promote high-speed infrastructures, safe and reliable digital content with adequate regulation; and
- take advantage of the growth potential of ICT, cloud computing, big data and innovation to boost competitiveness.

The strategy addresses regulatory reforms of a transversal nature on telecommunications, intellectual property, consumer protection, electronic contracting, cybersecurity, privacy and data protection, electronic public administration, competition, initiatives on the ownership of data and its free movement, parcel shipments or audio-visual communication, that among others aim to define the main lines of a digital single market without barriers to allow Europe to lead the global digital economy (COM 2015, *Comisión Europea*, 2015, 192, p. 2).

This paper addresses the new European strategy on personal data protection based on its most recent regulatory initiative and with the greatest economic and social impact. After more than 20 years of validity of the *Directive 95/46/EC*, the *Official Journal of the European Union* (*OJEU*) of May 4th, 2016, published the *Regulation (EU) 2016/679* of the *European Parliament* and the *Council* of April 27th, concerning *the protection of natural persons regarding the processing of personal data and on the free circulation of such data* (*General Data Protection Regulation - GDPR*) which will be directly applicable in all EU States from May 25th 2018.

> "Data" and "information" represent the main production factor of the new digital market

The *GDPR* provides a common framework that is more solid and coherent with technological advances, globalisation and the level of development of the digital economy in the Union, also providing the legal security demanded by natural persons in the processing of their personal data. The "principle of control over personal data" is generalised via the regulatory unification used. Although it allows some room for manoeuvre for the Member States in certain matters that require national legislation, as in the cases of appointment and competency of the national authorities for data protection or processing of "sensitive data". The Regulation is a legislative milestone in the field of privacy and protection of personal data, and a very substantial change of focus when trying to establish a true culture of privacy and the protection of personal data (*ESYS Report*, 2016, p. 46) affecting all the market operators and their main lines. We will try to outline these in the following sections, beginning with the conceptual and legal delimitation of the fundamental right to the protection of personal data.

2. The protection of personal data as a fundamental right

Convention No. 108 of the *Council of Europe* of January 28th, 1981, currently signed by 47 countries, is the first legally binding international instrument that recognises the protection of individuals regarding the automatic processing of their personal data. The "processing of personal data" is integrated into the content of Article 8 of the *European Convention on Human Rights* (*ECHR*, 1950), guaranteeing the right of every person to respect their private and family life, their home address and correspondence, with the exception of interference permitted to public authority by law and for reasons of national and/or public security, defence of the order and prevention of crime, protection of health or morals, or protection of the rights and freedoms of others.

> The strategy for the *Digital Single Market in Europe* marks the beginning of a new Community legislative policy of the digital economy

In the same sense, article 18 of the *Spanish Constitution* (*SC*) in the second chapter on fundamental rights and public liberties, guarantees the protection of the right to honour personal and family privacy and to one's own image; as well as the inviolability of the home address and the secrecy of communications, especially postal, telegraphic and telephonic ones, except by judicial resolution. The last section Article 18.4 *SC* establishes that:

> "the law will limit the use of information technology to guarantee the honour, and personal and family privacy of citizens, and the full application of their rights."

This section supports the legal regime and content of the right to the protection of personal data developed by subsequent Organic Laws such as the repealed *LO 5/1992, of October 29th, regulating the automatic processing of personal data (Lortad)* and the currently valid *LO 15/1999 protection of personal data (LOPD) of December 13th*.
The *Sentence of the Constitutional Court (STC) 292/2000, of November 30th*, Spain, defines the fundamental right to the protection of personal data as:

> "a fundamental right or freedom [...] in in the face of potential aggression to the dignity and freedom of the people, by means of an illegitimate use of mechanised data processing, which the Constitution calls computing."

It is, according to the Spanish *Constitutional Court*, the right to control the data relating to any person involved in a computer program, the "habeas data" (*STC 254/1993, of July 20th*) also known as "computing freedom" in other judgments (*SSTC 143/1994*, *11/1998*, *94/1998*, *202/1999*, and *292/2000*). The *Constitutional Court* affirms that alongside negative content –limiting the use of information techno-

logy to guarantee the honour and personal and family privacy of citizens and the full application of their rights-, this fundamental right has positive aspect: the attribution to the affected citizen of certain courses of action, of actions which demand certain behaviour of third parties, such as the citizen's opposition to certain personal data being used for purposes other than the legitimate one that it was intended for (*SSTC 11/1998*, FJ 5; *94/1998*, FJ 4).

