UNIO - *EU Law Journal*. Vol. 9, No. 1, July 2023, pp. 58-79.

School of Law – University of Minho

The concept of personal data protection culture from European Union documents: a "Brussels effect" in Latin America?*

Alexandre Veronese**
Alessandra Silveira***
Rebecca Lemos Igreja****
Amanda Nunes Lopes Espiñeira Lemos*****
Thiago Guimarães Moraes******

ABSTRACT: This article aims to analyse, based on documentary sources and data collected through extensive field research, the potential cultural influence of EU (European Union) standards for protecting personal data in Latin American countries, which have data protection

* The authors are deeply grateful to the São Paulo Research Foundation (FAPESP) for funding this research. They also thank the Faculty of Latin American Social Sciences in Brazil (FLACSO Brazil) and the College of Latin American Global Studies. Special thanks are due to the over seventy interviewees who generously dedicated their time to collaborate in more than sixty interviews for this research. Finally, the research team also acknowledges the support of Márcio Iório Aranha (Associate Professor of Law at the University of Brasilia), as well as Mariana Moutinho Fonseca (researcher with a master's degree from the University of Brasilia and the University of Connecticut), Luiza Mendonça da Silva Belo Santos, and Luiza Peixoto Veiga (master's degree students in Law at the University of Brasilia), and also Amanda Braga, Eduarda Costa Almeida, and Vitória Sernégio (scientific initiation scholarships at the University of Brasilia). Translation by Eduardo Monteiro. Review by Alexandre Veronese.
** Associate Professor of Social Theory and Law at the Faculty of Law of the University of Brasilia and coordinator of the Telecommunications Law Study Group.
*** Associate Professor with Aggregation at the School of Law of the University of Minho (Portugal) and coordinator of the Jean Monnet Centre of Excellence on Digital Citizenship and Technological Sustainability (CitDig).
**** Associate Professor at the Institute of Social Sciences and Graduate Program of the Faculty of Law at the University of Brasilia, coordinator of the Latin American College of World Studies, and member of the International Council of FLACSO.
***** Ph.D. student in Law at the University of Brasilia and the University of Minho.
****** Ph.D. student in Law at the University of Brasilia and Vrije Universiteit Brussel (Belgium).

authorities and specific laws on the subject. The text has two sections, with an introduction and a conclusion. The introduction presents the subject, indicating the sources that lead up to the text analysis and conclusions. In the first section, the article deals with the EU's data protection model from its fundamentalist legal perspective. The second section deals with constructing the personal data protection culture concept and how extensive EU documents research can help infer it. The conclusion indicates that the EU's data protection perspective – as a fundamental right and public policy – can potentially influence several Latin American countries. Also, it concludes that there is an evident difficulty in culturally measuring greater or lesser effectiveness in protecting personal data based on the documents. Despite this dilemma, the EU documentation points to some qualitative suggestions that deserve to be incorporated into the analysis of cultures of personal data protection, focusing on Latin American countries.

KEYWORDS: Personal data protection – European Union – Latin America – culture of personal data protection – cultural influences.

Introduction

This text was prepared based on information gathered by the research project entitled "*Documentary and field research on the Latin American data protection authorities: the social and institutional concept of privacy and personal data*". It received approval from the FAPESP/MCTIC 2018 call.[1] It is a comprehensive project that proposed, among its various analytical objectives, to observe the international cultural influences, specifically of the EU on Latin America, and to identify local peculiarities of national laws, institutional organisations, and the management of the subject. Thus, through field research and documentary analysis, the project sought to understand the existence of movements toward the universalisation or expansion of the concept of a "*culture of personal data protection*" in Latin America.

The term "*culture of personal data protection*" has become common in the discourse of experts and the general media. In order to understand the management and expansion of this concept, the research aimed to verify its approach in technical documents from the EU and in the statements of over seventy interviewees from various fields of work – governments, data protection authorities, academics, civil society, and businesses – in the countries surveyed, throughout 2021 and 2022 (Argentina, Brazil, Chile, Colombia, Costa Rica, Spain, Mexico, Panama, Peru, Portugal, and Uruguay). By comparing the legal documents from the EU with the data collected in the field, it was possible to identify a cultural influence of standards regarding protecting personal data in the analysed Latin American countries. The text concludes that the EU documents have developed public policies to promote a harmonious culture of personal data protection among its Member States and achieve global reach. Nevertheless, the assessment of how these concepts have been received and translated in various Latin American countries relied on other specific sources, which were understood through documentary and field research, focusing on their social and institutional structures. This last topic, concerning the local peculiarities of Latin America, will be the subject of another article to be published.

[1] FAPESP, "Documentary and field research on the Latin American data protection authorities: the social and institutional concept of privacy and personal data," accessed July 24, 2023, https://bv.fapesp.br/en/auxilios/105576/documentary-and-field-research-on-the-latin-american-data-protection-authorities-the-social-and-inst/.

1. The protection of personal data in the EU is a fundamental right

Protecting personal data is recognised as a fundamental right in Article 8 of the Charter of Fundamental Rights of the European Union (CFREU), as follows: "*Article 8. Protection of personal data. 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and based on the consent of the person concerned or some other legitimate basis laid down by Law. Everyone has the right access to data collected concerning him or her and the right to rectify it. 3. Compliance with these rules shall be subject to control by an independent authority*".[2]

The protection of personal data develops in the EU as an autonomous fundamental right with its normative recognition. This protection is provided for in EU law to prevent the protection of personal data from occupying a hierarchically inferior position in conflict with other protected rights and interests. A good example is the differentiation concerning the right to privacy protection. Initially recognised as the right to be left alone, the right to privacy has undergone considerable developments since its first doctrinal references in the United States of America in the 19th century.[3] However, more is needed to meet the protection needs of global citizens, whether in internet applications or database processing, which have become ubiquitous in recent decades. Indeed, the right to privacy cannot be reduced solely to desiring solitude in the presence of third parties, whether states or companies.

This social transformation has determined the need for legal reconstruction, a social process, in favour of a broader design of personal data protection. Therefore, EU law, with particular emphasis on the CFREU, has enshrined this fundamental right to protect data, which does not necessarily need to be private or intimate; it is enough that they are personal.[4] Consequently, this legal and cultural peculiarity is not unusual. After all, this fundamental right, which derives from the right to privacy, has long been debated.[5] However, the innovation of EU law lies precisely in separating these rights, granting them autonomous fundamental legal status. It is enough to analyse that the fundamental right to respect for private and family life is allocated in Article 7 of the CFREU as follows: "*Article 7. Respect for private and family life Everyone has the right to respect for his or her private and family life, home and communications.*"[6]

It is essential to emphasise the importance of considering this right a fundamental right, as it provides additional protection to individuals, especially when it comes into conflict with other rights and duties. In addition, Article 16 of the Treaty on the Functioning of the European Union (TFEU) provides for the competencies of the EU, which are shared with the Member States to regulate the

[2] European Union, "Charter of Fundamental Rights" (Brussels, June 6, 2016), 395, accessed July 22, 2023, https://eur-lex.europa.eu/eli/treaty/char_2016/oj.

[3] Samuel D. Warren and Louis D. Brandeis. "The right to privacy." *Harvard Law Review*, v. 4. no. 5, (1890): 193-220.