The link between both fundamental rights, the right to privacy (Article 18.1 *Spanish Constitution*) and the right to protection of personal data (Article 18.4 *Spanish Constitution*) is justified by the common purpose pursued: to offer protection to the private and family life of people, although they differ in the object and the content as it warns the *Constitutional Court* itself (*STS 292/2000*, FJ 6).

The object of the right to data protection is broader than the right to privacy (Article 18.1 *Spanish Constitution*) affecting the sphere of other personality assets such as personal dignity, honour and the full application of the person's rights, in such a way that their protection not only applies to intimate data but also

> "to any type of personal data, intimate or not, whose use or knowledge by third parties may affect their rights."

Reaches therefore the public personal data (*Civil Registry*, *Commercial Registry*, etc.), the data that identify or make possible to identify the person and enable the creation of an ideological, racial, sexual or any other profile, or any other use that in certain circumstances constitutes a threat for the individual, or has an impact on the application of any of the rights of the person, whether constitutional or not.

> The Union's strategy is ambitious, with 22 short-term actions based on three basic pillars: accessibility, infrastructures and growth of ICT

On the other hand, the content of the fundamental right to data protection is extended in relation to the right to privacy by conferring on its owner an array of capacities such as prior consent for the collection of data, the right to be informed of the destination and use of the data, the right of access, rectify or cancel the data; summarising, "the power of disposal and control of their personal data," different from the content of the right to honour, personal and family privacy, and to one's own image that is civilly protected "in the face of all types of interference or illegitimate intrusion," these rights being inalienable and imprescriptible (cf. art. 1 *LO 1/1982, May, of Civil protection of the right to honour, to personal and family intimacy and to one's own image*).

At this point it is appropriate to differentiate between intimacy, privacy and protection of personal data. From a technical-legal point of view, it affects different areas. In accordance with the doctrine of the Spanish *Constitutional Court*, the right to personal intimacy is derived from the fundamental right to personal dignity (Article 10.1 *Spanish Constitution*)

> "it implies the existence of a private space and reserved to the action and knowledge of others, necessary, according to the guidelines of our culture, to maintain a minimum quality of the human life."

The sphere of personal intimacy is related to the delimitation of the same by its owner, each person being able to reserve a specific space of personal, family or even professional intimacy from the knowledge of others, so guaranteeing the secret of one's own sphere of personal life and consequently, forbidding third parties, individuals or public authorities from deciding on the delineations of private life (*STC 241/2012*, FJ 3). The scope of the protection of this right is described by the existence of "a reasonable expectation of privacy or confidentiality." The Spanish *Constitutional Court* uses privacy or rather, "the expectation of privacy" as a delimiting criterion of the scope of coverage of the right to intimacy. Thus, the manifestations of private life protected against illegitimate interference are subject to

> "the reasonable expectation that the person himself, or any other in his place, in that circumstance, may have to be protected from observation or from the scrutiny of others" (*SSTC 170/2013*, *12/2012*, FJ 5).

For example, when a person is in an inaccessible or solitary place due to the time of day, he can conduct himself with full spontaneity in the founded trust of the absence of observers, or on the contrary, cannot harbour reasonable expectations of privacy, when someone participates in activities that, due to the circumstances surrounding it, can clearly be subject to registration or public information (privacy criterion shared with judgments of the *European Court of Human Rights* of September 25, 2001, PG and JH v. United Kingdom; and January 28, 2003, Peck v. United Kingdom).

None of the Spanish rules of positive law regulates the content, scope of protection or legal concept of privacy despite being one of the terms most used on the Internet. The statement of motives of the repealed *Lortad* of 1992 is the only one that

> "talks about privacy and not about intimacy" and expressly:
> "…privacy is a broader, more global, set of facets of a personality that, considered in isolation, may lack intrinsic significance but, coherently linked together, generate a quick portrait of the personality of the individual that he has the right to maintain reserved ... privacy may be undermined by the use of computer technologies of recent development".