[4] Alessandra Silveira and João Marques, "Do direito a estar só ao direito ao esquecimento – considerações sobre a proteção de dados pessoais informatizados no direito da União Europeia: sentido, evolução e reforma legislativa." *Revista da Faculdade de Direito da Universidade Federal do Paraná*, v. 61, no. 3 (2016), accessed July 22, 2023, http://revistas.ufpr.br/direito/article/view/48085/29828.

[5] Orla Lynskey, *The foundations of EU data protection law* (Oxford: Oxford University Press, 2015).

[6] European Union, "Charter of Fundamental Rights of the European Union" (Brussels, June 6, 2016), 395, accessed July 22, 2023, https://eur-lex.europa.eu/eli/treaty/char_2016/oj.

processing of personal data and its free movement: "*Article 16. 1. Everyone has the right to the protection of personal data concerning them. 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices, and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted based on this Article shall be without prejudice to the specific rules in Article 39 of the Treaty on European Union.*"[7]

The significance of the CFREU lies in its legally binding force since the entry into force of the Lisbon Treaty in 2009, as provided in Article 6(1) of the Treaty on the European Union (TEU).[8] Thus, the EU institutions and Member States must respect and promote the enforcement of its fundamental rights, as stated in Article 51 of the CFREU. Indeed, this also applies to the topic of personal data protection. One of the interviewees from the academic sector in Portugal presents this argument: "*European law, as a whole, is made in the light of the protection of fundamental rights, especially with the European Charter of Fundamental Rights, which establishes, in fact, a materiality of European law that no one can escape from.*"[9]

The Court of Justice of the European Union (CJEU) decisions also support protecting personal data. This Court, over time, has addressed the topic from some main perspectives: data de-indexation, data retention, data transfer, and issues related to responsibility for processing operations. This fundamentalist legal perspective on protecting personal data in the EU comes from the functioning of the Single Market and, consequently, the recognition of economic freedoms and existing relations between Member States and between the EU and other countries worldwide. The protective scope includes the international transfer of personal data and the need to adapt the legal systems of Member States and third countries to protect personal data. This protection is essential to promote better social and commercial exchanges. In this regard, that is, due to the interaction of the EU with third countries, it is possible to observe, in the statements of interviewees in the field research, in the documents, and in the academic works analysed, a movement towards recognising the protection of personal data as a fundamental right in the regulatory framework of several Latin American countries.

The existing challenge in regulating the transfer of personal data is precisely to strike a balance between ensuring the protection, constitutionally and legally recognised as a fundamental right, on the one hand and, on the other hand, ensuring that there is the exchange of information facilitated by this transfer,

[7] European Union, "Consolidated version of the Treaty on the Functioning of the European Union" (Brussels, October 26, 2012), 55, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF.

[8] European Union, "Consolidated version of the Treaty on European Union" (Brussels, November 26, 2012), 19, https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF. European Union. "Consolidated version of the Treaty on European Union" (Brussels, November 26, 2012), 19, https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF.

[9] POR2ACA, in *Pesquisa documental e de campo sobre autoridades de proteção de dados na América Latina: o conceito social e institucional de privacidade e de dados pessoais – Anexo 2 (entrevistas não identificadas) – volume 1*, Alexandre Veronese *et al.* (Brasília: Fapesp, January 31, 2023), 231.

which is essential for international trade.[10] Latin America tries to advance precisely in this direction, as indicated by an author from Costa Rica: "*Ibero-America is moving towards legislation on a fundamental right inherent to individuals, taking steps towards a space of legal security both in the business environment and in economic transactions and services, as well as in the freedom of movement of people and their relationships with their daily space, in which the Internet plays a fundamental role, and data spread rapidly through social networks (authors' translation).*"[11]

This Latin American movement to grant personal data protection status as a constitutional or fundamental right in domestic legal systems is a result of the influence of the EU model. This movement occurs in two main ways. First, it comes through the adequacy decisions of the European Commission (EC), as it occurred with the repealed Directive 95/46/EC and may take place with Regulation (EU) 2016/679, known as the General Data Protection Regulation (GDPR). Notwithstanding, the EC decisions taken during the Directive's force are still in force. Second, this also occurs through attempts to update the legal systems of Latin American countries, which have had laws since 1999, such as the Ley No. 19.628 from Chile.

Another potential leverage route is the creation of new national laws on personal data protection in countries that did not have them before. One of the recurring themes in these social processes is the discussion on the implementation and effectiveness of supervisory authorities – or data protection authorities –, especially in political and social movements, after the advent of the GDPR: "*The path of normative changes has already origins from the important effort in the EU that includes the approval of the GDPR and its entry into force in 2018. So it is now up to our authorities to promote the legislative changes that insert us into the global approach, whose most important characteristic is to design standards that offer homogeneous guarantees that allow the Law to prevent risks or resolve conflicts that may arise regarding the holders of personal data and those responsible for processing (public or private) their information in different latitudes (authors' translation).*"[12]

Some interviewees from Portugal explain the evolution of EU law regarding the ruling of personal data protection through a Regulation rather than a Directive. They demonstrate the difference between these two types of EU normative acts. This difference is relevant in the applicability and enforcement of the Law by the Member States, as a Directive requires the transposition of norms into national laws. In contrast, although Regulations require norms that enable enforceability, they are directly applicable. Thus, personal data protection has gained greater normative strength, demonstrating its relevance within the logic of the free movement of data in the Internal Market. This phenomenon would be the culmination of a process related to the advent of digitisation. According to an interviewee from Portugal, this process would require a more robust regime concerning the protection of personal data. He further explains: "*Why was there a need to advance personal data protection to a Regulation? Under the Directive, which preceded the regulation, what emerged was that, in practice, the national schemes were very diverse. A directive is a European legal act that allows Member States – provided that they achieve those normative objects and that they achieve*

[10] Mauricio París Cruz and Juan Ignacio Zamorra Montes de Oca, *Ley de protección a la persona frente al tratamiento de sus datos personales*. (San José: Editorial Jurídica Continental, 2015), 75.
[11] Cruz and Montes de Oca, *Ley de protección a la persona frente al tratamiento de sus datos personales*, 14.
[12] Diego Valdivia, "La normativa peruana de protección de datos personales frente al reto de pasar de un modelo de gestión de datos al uso responsable de la información," in *La proyección del Derecho Administrativo Peruano - estudios por el Centenario de la Facultad de Derecho de la PUCP*, ed. Diego Valdivia. (Lima: Palestra Editores, 2019), 205.

that proposed regime – to release all their constitutional and administrative procedures. In essence, it allows them to carry out this normative creation, to do what is called the transposition of Law (...). This diversity, this lack of homogeneity, began to cause obstacles, difficulties, and problems. (...). There was also a need to intensify, so to speak, the degree of personal data protection. This upgrade motivates the appearance of the GDPR, which comes into effect in 2018, although it is from 2016. (...). The sophistication of issues related to personal data protection was not unprecedented in terms of European integration. (...). That is, now there is no room for each member state to end up with variations regarding the transposed regime. (...). Moreover, when there are national laws, as is the case with Portugal? Theoretically, it first specifies, clarifies, and potentially develops aspects that can do so when they are missing in the Regulation. However, if it does, it must do so in line with the Regulation due to the doctrinal principle [of the primacy of EU law]."[13]