Thus, strict sense, the Spanish legislation recognises a fundamental right to intimacy (Article 18.1 *Spanish Constitution*) while the so-called "right to privacy" that is born as an Anglicism of the English term "privacy" would be directly related to the "fundamental right to the protection of personal data "(Article 18.4 *Spanish Constitution*) defined as

> "the fundamental right that the competent authorities protect all citizens against the possible non-authorized use of their personal data to obtain a specific profile with a specific purpose, without the knowledge or consent of

> the owner of the data" (**Davara-Fernández-De-Marcos**, 2015, pp. 30-31).

At Community level, the express recognition of the fundamental right to the protection of personal data of Article 8 of the *Charter of Fundamental Rights of the European Union* of the year 2000 is legally binding as a primary right with the entry into force of the *Treaty of Lisbon* of December 1, 2009; and in the same way, Article 16.1 of the *Treaty on the Functioning of the European Union* (*TFEU*). Paragraphs 2 and 3 of Article 8 of the *Charter* establish the basic principles and content of this right:

> "...2. This data will be treated fairly, for specific purposes and on the basis of the consent of the affected person or by virtue of another legitimate basis provided by law. Everyone has the right to access the data collected that concerns them and to rectify it.
> 3. Respect for these rules will be subject to the control of an independent authority"

which are subject to further development due to legal EU heritage.

The fundamental right to the protection of personal data or computer freedom (*habeas data*) has evolved, as has the object of its regulation. Initially considered as a right dependent on and subordinated to the right to personal privacy (Article 18 *Spanish Constitution*) designed for an analogue society, in the 21st century it is an autonomous and independent fundamental right that retains its initial objectives of guaranteeing other rights and freedoms (intimacy, one's own image, honour, freedom of thought, conscience, freedom of enterprise ...), but that faces the challenge of a flow of personal cross-border data on an unprecedented scale fostered by rapid technological evolution and globalisation (Whereas 6 *GDPR*).

The content and internal logic of the fundamental right to data protection in the European Union has been shaped by national and European jurisprudential resolutions: *STC 292/2000*, November 30th; *Stjue* of 18.12.2008, case C-73/07 *Tietosuojavaltuutettu* and *Satakunnan Markkinapörssi Oy*, *Satamedia Oy*; *Stjue of 05.13.2014*, case C-131/12 *Google Spain SL*; *Google Inc* and *Spanish Data Protection Agency*. Also for the work of the *European Data Protection Group of Article 29* of *Directive 95/46/EC* (*WG 29* integrated by the *National Data Protection Authorities*, *European Data Protection Supervisor* and the *European Commission*) and the development of other sectoral regulations (health, crime, child protection). The quality standards achieved in this sense allow the EU to aspire to impose them internationally, especially in relations between Europe and the United States, and to lead the regulation of the global digital market (cfr. article 3 *GDPR* on the territorial scope of application of the *Regulation*) (**Fernández-Villazón**, 2016).

3. *General European Data Protection Regulation*

3.1. New legislative strategy

Regulation 2016/679 (*Unión Europea*, 2016) which had been over 4 years in negotiation, is one of the most important legislative processes in the history of the European Union. It modernises and improves the previous regulation (*Directive 95/46/CE*) increasing the legal security provided by its "strict enforcement" as a community regulation or in its consideration of true "European law". It is conceived as a framework law to homogenise the matter of protection of personal data throughout the EU, and to provide consistency and coherence to other provisions that are part of the so-called "data protection package". This is stated by the *European Data Protection Supervisor* in his judgement summary published in the *OJEU* of 20.7.17 (*C 234/3-5*) on the *Proposal for a Regulation of privacy and electronic communications* [*COM* (2017) 10 final Brussels 10.1.17] (*ePrivacy Regulation*), that repeals *Directive 2002/58/EC* by requiring it to adapt to the *GDPR* and to avoid gaps in the protection of personal data.

> "The new *GDPR* provides a common framework more consistent with technological advances and globalisation, providing legal security to the processing of personal data"

The *GDPR*, in spite of its persistent objective of guaranteeing a uniform and coherent protection in the treatment of personal data in the European Union that promotes the free circulation of these, presents limitations or exceptions.