In another way, an academic interviewee from Portugal has the same explanation, emphasising that the most significant limitation Regulations impose on the Member States is adapting their national legal systems to EU law: "*The European regulation is directly applicable. It is published in the Official Journal of the European Union, and from there, it binds Member States, public and private entities, and citizens. In other words, it binds everyone. It is directly applicable. Nevertheless, even so, in some regulations, for certain major and complex matters, the European Union admits (not in all cases, it is an exception, not a rule) that the Member States may create their national laws to adapt the logic of the Regulation to their distinct realities.*"[14]

It is clear, then, that there is a legal and binding framework within the EU Member States. However, the production of EU law has another peculiarity compared to the production of other national laws, namely its power of representation and symbolism for other countries outside the Union. Elaine Fahey describes this process of representation and symbolic influence that the EU has in the world and refers to it as a "*global reach*." According to the author, this would be the global reach of standards and regulatory models for other countries. The "*data privacy standards*" are used here as examples of the so-called "*Brussels effect*."[15] According to Fahey, this phenomenon is noticeable in the rules for international data transfers made by the EU, which, in a way, unfold into a "*Europeanisation and governance scholarship*."[16] The following section draws data from EU documents and addresses the conceptual consolidation of personal data protection.

2. The construction of the concept of personal data protection culture in EU documents

Researching the term "*data protection culture*" in the EUR-LEX database led to finding a number of documents. The first EU document highlighting "*data protection culture*" dates back to 2009. This document referred to the *European Data Protection Supervisor's* (EDPS) Opinion. The EDPS is an agency established by Regulation (EC) 45/2001 to carry out and collaborate with protecting personal data within the EU

[13] POR1ACA, in *Pesquisa documental e de campo sobre autoridades de proteção de dados na América Latina: o conceito social e institucional de privacidade e de dados pessoais – Anexo 2 (entrevistas não identificadas) – volume 1*, Alexandre Veronese et al. (Brasília: Fapesp, January 31, 2023), 240-241.

[14] POR2ACA, in *Pesquisa documental e de campo sobre autoridades de proteção de dados na América Latina: o conceito social e institucional de privacidade e de dados pessoais – Anexo 2 (entrevistas não identificadas) – volume 1*, Alexandre Veronese et al. (Brasília: Fapesp, January 31, 2023), 227.

[15] Fahey, *The global reach of EU Law*, 1-2.

[16] Fahey, *The global reach of EU Law*, 8.

institutions themselves. This Regulation was repealed in 2018 to make way for another, in line with the GDPR. The EU established EDPS in 2004 but renewed its mission with the GDPR and Regulation 2018/1725.[17] It is distinct from the *European Data Protection Board* (EDPB), the coordination body for data protection authorities in the various Member States.[18] The document dealt with the creation of a multi-year plan for the protection of children in the use of the Internet and information and communication technologies. The EDPS Opinion was an instructive document for a public policy of the EU: "*Several initiatives can be mentioned as an illustration of recent actions taken in this perspective in Member States or Members of the EEA. The Swedish DPA conducts a yearly survey on young people's attitudes towards the Internet and surveillance, just like the DPA of the United Kingdom, which conducted a survey directed at 2000 children between 14 and 21 years old. In January 2007, together with the Ministry of Education, the Norwegian DPA launched an education campaign directed at schools. In Portugal, a protocol has been signed between the DPA and the Ministry of Education to promote a data protection culture on the Internet and especially on social networks. Following this project, Portuguese social networks have integrated an interface and a mascot dedicated to children between 10 and 15 years old.*"[19]

In this document, data protection culture refers to state actions to clarify and modify the behaviours of citizens and internet applications. Thus, it becomes evident that the expression adds some elements to analysing the issue. However, it cannot be fully understood because the conceptual framework of personal data protection and privacy culture is much more complex. It encompasses more than state actions.

The second point provides a more comprehensive understanding of the issue at hand. A report from the EC mentions advances in the processing of a proposal for a Regulation to create the European Agency for the operational management of large-scale IT systems in the area of freedom, security, and justice. It was created definitively by Regulation (EU) 1077/2011.[20] Despite being a small agency, it has the mission of managing large-scale information systems, such as those dedicated to travel visas, the management of the Schengen Area, and EURODAC (*European Asylum Dactyloscopy Database*). It also contributed to the construction of new large-scale systems for the administrative integration of Member States. This Agency was reformulated by Regulation (EU) 2018/1726 and transformed into the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security, and Justice (EU-LISA).[21] The noteworthy point is that

[17] Alessandra Silveira and João Marques, "Autoridade Europeia para a Proteção de Dados" in *Instituições, órgãos e organismos da União Europeia*, ed. Joana Covelo de Abreu and Liliana Reis (Coimbra: Almedina, 2020), 157-163.

[18] Francisco Pereira Coutinho, "Comité Europeu para a Proteção de Dados" in *Instituições, órgãos e organismos da União Europeia*, ed. Joana Covelo de Abreu and Liliana Reis (Coimbra: Almedina, 2020), 163-168.

[19] European Data Protection Supervisor, "Opinion of the European Data Protection Supervisor on the Proposal for a Decision of the European Parliament and of the Council establishing a multiannual Community program on protecting children using the Internet and other communication technologies (2009/C 2/02)", (Brussels, January 7, 2009), 4, accessed July 22, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2009:002:FULL.

[20] European Union, "Regulation (EU) No 1077/2011 of the European Parliament and of the Council of October 25, 2011, establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice" (Brussels, January 11, 2011), accessed July 22, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011R1077&qid=1690060797879.

[21] European Union, "Regulation (EU) 2018/1726 of the European Parliament and of the Council

this Regulation underwent updates and consolidation in 2023. The text has some references to the expression "*data protection culture.*" The first of these is as follows: "*Consultation also included the SIS II and VIS rapporteurs on behalf of the European Parliament, representatives of the European Data Protection Supervisor and the Schengen Joint Supervisory Authority and addressed in particular the following issues: application of the relevant data protection provisions, and the data protection cultures within the institutions which have been proposed to manage the systems.*"[22]

The document works with two concepts of personal data protection culture. The first one refers to the excerpt above, which indicates the existence of an organisational culture of personal data protection. This concept relates to another element: the data protection culture of the Member State that will host the organisation. It is worth noting that the document in question also contains a report analysing the potential impact of establishing the new organisation. The following excerpt highlights the concern that cultural differences in personal data protection among institutions of the Member States may diminish the efforts of a managing body: "*Effective implementation and enforcement of data protection rules must be ensured. The SIS II, VIS, and EURODAC legal instruments contain specific data protection provisions applicable to SIS II, VIS, and EURODAC. Compliance with data protection requirements laid down in the specific legal instrument(s) for each system must be ensured under every option. Supervision by the European Data Protection Supervisor should be facilitated, and effective remedies must be in place. Nevertheless, different management structures may inherently have varying data protection cultures and would therefore be well-equipped to ensure proper implementation of data protection provisions. Under any of the options, data from the systems would be logically separated from each other and would, therefore, not be merged into one' pool.'*"[23]

The concern with standardised compliance regarding legal instruments is present in the document in question. Thus, as it becomes clear, in theory, the organisation's choice to manage the systems exceeded the appreciation only of the applicable legal rules. The objective was to indicate the need to analyse the potential effectiveness of the EU legal rules, with a particular contrast between the internal culture of personal data protection of the chosen organisation and the data protection culture of the Member State: "*The legal requirements on privacy and data protection as described in the legal instruments*

---

of November 14, 2018, on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011" (Brussels, November 28, 2018), accessed July 22, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1726.

[22] European Commission, "Accompanying document to the proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice and Proposal for a Council Decision conferring upon the Agency established by Regulation XX tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty – Impact assessment" (Brussels, June 24, 2009), accessed July 22, 2023, 9, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009SC0837&from=EN.

[23] European Commission, "Accompanying document to the proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice and Proposal for a Council Decision conferring upon the Agency established by Regulation XX tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty – Impact assessment" (Brussels, June 24, 2009), accessed July 22, 2023, 13, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009SC0837&from=EN.

establishing the systems are binding for every potential option and therefore are not differentiating factors. Compliance with data protection requirements laid down in specific legal instruments for each system has to be ensured. More important than reviewing the actual rules is to assess the effectiveness of oversight and factors influencing the internal data protection culture and awareness of the Management Authority. Another determining factor is the ability to withstand pressure from third parties to gain data access or compromise the system. In addition, it should be noted that the perception of the (risk of) abuse of personal data should also be avoided where possible, as this can undermine the trust of data subjects and public authorities in the Management Authority (which will be discussed in the section on mission creep). Furthermore, the political concerns around data protection, particularly in the European Parliament, make it an important issue. Any situation where there are more systems with different rules is likely to create complications for effective data protection (although not impossible to organize). Further complications can be expected if the host organization has its own existing data protection regime and supervision authorities, other than foreseen under the three systems."[24]

This 2009 report on the creation of EU-LISA presents a better-elaborated expression of the concept in question. It clarifies cultural differences among the various Member States and local organisations. The term "*data protection culture*" reappeared in 2013 in Article 47 (3) of the EDPS Internal Rules of Procedure, which determines that it: "*...shall organize regular workshops with representatives of international organizations with a view to sharing best practices and developing a data protection culture in those organizations.*"[25] In 2014, the EDPS reintroduced the expression in a preliminary report on the issue of Big Data: "*The EDPS promotes a 'data protection culture' in EU institutions and bodies where data protection principles find expression in all relevant areas of policy and Law. As a contribution to that aim, this preliminary Opinion seeks to stimulate a dialogue between experts and practitioners, including EU institutions and national regulatory authorities from the competition, consumer protection, and data protection fields. The EDPS will then reflect on the views and ideas arising from this exercise in a follow-up Opinion and include recommendations for action.*"[26]

The concept in this document repeats the logic by which the "*culture of personal data protection*" is a process driven by state actions, not indicating – or implicitly subsuming – societies and their social groups in these processes. Furthermore, the document does not provide elements to aid in conceptualising what a data protection culture entails.

In 2016, the year of approval of the GDPR and Directive (EU) 680/2016, the expression returns in a position paper of the Council of the European Union concerning the need for a new regulatory framework for EU law. There are two mentions. The first refers to the need to strengthen legal mechanisms for holding

[24] European Commission, "Accompanying document to the proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice and Proposal for a Council Decision conferring upon the Agency established by Regulation XX tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty - Impact assessment" (Brussels, June 24, 2009), accessed July 22, 2023, 90, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009SC0837&from=EN.

[25] European Data Protection Supervisor, "Executive Summary of the Preliminary Opinion of the European Data Protection Supervisor on privacy and competitiveness in the age of big data (2014/C 225/07)" (Brussels, July 16, 2014), accessed: July 22, 2023, 7, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014XX0716(01).

[26] European Data Protection Supervisor, "Executive Summary of the Preliminary Opinion of the European Data Protection Supervisor on privacy and competitiveness in the age of big data (2014/C 225/07)" (Brussels, July 16, 2014), accessed: July 22, 2023, 7, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014XX0716(01).

personal data processors accountable: "*In order to achieve the objectives of the Regulation, the Council Position at first reading strengthens the accountability of controllers (responsible for determining the purposes and the means of the processing of personal data) and processors (responsible for processing personal data on behalf of the controller) to promote a real data protection culture. Against that background, throughout the Regulation, a risk-based approach is introduced, which allows for the modulation of the obligations of the controller and the processor according to the risk of the data processing they perform. Furthermore, codes of conduct and certification mechanisms contribute to compliance with data protection rules. This approach prevents overly prescriptive rules and reduces administrative burden without reducing compliance. Moreover, the dissuasive character of the potential penalties that can be imposed creates incentives for controllers to comply with the Regulation.*"[27]

The Council of the European Union points out that the GDPR will potentially create (or strengthen) this culture of personal data protection. Additionally, this culture will be coherent and stimulated through cooperation through legal mechanisms or state actions. Once again, it is noteworthy that there is no indication of the issue as a more complex social process. The second mention is more enlightening, albeit implicit, as it indicates the contrast between this desirable culture of personal data protection with a "*culture of commercial complaints,*" as can be seen in the extract below: "*A data subject has the right to mandate bodies, organisations or associations that fulfil specific criteria, such as working on a non-profit basis and being active in the field of data protection, to lodge the complaint on his or her behalf and to exercise the rights of judicial remedy on his or her behalf and to exercise the right to receive compensation on his or her behalf if provided for by Member State law. These specific criteria aim to avoid the development of a commercial claims culture in the field of data protection. In addition, Member States may provide that any such body, organization, or association, independently of a data subject's mandate, has in such Member State the right to lodge a complaint with the competent supervisory authority and to exercise the rights on judicial remedy, if it considers that the rights of a data subject have been infringed as a result of the processing of personal data that is not in compliance with the Regulation.*"[28]

The objective, therefore, is to foster a culture of personal data protection, which differs from a mere pursuit of compensation, as evident in the statement above. Civil society emerges at this point. The document indicates an active space for citizen action, individually or through associations. Thus, it demonstrates the claim that the Council of the European Union considers that the GDPR can foster the construction of a non-profit associative culture in favour of the effectiveness of the rights of personal data subjects, which is also noteworthy. The same logic of applying EU law as a privileged means for promoting a culture of personal data protection returns, in 2017, with the document that sets in motion the Proposal for replacing Regulation (EC) 45/2001, which lays down rules for the protection of personal data within the

[27] Council of the European Union, "Position (EU) No 6/2016 of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of 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 repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) – adopted by the Council on April 8, 2016 (2016/C 159/01)" (Brussels, May 3, 2016), 84, accessed July 22, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2016:159:FULL.