On one hand, natural limitations or those inherent to the right to the protection of personal data on any situation that is not an

> "absolute right but must be considered in relation to its role in society and maintain the balance with other fundamental rights in accordance with the principle of proportionality" (Whereas 4 *GDPR*).

These are exceptions covered by a law and justified by public interest, national security or defence, crime prevention or respect for other fundamental rights and public freedoms, such as the right to information.
On the other hand, structural or formal limitations foreseen by the *GDPR* such as the continuity of national data protection laws, specific exceptions in terms of record keeping for micro and small and medium enterprises, or exceptions in the treatment of special categories of personal data such as "sensitive data". The *GDPR* contains authorisations and impositions for Member States to regulate certain matters impeding the anticipated unification and contributing to perpetuate different levels of protection in the Union. It is the ultimate responsibility of the Member States to harmonize their national legislation on the foundation of a uniform system throughout the Union, while preserving, to the extent that that system does not, its principles and legal tradition. The Member States have a 2-year *vacatio legis* to meet this mandate, until May 25th, 2018 date of application of the regulation and limit for entrepreneurs to adapt to the new system. On May 5th, 2017, the *Federal Council of Germany* approved the *Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der*

Richtlinie (EU) 2016/680 o *Bundesdatenschutzgesetz-BDSG* (*Federal Data Protection Law*), the first national standard adapted to the provisions of the *GDPR*, while in Spain the new draft of the *Organic Law on Data Protection*, submitted to report of the *Council of Ministers* on July 7th 2017, has a significant number of 78 articles regarding the adaptation and development of the *European Regulation* (the preliminary draft contemplates, for example, the treatment of the data of the deceased persons -article 3 and D. A. seventh, despite their exclusion by the *GDPR*).

> The Spanish *Constitutional Court* establishes the right to control the data relating to any person involved in a computer program, the "habeas data" also called "computer freedom"

3.1.1. Implications for the single digital market

The change of legislative strategy from directive to regulation directly applicable to citizens and economic operators involves important challenges. The *GDPR* is an extensive and complex standard with 11 chapters, 99 articles and 173 whereas obliged to address in more detail and completeness the different aspects of the treatment of personal data (not mere guidelines), many of them excessively technical (pseudonymisation, genetic data, biometrics ...) and bureaucratic ones that do not help to make the citizen aware of the risks that undue manipulation of their personal data entails for their rights and, therefore, would compromise the ultimate efficacy of the norm (**Fernández-Villazón**, 2016).

On the other hand, the new regulation involves organisational management and management challenges for the economic operators of the European digital market. One could speak of a "revaluation" of European personal data regarding other States with more "lax" legislation, since the implementation of risk management systems and protection of personal data in accordance with the requirements of the *GDPR* entails some costs that reassesses the value of the protected asset (personal data). The alternative to non-compliance with the *GDPR* also entails business costs as a result of the administrative sanctions incurred. The *GDPR* is applicable to personal data of users residing in the EU, and pertinent to the offer of goods or services to those users, independently of the fact that the person in charge and/or in charge of treatment and the processing of personal data are carried out in a State outside of the EU.

For those physical persons who are internet users, the *GDPR* supposes the empowerment of their personal digital information and an increase of their power of control and disposition (right of information, of suppression, portability), that is, greater guarantees of privacy in the treatment of their personal data throughout the Union, which should, in turn, encourage cross-border e-commerce and the dynamisation of the digital single market.

3.2. Most relevant news from the *GDPR*

The *Regulation*, and *Directive 95/46/CE* that the *Regulation* repeals, share the same principle:

> "natural persons must have control of their personal data"

although the homogeneous legal framework that the *Regulation* intends to create supposes a substantial change of approach towards a true culture of the prevention and protection of personal data in the Union. We address the list of the main changes to the articles following the *ESYS Report* (*Fundación ESYS*, 2016) and classifying them according to the area that we consider most affected:

3.2.1. Changes that affect business governance and compliance

The *GDPR* tries to simplify the bureaucracy that the implementation of data protection systems infers upon companies and those responsible for the processing of personal data. The previous advice or notice to the supervisory authority required by the *Directive* to carry out a personal data treatment disappears, but incorporates in its articles obligations and principles directly related to corporate governance, risk management models and regulatory compliance, already required in other legal areas such as the prevention of labour risks or criminal compliance.