[28] Council of the European Union, "Position (EU) No 6/2016 of the Council at First Reading with a view to the adoption of a Regulation of the European Parliament and of 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 repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) – adopted by the Council on April 8, 2016 (2016/C 159/01)" (Brussels, May 3, 2016), 96, accessed July 22, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2016:159:FULL.

internal administration of the EU institutions and bodies. This information is in Recital 68 of that proposed Regulation: "*To strengthen the supervisory role of the European Data Protection Supervisor and the effective enforcement of this Regulation, the European Data Protection Supervisor should, as a sanction of last resort, have the power to impose administrative fines. The fines should aim at sanctioning the institution or body – rather than individuals – for non-compliance with this Regulation, to deter future violations of this Regulation, and to foster a culture of personal data protection within the Union institutions and bodies. This Regulation should indicate infringements and the upper limits and criteria for setting the related administrative fines. The European Data Protection Supervisor should determine the number of fines in each individual case by taking into account all relevant circumstances of the specific situation, with due regard to the nature, gravity, and duration of the infringement and its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. When imposing an administrative fine on a Union body, the European Data Protection Supervisor should consider the proportionality of the amount of the fine. The administrative procedure for the imposition of fines on Union institutions and bodies should respect the general principles of Union law as interpreted by the Court of Justice of the European Union.*"[29]

The three most recent EU documents mentioning the term are annual assessments on the application of the GDPR. Subsequently, each document is analysed separately. The first document dates from 2018. It relates the concept of data protection culture to establishing a common standard of action and behaviour among the various Member States. From a legal perspective, this objective links directly to the duties of cooperation and consistency, which should guide the actions of the various DPAs across different Member States, as outlined in Chapter VII (Article 60 and onwards) of the GDPR. Thus, from the point of view of public policies for the protection of personal data in the EU, the role of the EDPB is crucial: "*The smooth and efficient functioning of the European Data Protection Board is therefore a condition for the system to function well. More than ever before, the European Data Protection Board will have to create a common data protection culture among all the national data protection authorities to ensure that the rules of the Regulation are interpreted consistently. The Regulation fosters cooperation between the data protection authorities by giving them the tools to cooperate effectively and efficiently: they will notably be able to do joint operations, adopt decisions in agreement and resolve divergences they might have concerned with the interpretation of the Regulation within the Board by means of opinions and biding decisions. The Commission encourages the data protection authorities to embrace these changes and adjust their functioning, financing, and work culture to be able to meet the new rights and obligations.*"[30]

Therefore, according to this document, the concept of personal data protection culture refers to a cultural change pursued by the EU institutions. Such a change is understandable as harmonising an EU regime to protect personal data between the various Member States. The means of implementing the changes to archive this goal are in a set of actions by many players, as seen in the three tables below.

[29] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data 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 (Brussels, January 1, 2017), accessed July 22, 2023, 30-31, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1609341026005&uri=CELEX%3A52017PC0008.

[30] European Commission, "Communication from the Commission to the European Parliament and the Council. Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of May 25, 2018" (Brussels, January 1, 2018), accessed July 22, 2023, 10, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0043.

This document brings a more developed concept than before. Although there is still an obvious marking of state actions, they also have a dimension related to companies. Understanding the concept of a culture of personal data protection and privacy is essential. For example, Table 1 presents actions to promote the culture of personal data protection in the EU, focusing on the EC. Two actions in Table 1 are worth highlighting. The first action is maintaining a dialogue between data protection authorities and other actors, including local public authorities, commissioners, the private sector, and the legal community. The second is the spread of GDPR in other regions and countries, emphasising Latin America. It is essential to note the timeframe of the report. It dates back to 2018, that is, the beginning of the enforcement of the GDPR, and outlines some actions that have already been carried out up to that point (past), others that were ongoing (present), and those that are expected to come into play (future).

Table 1

Actions to actualise the culture of personal data protection in the EU by the EC[31]

Past, present, and future	Supporting Member States and their authorities. The Commission has been working very closely with the Member States to support their work during the transition period, with a view to ensuring the highest possible level of consistency. To this end, the Commission has set up an Expert Group to accompany the Member States in their effort to prepare for the Regulation. The Group, which already met 13 times, acts as a forum where the Member States can share their experiences and expertise. The Commission also engaged in bilateral meetings with Member States' authorities to discuss issues arising at national level.
Past, present, and future	Supporting the individual data protection authorities and the creation of the European Data Protection Board. The Commission has been actively supporting the work of the Article 29 Working Party also in view of ensuring a smooth transition to the European Data Protection Board.
Past, present, and future	International outreach. The Regulation will further strengthen the EU's ability to actively promote its data protection values and facilitate cross-border data flows by encouraging the convergence of legal systems globally. (...). Furthermore, several countries and regional organisations outside the EU – from our immediate neighbourhood to Asia, Latin America, and Africa –, are adopting new data protection legislation or updating the existing one in order to harness the opportunities offered by the global digital economy and respond to the growing demand for stronger data security and privacy protection. While countries differ in their approach and their level of legislative development, there are signs that the Regulation serves increasingly as a reference point and a source of inspiration. In this context, the Commission is pursuing its international outreach in line with its January 2017 Communication by actively engaging with key trading partners, notably in East and South-East Asia and Latin America, to explore the possibility to adopt adequacy decisions (...). At the same time, the Commission is working with stakeholders with a view to harnessing the full potential of the GDPR toolkit for international transfers by developing alternative transfer mechanisms adapted to the particular needs of specific industries and/or operators.

[31] European Commission, "Communication from the Commission to the European Parliament and the Council. Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of May 25, 2018" (Brussels, January 1, 2018), accessed July 22, 2023, 10, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0043.

Past, present, and future	Engaging with stakeholders. The Commission has organised a number of events to reach out to stakeholders. A new workshop aimed at consumers is planned for the first quarter of 2018. Dedicated sectoral discussions in areas such as research and financial services have also taken place. The Commission has also set up a multi-stakeholder group on the Regulation composed of civil society and business representatives, academics, and practitioners. This group will advise the Commission on how to achieve an appropriate level of awareness about the Regulation among stakeholders. Finally, the European Commission, through its Framework Program for Research and Innovation Horizon 2020, has funded actions to develop tools supporting the effective application of the rules under the Regulation in relation to consent and privacy-preserving methods of data analytics such as multi-party computing and homomorphic encryption.
Future	Work with Member States. The Commission will continue working with Member States in the lead-up to May 2018. From May 2018 onward, it will monitor how Member States apply the new rules and take appropriate action as necessary.
Future	New online guidance in all EU languages and awareness-raising activities. The Commission is making available practical guidance materials to help businesses, in particular SMEs, public authorities, and the public to comply with and benefit from the new data protection rules. The guidance takes the form of a practical online tool available in all EU languages. The online tool will be regularly updated and is intended to serve three main target audiences: citizens, businesses (SMEs) and other organisations, and public administrations. It comprises questions and answers selected based on feedback received from stakeholders with practical examples and links to various sources of information (e.g., articles of the Regulation, guidelines of Article 29 Working Party/European Data Protection Board, and materials developed at the national level). The Commission will regularly bring up to date the tool, adding questions and updating the answers based on the feedback received and in the light of any new issues arising from implementation. The guidance will be promoted through an information campaign and dissemination activities in all Member States, targeting businesses and the public. As the Regulation provides for stronger individual rights, the Commission will also engage in awareness-raising activities and participate in events across the Member States to inform citizens about the benefits and impact of the Regulation.
Future	Financial support for national campaigns and awareness raising. The Commission is supporting awareness-raising and compliance efforts undertaken at the national level by awarding grants that can be used to provide training to data protection authorities, public administrations, legal professions, and data protection officers and to familiarise them with the Regulation. Around EUR 1.7 million will be allocated to six beneficiaries, covering more than half of the EU Member States. Funding will be targeted at local public authorities, including data protection officers of local public authorities, public authorities and from the private sector, judges, and lawyers. The grants will be used to develop training materials for data protection authorities, data protection officers, and other professionals, as well as 'train the trainer' programs. The Commission has also issued a call for proposals specifically aimed at data protection authorities. It will have a total budget of up to EUR 2 million and will support them in reaching out to stakeholders. The objective is to provide 80 % co-financing to measures taken by data protection authorities in 2018-2019 to raise awareness among businesses, in particular SMEs, and reply to their queries. This funding can also be used to raise awareness among the public.