> The fundamental right to the protection of personal data faces the challenge of a flow of personal cross-border data on an unprecedented scale fostered by rapid technological evolution and globalisation

In this respect, new personal data protection principles are introduced (Article 5), such as:

- transparency in the way data is treated; proactive responsibility in compliance with the principles and their accreditation (accountability);
- protection of data from design (privacy by design) or proactive responsibility as a global and predetermined model of compliance with privacy regulations embedded in the design of computer systems (**Agustinoy-Guilayn**; **Monclús-Ruiz**, 2016; **Megías-Terol**, 2013);
- protection of data by default, that is, the obligation that by default, only the personal data necessary for each of the specific purposes of the treatment (privacy by default) and the obligation of a prior impact assessment (privacy impact assessment, PIA) in treatments that entail a high risk for the rights and freedoms of natural persons;
- obligation to appoint a *Data Protection Officer* (DPO) contained in articles 37 to 39 of the *GDPR* for companies that perform large-scale personal data processing as part of their primary activity. The DPO advises and informs the person in charge and / or in charge of treatments and the employees, playing a crucial role in guaranteeing compliance with regulations.
- obligation to keep an internal record in writing or electronic

format of the treatment activities carried out (Article 30) does not apply to companies with less than 250 workers.

The *GDPR* also promotes, as the previous *Directive* did, adherence to codes of conduct and submission to certification mechanisms such as the *European Seal of Data Protection* (articles 40 to 43).

3.2.2. Strengthening and new citizens' rights

Article 7 of the *GDPR* develops the new conditions of validity of the consent of interested parties for the treatment of their personal data that must no longer be unambiguous, free and revocable, but a declaration or clear affirmative action requiring the controller to be

> "able to demonstrate that he (the interested party) consented to the processing of his personal data."

Tacit consent is still accepted unless it affects special categories of data and as long as the person in charge can demonstrate that it complies with the legal requirements. Article 8 regulates the consent of minors by establishing a kind of "*computer age majority*" by recognising as valid the consent given by those over 16 years (Member States can reduce itto 13 years). Below that age the authorisation of the nominated parental authority is required.

The content of the right to information to the interested party is reinforced and extended (Article 12), requiring privacy clauses to be "concise, transparent, intelligible and easily accessible". It is even foreseen the use of standardized icons that facilitate the understanding the information contained in many of the privacy policies, which are too technical for an average citizen. It also strengthens the right not to be subject to automated decisions, including the preparation of profiles (Article 22). *GDPR* doesn't prohibit these practices, but it guarantees the affected person's right to have human intervention, to express their point of view and to challenge the decisions, essential possibilities that should be offered to the user before the consequences that can be derived from techniques such as big data and the elaboration of predictions about work performance, economic situation, individual behaviour, etc. (**De-Roselló-Moreno**, 2016, **Recio-Gayo**, 2017).

New rights have been added alongside the traditional ARCO rights (right of access, rectification, cancellation and opposition), such as

- the "right to be forgotten" or the right to demand the deletion of personal data that concerns them (Article 17);
- the right to limitation of treatment (Article 18), that is, cases in which the data are not deleted but are no longer processed and are kept only for procedural or trial purposes, and
- the right to portability of the data (art. 20) that recognises the right to receive the personal data that concern us in a structured format of common use and mechanical reading, and transmit them to another person responsible for processing, without being able to oppose the first one. Direct portability between responsible parties is allowed when technically possible (frequent situation among mobile telephony operators).

3.2.3. Changes that affect the control and supervision of regulatory compliance

The *European Data Protection Commission* has been created as the body in charge of ensuring compliance with the standard and advising the *European Commission*, replacing the current *GT-29*. The one-shop system is established in such a way that companies with personal data treatment in different Member States have a single *National Control Authority* as interlocutor (articles 56 to 76). The *Control Authorities* have the obligation to cooperate with each other and provide mutual assistance. The "coherence mechanism" is also arbitrated for the solution of conflicts between *National Control Authorities* or to unify criteria for interpretation and application of the *GDPR*. The competent *European Data Protection Committee* has to arbitrate the coherence mechanism and its decisions are binding.

The *Regulation* provides for administrative penalties with fines of up to 20 million euros or 4% of the annual turnover of the offending company (articles 83 and 84). This system of administrative fines is conceived as a deterrent, a proportional and effective system that will address the individual circumstances of the specific case and where collaboration with the *Control Authority*, adherence to *Codes of Conduct*, intentionality or the nature of the infraction operate as mitigating liability for regulatory breach. The obligation to communicate regulation breaches or violations of data security to the *National Control Authorities* within 72 hours and without undue delay is also regulated (Articles 33 and 34). In this case, users will also be directly informed when security breaches of personal data entail a high risk for their rights and freedoms, adopting the necessary measures to avoid generating undue alarm and after having carried out the corresponding evaluation (**Olejnik**, 2017).

> "The *GDPR* represents a substantial change of approach towards a true culture of the prevention and protection of personal data in the EU"

The *GDPR* extends the concept of "personal data" (Article 4). It is kept as "*all information about an identified or identifiable natural person*" specifying that the identifiable natural person is anyone whose identity can be determined, directly or indirectly, in particular by means of an identifier, such as a name, an identification number, location data, an online identifier or one or several elements of the physical, physiological, genetic, psychic, economic, cultural or social identity of said person. The "special" categories of personal data are extended by adding to the traditional "sensitive data" (ethnic or racial origin, political opinion, religion, union affiliation, health and sex life), genetic data, biometrics that identify in a unique way to a physical person, philosophical convictions and sexual orientation. Introduces new concepts such as "*pseudonymous*" personal data with a specific treatment.

4. Conclusions

The role of EU policies in the development of the digital market and its implications for the treatment and personal information online is decisive for its link with rights and fundamental freedoms around privacy. *General Data Protection Regulation 2016/679* on data protection is presented as a milestone in the legal history of the European Union (more than 20 years since *Directive 95/46/EC* (Unión Europea, 2016, now repealed), although we understand that it shares some considerations similar to other European legal milestones such as *Regulation (EC) 2157/2001*, on the *Statute of the European Company (SE)*.

First of all, it is a milestone because of the object or regulated matter. If during the twentieth century the European limited company or "SE" was considered the "flagship" of European corporate law for the completion of the internal market with a legislative process of more than 30 years, such consideration can be predicated now on personal "data protection". In the 21st century and before the expectations of a digital single market, data, and in particular personal data, have acquired double relevance not only as a fundamental right (Article 8 *European Charter*, and Article 18.3 *Spanish Constitution*) but also as a new factor in production or "a new currency of change" of the digital economy (**Gómez-Barroso**, **Feijóo-González**, 2013).

> "The GDPR extends the concept of "personal data"

The new *GDPR* protectionist and privacy protection legal system empowers and revalues the treatment of personal data of European users against the most permissive of legislation. However, the information and personal data in its consideration as a factor of production and "currency of change" of the digital market, would demand in accordance with our legal tradition where personal and family privacy, honour and self-image are inalienable rights, a process of "reification" (**Navas-Navarro**, 2015). Equally would demand a recognition as an "intangible asset" and birthright in such a way that it attributes to its owner exclusive exploitation rights through the transfer of its use (not sale) to third parties in exchange for an economic consideration (price) or of any other nature (a type of data exchange for services).

The new *GDPR* demands the highest standards of legal certainty because it is a fundamental right. The content of this right is not absolute and evolves under the protection of resolutions of different jurisdictional orders, and although it pursues the protection of "technologically neutral" natural persons, it is always influenced by the evolution of ICTs themselves (internet of things, artificial intelligence, massive data, etc.).

From a formal viewpoint, the use of European regulation as a legal instrument of unification and uniformity of the legal regime of personal data in the EU is more theoretical than real. The *GDPR* cannot guarantee the same level of protection of personal data of natural persons in all Member States for two reasons:

- by the authorisations and express remissions of the *GDPR* itself to national legislation on data protection that generates new normative sources;
- because specific sector regulations coexist with the *GDPR* that exempt the general system such as rules for the prevention, investigation, detection or prosecution of criminal offences and / or execution of criminal sanctions, or rules on protection against threats against the public security or terrorism, among others.

The *GDPR* is formally a unifying instrument directly applicable in all the Member States, but functionally requires the adaptation and harmonisation of national legislations as if it were a directive. A uniform legal system but territorially fragmented.