Future	Assessing the need to make use of the Commission's empowerment. The Regulation allows the Commission to issue implementing or delegated acts to further support the implementation of the new rules. The Commission will only make use of this empowerment when there is a clearly demonstrated added value and based on feedback from stakeholders' consultation. In particular, the Commission will look into the issue of certification based on a study contracted with external experts and input and advice on this issue from the multi-stakeholder group on the Regulation established at the end of 2017. The work done by the European Union Agency for Network and Information Security (ENISA) in the field of cybersecurity will also be relevant in this context.
Future	Integration of the Regulation into the EEA Agreement. The Commission will pursue its work with the three EFTA States (Iceland, Liechtenstein, and Norway) in the European Economic Area (EEA) to integrate the Regulation into the EEA Agreement. It is only once the integration of the Regulation into the EEA Agreement is in force that personal data can flow freely between EU and EEA countries in the same way as they do between EU Member States.
Future	Withdrawal of the United Kingdom from the EU. In the context of the negotiations of a withdrawal agreement between the EU and the United Kingdom on the basis of Article 50 of the Treaty on the European Union, the Commission will pursue the objective to ensure that the provisions of Union law on personal data protection applicable on the day preceding the withdrawal date continue to apply to personal data in the United Kingdom processed before the withdrawal date- For example, the individuals concerned should continue to have the right to be informed, the right of access, the right to rectification, to erasure, to restriction of processing, to data portability as well as the right to object to processing and not to be subject to a decision based solely on automated processing, based on relevant provisions of Union law applicable on the withdrawal date. Personal data referred to above should be stored no longer than is necessary for the purposes for which the personal data was processed. As of the withdrawal date, and subject to any transitional arrangement that may be contained in a possible withdrawal agreement, the rules of the Regulation for transfers of personal data to third countries will apply to the United Kingdom.
Future	Taking stock in May 2019. After May 25, 2018, the Commission will closely monitor the application of the new rules and will stand ready to act should any significant problems arise. One year after the Regulation enters into application (2019), the Commission will organise an event to take stock of different stakeholders' experiences of implementing the Regulation. This will also feed into the report the Commission is required to produce by May 2020 on the evaluation and review of the Regulation. This report will focus on international transfers and the provisions on cooperation and consistency which pertain to the work of data protection authorities.

Table 2 deals with the EC's diagnosis regarding the actions of the Article 29 Group and its consolidation as the EDPB. Table 3 will address the obligations of the Member States, as defined by the EC, to pursue the total effectiveness of the GDPR.

Table 2

Actions to actualise the personal data protection culture in the EU by EDPB[32]

Present and future	The Article 29 Working Party, which groups all national data protection authorities, including the European Data Protection Supervisor, is crucial in preparing the Regulation application by issuing guidelines for companies and other stakeholders. As enforcers of the Regulation and direct contacts for stakeholders, national data protection authorities are best placed to provide additional legal certainty regarding the interpretation of the Regulation. Guidelines or working documents by the Article 29 Working Party in view of the entry into application of the Regulation: right to data portability, data protection officers, designation of the lead supervisory authority, data protection impact assessment, administrative fines, profiling, data breach, consent, transparency, certification and accreditation, adequacy referential, binding corporate rules for controllers, binding corporate rules for processors.

Finally, Table 3 lists actions indicated by the EC for the Member States in favour of the effectiveness of the GDPR. In addition to suggesting a dialogue dimension between EU and Member State bodies, it points to the need to engage in dialogue with businesses.

Table 3

Actions to actualise the personal data protection culture by Member States[33]

Present and future	Member States to finalise the set-up of the legal framework at the national level. The Regulation is directly applicable in all the Member States. This means that it enters into force and applies irrespective of any national law measures: the provisions of the Regulation can normally be directly relied on by citizens, businesses, public administrations, and other organisations processing personal data. Nevertheless, in accordance with the Regulation, Member States must take the necessary steps to adapt their legislation by repealing and amending existing laws, setting up national data protection authorities, choosing an accreditation body, and laying down the rules for the reconciliation of freedom of expression and data protection. Also, the Regulation gives Member States the possibility to further specify the application of data protection rules in specific fields: public sector, employment and social security, preventive and occupational medicine, public health, archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, national identification number, public access to official documents, and obligations of secrecy. In addition, for genetic data, biometric data and data concerning health, the Regulation empowers Member States to maintain or introduce further conditions, including limitations.

[32] European Commission, "Communication from the Commission to the European Parliament and the Council. Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of May 25, 2018" (Brussels, January 1, 2018), accessed July 22, 2023, 10, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0043.

[33] European Commission, "Communication from the Commission to the European Parliament and the Council. Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of May 25, 2018" (Brussels, January 1, 2018), accessed July 22, 2023, 10, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0043.

Present and future	Data protection authorities to ensure that the new independent European Data Protection Board is fully operational. It is essential that the new body established by the Regulation, the European Data Protection Board, the successor of the Article 29 Working Party, is fully operational as of May 25, 2018. (...). The smooth and efficient functioning of the European Data Protection Board is, therefore, a condition for the system to function well. More than ever ~~before~~, the European Data Protection Board will have to create a common data protection culture among all the national data protection authorities to ensure that the rules of the Regulation are interpreted consistently. The Regulation fosters the cooperation between the data protection authorities by giving them the tools to cooperate effectively and efficiently: they will notably be able to do joint operations, adopt decisions in agreement and resolve divergences they might have concerned the interpretation of the Regulation within the Board by means of opinions and biding decisions. The Commission encourages the data protection authorities to embrace these changes and adjust their functioning, financing, and work culture to be able to meet the new rights and obligations.
Present and future	Member States to provide the necessary financial and human resources to national data protection authorities. The establishment of fully independent supervisory authorities in each Member State is essential to ensure the protection of natural persons regarding the processing of their personal data in the EU. Supervisory authorities cannot effectively safeguard individual rights and freedoms unless they act completely independently. Any failure to ensure their independence and the effective exercise of their powers has a wide-ranging negative impact on the enforcement of data protection legislation. The data protection authorities are the natural interlocutors and first point of contact for the public, businesses, and public administrations for questions regarding the Regulation. The data protection authorities' role includes informing controllers and processors of their obligations and raising awareness among the general public and understanding of the risks, rules, safeguards, and rights in relation to data processing. It does not mean, however, that controllers and processors should expect to be provided by the data protection authorities with the kind of tailored, individualised legal advice that only a lawyer or a data protection officer can provide. The national data protection authorities therefore play a central role, but the relative imbalance between the human and financial resources allocated to them in different Member States can jeopardise their effectiveness and, ultimately, the complete independence required under the Regulation. It can also negatively impact the way the data protection authorities are able to exercise powers such as their investigation powers. Member States are encouraged to fulfil their legal obligation to provide their national data protection authority with the human, technical, and financial resources, premises, and infrastructure necessary for the effective performance of its tasks and exercise of their powers.