Undoubtedly, the most relevant contribution of the *GDPR* is the modernisation of the legal system on the fundamental right to personal data protection. It defines its general principles and provides a legal reference framework throughout the Union for the implementation of management systems inspired by the culture of prevention and regulatory compliance of privacy and the protection of personal data. The *European Data Protection Committee* and the *National Agencies* will be responsible, in any case, to ensure the effectiveness and coherence of the new system in the digital single market.

5. References

Agencia de los Derechos Fundamentales de la Unión Europea (2014). *Manual de legislación europea en materia de protección de datos*. Bruselas: Agencia de los Derechos Fundamentales de la Unión Europea; Consejo de Europa.
https://rm.coe.int/16806ae663

Agustinoy-Guilayn, Albert; **Monclús-Ruiz, Jorge** (2016). *Aspectos legales de las redes sociales. Estudio introductorio. Problemática jurisprudencial ordenada y sistematizada. Esquemas procesales. Formularios generales. Normativa reguladora*. Barcelona: Bosch. ISBN: 978 84 9090 105 2

Alonso-García, Javier (2015). *Derecho penal y redes sociales*. Pamplona: Aranzadi. ISBN: 978 84 90983263

CNMC (2016). *Informe económico sectorial de las telecomunicaciones y el audiovisual 2016*. Comisión Nacional de los Mercados y la Competencia.
https://www.cnmc.es/expedientes/estadcnmc00516

Cohen, Julie E. (2017). "Property and the construction of the information economy: A neo-Polanyian ontology". En: Lievrouw, Leah; Loader, Brian (eds.). *Handbook of digital media and communication*. Routledge, forthcoming. ISBN: 978 1 138672093
https://ssrn.com/abstract=2991271

Comisión Europea (2015). *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una estrategia para el mercado único digital de Europa.* Bruselas, 6 mayo.
https://goo.gl/Gf9ZyA

Comisión Europea (2016). *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones. La conectividad para un*

mercado digital único competitivo. Hacia una sociedad europea del Gigabit. Bruselas, 14 septiembre.
https://goo.gl/64xNgR

Comisión Europea (2017). *Propuesta de Reglamento del Parlamento Europeo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la directiva 2002/58/CE* (*Reglamento sobre la privacidad y las comunicaciones electrónicas*). Bruselas, 10 enero.
https://goo.gl/fs1tQx

Costas, Antón (2017). "Economía digital, ¿vidas precarias?". *La vanguardia*, 5 abril.
https://goo.gl/VDqwYK

Davara-Fernández-de-Marcos, Laura (2015). *Implicaciones socio-jurídicas de las redes sociales*. Pamplona: Aranzadi. ISBN: 978 84 9098 912 8

De-Roselló-Moreno, Rocío (2016). "Nuestros datos personales, fuente de negocio y actividades de *profiling*". *Blog Consejo General Abogacía Española*, 21 septiembre.
https://goo.gl/CvaucG

España (2002). "Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico". *Boletín oficial del Estado*, n. 166, 12 julio.
https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

Feijóo-González, Claudio; Gómez-Barroso, José-Luis; **Martínez-Martínez, Inmaculada J.** (2010). "Nuevas vías para la comunicación empresarial: publicidad en el móvil." *El profesional de la información*, v. 19, n. 2, pp. 140-148.
https://doi.org/10.3145/epi.2010.mar.04

Fernández-Villazón, Luis-Antonio (2016). "El nuevo Reglamento europeo de protección de datos". *Foro. Nueva época*, v. 19, n. 1, pp. 395-411.
https://goo.gl/2vk2fq

Fundación ESYS (2016). *El Reglamento general de protección de datos de la UE: una perspectiva empresarial*, octubre.
https://goo.gl/Y96Abt

Gómez-Barroso, José-Luis; **Feijóo-González, Claudio** (2013). "Información personal: la nueva moneda de la economía digital". *El profesional de la información*, v. 22, n. 4, pp. 290-297.
https://doi.org/10.3145/epi.2013.jul.03

Hernández-Guerrero, Francisco (2013). "Las conductas de acoso por medio de las tecnologías de la información y de las comunicaciones". En: Rallo-Lombarte, Artemi; Martínez-Martínez, Ricard. *Derecho y redes sociales* (eds.). Civitas Ediciones, pp. 259-298. ISBN: 978 84 470 3578 4

Martí-Parreño, José; **Cabrera-García-Ochoa, Yolanda**; **Aldás-Manzano, Joaquín,** (2012). "La publicidad actual: retos y oportunidades". *Pensar la publicidad*, v. 6, n. 2, pp. 327-343.
http://dx.doi.org/10.5209/rev_PEPU.2012.v6.n2.41219

Martínez-Martínez, Dolores-Fuensanta (2014). *El proceso de constitución de una sociedad europea-filial en España*. Murcia: Iuris Universal Ediciones. ISBN: 978 84 94187865

Martínez-Martínez, Inmaculada J.; **Aguado, Juan-Miguel**; **Boeykens, Yannick** (2017). "Ethical implications of digital advertising automation: The case of programmatic advertising in Spain". *El profesional de la información*, v. 26, n. 2, pp. 201-210.
https://doi.org/10.3145/epi.2017.mar.06

Martínez-Martínez, Ricard (2013). "Protección de datos personales y redes sociales: un cambio de paradigma". En: Rallo-Lombarte, Artemi; Martínez-Martínez, Ricard (eds.). *Derecho y redes sociales*. Civitas Ediciones, pp. 83-116. ISBN: 978 84 470 3578 4

Megías-Terol, Javier (2013). "Privacy by design, construcción de redes sociales garantes de la privacidad". En: Rallo-Lombarte, Artemi; Martínez-Martínez, Ricard (eds.). *Derecho y redes sociales*. Civitas Ediciones, pp. 319-334. ISBN: 978 84 470 3578 4

Navas-Navarro, Susana (2015*). La personalidad virtual del usuario de internet. Tratamiento de la información personal recogida mediante cookies y tecnología análoga*. Valencia: Tirant lo Blanch. ISBN: 978 84 9086 081 6

Olejnik, Lukasz (2017). "Organizations must inform users about privacy breaches". *Lukasz Olejnik*, 13 Nov.
https://blog.lukaszolejnik.com/organizations-must-inform-users-about-privacy-breaches

Ortiz-López, Paula (2013). "Redes sociales: funcionamiento y tratamiento de información personal". En: Rallo-Lombarte, Artemi; Martínez-Martínez, Ricard (eds.). *Derecho y redes sociales*. Civitas Ediciones, pp. 23-36. ISBN: 978 84 470 3578 4

Recio-Gayo, Miguel (2017). "Nuevo dictamen del GT-29 sobre tratamiento de datos en el trabajo: el interés legítimo". *Diario la ley*, Sección ciberderecho, n. 8, 19 de julio.
https://goo.gl/6kPKBR

Santamaría, Fernando (2016). "Datificación: una alternativa de control de información para grandes empresas". *Reporte digital*, 11 de mayo.
https://goo.gl/ij5zy4

Unión Europea (2000). "Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (directiva sobre el comercio electrónico)". *Diario oficial de las Comunidades Europeas*, 17 julio.
http://www.wipo.int/edocs/lexdocs/laws/es/eu/eu107es.pdf

Unión Europea (2016). "Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos". *Diario oficial de la Unión Europea*, 4 mayo.
https://www.boe.es/doue/2016/119/L00001-00088.pdf

Unión Europea (2017). "Resumen del Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Reglamento relativo a la privacidad y las comunicaciones electrónicas (Reglamento ePrivacy)". *Diario oficial de la*

Unión Europea, 20 julio. *https://edps.europa.eu/sites/edp/files/publication/17-07-20_eprivacyreg_ex_summ_es.pdf*

Valera-Ferrío, José (2015). *La brecha digital en España. Estudio sobre la desigualdad postergada*. Madrid: Comisión Ejecutiva Confederal de UGT. *http://www.ugt.es/Publicaciones/BRECHADIGITAL_WEB.pdf*

Vilajoana-Alejandre, Sandra; **Rom-Rodríguez, Josep** (2017). "Sistema de autorregulación publicitaria: del compromiso ético al control efectivo de la publicidad en España". *El profesional de la información*, v. 26, n. 2, pp. 192-200. *https://doi.org/10.3145/epi.2017.mar.05*