Present and future	Businesses, public administrations, and other organisations process data to get ready for the application of the new rules. The Regulation did not substantially change the core concepts and principles of the data protection legislation put in place back in 1995. This should mean that most controllers and processors, provided that they are already in compliance with the existing EU data protection laws, will not need to make major changes to their data processing operations to comply with the Regulation. The Regulation impacts most on operators whose core business is data processing and/or dealing with sensitive data. It also impacts on those that regularly and systematically monitor individuals on a large scale. These operators will most probably have to appoint a data protection officer, conduct a data protection impact assessment, and notify data breaches if there is a risk to the rights and freedoms of individuals. By contrast, operators, in particular SMEs, which do not engage in high-risk processing as their core activity, will normally not be subject to these specific obligations of the Regulation. It is important for controllers and processors to undertake thorough reviews of their data policy cycle to clearly identify which data they hold, for what purpose, and on what legal basis (e.g., cloud environment; operators in the financial sector). They also need to assess the contracts in place, those between controllers and processors, the avenues for international transfers, and the overall governance (what IT and organisational measures to have in place), including the appointment of a Data Protection Officer. An essential element in this process is to ensure that the highest level of management is involved in such reviews, provides its input, and is regularly updated and consulted on changes to the business's data policy. However, while big companies are actively preparing for the application of the new rules, many SMEs are not yet fully aware of the forthcoming data protection rules.
Present and future	To inform stakeholders, in particular citizens and small and medium-sized businesses. The success of the Regulation rests on proper awareness of all those affected by the new rules (the business community and other organisations processing data, the public sector, and citizens). At the national level, the task of raising awareness and being the first point of contact for controllers, processors, and individuals lies primarily with the data protection authorities. As enforcers of data protection rules in their territory, data protection authorities are also the best placed to explain the changes introduced by the Regulation to companies and the public sector and to familiarise citizens with their rights. Data protection authorities have started informing stakeholders in line with the specific national approach. Some hold seminars with public administrations, including at regional and local levels, and run workshops with different business sectors to raise awareness about the main provisions of the Regulation. Some run specific training programs for data protection officers. Most of them provide information materials in various formats on their websites (checklists, videos, etc.). However, there is not yet a sufficiently widespread level of awareness among ~~the~~ citizens of the changes and enhanced rights that the new data protection rules will bring. The training and awareness-raising initiative set in motion by Data Protection Authorities should be continued and intensified, with a particular focus on SMEs. Furthermore, national sectoral administrations can support the activities of data protection authorities and based on their input, do their own outreach among the different stakeholders.

The concept of a personal data protection culture extracted from this document has some legal content since it refers to the effectiveness of prescriptions of EU law in a coherent way in the various Member States. It also acquires an international bias. The most evident example refers to the countries of the European Economic Area (Iceland, Liechtenstein, and Norway). However, the EC annual analysis document of 2018 refers to countries in Asia, the Americas, and Africa, which would already

have their national laws on personal data protection – or would be approving them. The document also mentions companies as focal points of dialogue to promote the expansion of a culture of personal data protection, as well as lists some scientific and technological development programs through which the identification of societies and social groups can be perceived, albeit implicitly.

The second document is from 2019. It is precisely the reassessment point of the efforts in applying the GDPR, as defined by the 2018 document. The concept of an EU personal data protection culture continues to feature prominently. Central to its emergence is the EDPB, which has a strategic and operational role in international cooperation among EU Member States regarding personal data protection, with the aim of harmonising Regulations. It indicates, however, that it would require more effort to reach the level of effectiveness of the personal data protection culture. Nevertheless, before continuing with this issue, there is a specific mention of the various social behaviours within the Member States, which deserves to be transcribed: "*That being said, the success of the Regulation should not be measured by the number of fines imposed, but by changes in the culture and behaviour of all actors involved. In this context, data protection authorities have other tools at their disposal such as imposing a temporary or definitive limitation on processing including a ban or ordering the suspension of data flows to a recipient in a third country.*"[34]

This question about the measurability of personal data protection is a crucial issue despite several challenges. It may refer to the difficulties faced, over decades, in Law and Society research on the problems of defining cultural issues through quantitative elements. Returning to the second document, it is worth mentioning that the EC attributes a significant role to the EDPB, as it is the coordinating and harmonising body for the various DPAs, which are responsible for supervising the application of the GDPR within the Member States: "*Towards the creation of an EU data protection culture. The new governance system still needs to realise its full potential. It is important for the Board to further streamline its decision-making and develop a common EU data protection culture among its members. The possibilities for data protection authorities to pool their efforts on issues affecting more than one Member State, for instance to carry out joint investigations and enforcement measures, can contribute to such an objective while mitigating resources' constraints. Many stakeholders wish to see even more cooperation and a uniform approach by national data protection authorities. They also request more consistency in the advice provided by data protection authorities and a full alignment of national guidelines with those of the Board. Some also expect further clarifications of key concepts of the Regulation, such as the risk-based approach, taking particular account of the concerns notably of small and medium size enterprises. In this context, allowing stakeholders to better feed into the work of the Board is essential. This is why the Commission welcomes the systematic public consultation organised by the Board on guidelines. This practice, together with the organisation of stakeholder workshops on targeted topics at an early stage of the reflection, should be continued and amplified to ensure the transparency, inclusiveness and relevance of the work of the Board.*"[35]

Furthermore, the EC reiterated the need for various actions to continue, such as raising awareness among public administrations, citizens, and civil society.

[34] European Commission, "Communication from the Commission to the European Parliament and the Council. Data protection rules as a trust-enabler in the EU and beyond – taking stock" (Brussels, July 24, 2019), accessed July 22, 2023, 5-6, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0374.

[35] European Commission, "Communication from the Commission to the European Parliament and the Council. Data protection rules as a trust-enabler in the EU and beyond – taking stock", 6-7, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0374.

Additionally, there is a specific mention of the need to support the development of the right to personal data protection. The second report concludes by communicating to the European Parliament and Council that data protection rules work as an instrument that generates trust inside and outside the EU. This conclusion reinforces the point of view through which the EC emphasises that it has made efforts to disseminate the issue. It also lists several future actions regarding the protection of personal data. As the issue advances in the EU regulatory agenda, what is perceived is the reception of a more active concept – concerning societies – in the concept of personal data protection culture.

In the third document, from 2020, the subject of the EU's personal data protection culture returns. However, it is given an international dimension, with an account of the EU's bilateral cooperation actions and its performance in multilateral bodies. Furthermore, the dissemination of actions and standards for the protection of personal data to other countries and regions of the world is indicated, including Latin America, explicitly: "*Building on this trend, the Commission has intensified its dialogue in a number of bilateral, regional, and multilateral fora to foster a global culture of respect for privacy and develop elements of convergence between different privacy systems. In its efforts, the Commission has relied and will continue to count on the active support of the European External Action Service and the network of EU delegations in third countries and missions to international organisations. This has also allowed for greater consistency and complementarity between different aspects of the external dimension of EU policies – from trade to the new EU-Africa partnership. The G20 and G7 have also recently recognised the contribution of data protection to trust in the digital economy and data flows, in particular through the concept of 'Data Free Flow with Trust' originally proposed by the Japanese G20 Presidency. The Data Strategy highlights the Commission's intention to continue promoting data sharing with trusted partners while fighting against abuses such as disproportionate access of (foreign) public authorities to personal data (…). This has included actively engaging with key partners with a view to reaching an 'adequacy decision.' The effect of such a decision is to enable the safe and free flow of personal data to the concerned third country without the need for the data exporter to provide further safeguards or obtain any authorisation. In particular, the EU-Japan mutual adequacy decisions, which entered into force in February 2019, created the world's largest area of free and safe data flows. In addition, the adequacy process with the Republic of Korea is at an advanced stage and exploratory talks are ongoing with other important partners in Asia and Latin America.*"[36]

This document, from 2020, also has an excerpt that refers to the training of citizens for the protection of personal data in the context of digital transformation: "*The GDPR set up an innovative governance system, based on independent data protection authorities in the Member States and their cooperation in cross-border cases and within the European Data Protection Board ('the Board'). The general view is that data protection authorities have made balanced use of their strengthened corrective powers, including warnings and reprimands, fines and temporary or definitive processing limitations. The Commission notes that the authorities made use of administrative fines ranging from a few thousand euros to several million, depending on the gravity of the infringements. Other sanctions, such as bans on processing, may have an equally, if not higher deterrent effect than fines. The ultimate objective of the GDPR is to change the culture and behaviour of all actors involved for the benefit of the individuals. More detailed information on the use of the corrective powers by*

[36] European Commission, "Communication from the Commission to the European Parliament and the Council. Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation (SWD(2020) 115 final)" (Brussels, June 24, 2020), 12-13, accessed July 22, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264.

data protection authorities is presented in the accompanying staff working document. (...). However, developing a truly common European data protection culture between data protection authorities is still an ongoing process. Data protection authorities have not yet made full use of the tools the GDPR provides, such as joint operations that could lead to joint investigations. At times, finding a common approach meant moving to the lowest common denominator and as a result, opportunities to foster more harmonisation were missed. (…). According to a Fundamental Rights Survey, 69% of the EU population above the age of 16 have heard about the GDPR, and 71% of people in the EU know about their national data protection authority. Individuals are increasingly aware of their rights: the rights of access, rectification, erasure, and portability of their personal data, the right to object to a processing, as well as enhanced transparency. The GDPR strengthened procedural rights, encompassing the right to lodge a complaint with a data protection authority, including through representative actions, and to judicial redress. Individuals are increasingly using these rights, but there is a need to facilitate their exercise and their full enforcement. The reflections being led by the Board will clarify and further facilitate the exercise of individual rights, while the proposed Directive on representative actions, once adopted, is expected to enable individuals to bring collective actions in all Member States and will lower the costs of cross-border actions."[37]

In addition to the three annual reports from the EC, a fourth document that stands out is the European Declaration on Digital Rights and Principles for the Digital Decade, published in February 2023.[38] This document contains digital principles and digital rights that assist Member States and the EC in cooperating to meet the general objectives set out in the program for 2030 ("*Guide for the Digital Decade*").[39] It also aims to promote European values in the context of digital transformation.[40] This document has six relatively short chapters, each focusing on central themes. The first chapter, titled "*Prioritizing People in the Digital Transformation Process*", emphasises strengthening democratic processes and digital transformation, ensuring fundamental rights, and leveraging technology to benefit EU citizens to achieve these goals. The second chapter addresses "*Solidarity and Inclusion*", which involves social responsibilities within the digital transformation, respect for cultural and linguistic diversities, education, online public services, fair working conditions, and promotion of access and connectivity. Chapter three is titled "*Freedom of Choice*" and discusses a secure digital environment, interoperability, and ethical and transparent boundaries for using artificial intelligence. The fourth chapter deals with "*Participation*" in the digital public space that concerns freedom of expression and media pluralism, with efforts to combat misinformation. Chapter five deals with "*Security, Protection, and*

[37] European Commission, "Communication from the Commission to the European Parliament and the Council – data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation (SWD(2020) 115 final)" (Brussels, June 24, 2020), 5 and 8, accessed July 22, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0264.

[38] European Union, "European Declaration on Digital Rights and Principles" (Brussels, February 7, 2023), accessed July 22, 2023, https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles.

[39] European Commission, "Proposal for a Decision of the European Parliament and the Council establishing the 2030 Policy Programme' Path to the Digital Decade' (Text with EEA relevance) (SWD(2021) 247 final)" (Brussels, September 15, 2021), accessed July 22, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0574.

[40] Council of the European Union, "Declaration on digital rights and principles: EU values and citizens at the centre of digital transformation", Press release, Brussels, November 14, 2022, accessed July 22, 2023, https://www.consilium.europa.eu/pt/press/press-releases/2022/11/14/declaration-on-digital-rights-and-principles-eu-values-and-citizens-at-the-centre-of-digital-transformation.

Empowerment", encompassing cybersecurity. However, it deserves particular attention for addressing the central theme of this discussion, which is protecting personal data and controlling it. The document addresses, in this sense, the principles of privacy "*by design*" and "*by default*," stating that everyone should have access to technologies, products, and services that "*from their design, are safe and secure and protect privacy, resulting in a high level of confidentiality, integrity, availability, and authenticity of the information processed.*" Another topic within personal data protection concerns children and young people in the digital environment.

3. Conclusion

Protecting personal data is considered an autonomous fundamental right, with legal provisions in the EU and Member States law and benefiting from public policies for its implementation. Furthermore, the EU makes evident efforts to disseminate its standards internationally through cooperation actions, inspiring a global model or even driven by commercial imperatives. This combination of perspectives aids in the diffusion and influence of the EU's data protection standards in reaching other regions of the world, especially Latin America. This collection of pragmatic imperatives with the symbolic dimension is its central distinguishing feature. Moreover, it has been operating over the years. Some interviewees reported this reception and integration of EU law in their countries. For example, one of the interviewees reported that, since the advent of the old Directive 95/46/EC, the legal systems of several Latin American countries, including Mexico, had already passed through the influence of the EU: "*I believe that, after all, much of the context of the development of personal data that has occurred in Latin America comes from the European Union, from the 1995 Directive, that establishes data protection principles. At that time, I think that the Directive on data protection was very noble because it set good precedents. At some point, it concluded that the Directive was no longer sufficient, and the European Regulation on personal data was enacted based on its principles. Look at several of the data protection legislation that exists in Latin America. You will find the principles from the Directive and the rights of the holders, the rights of access, rectification, cancellation, and opposition (translated by the authors).*"[41]

Another example of influence is related to EC adequacy decisions, which existed in Directive 95/45/EC and the GDPR. They reveal efforts by Latin American countries to align themselves with EU standards. Additionally, the Spanish Royal Decree for the Protection of Personal Data (Ley Orgánica 15/1999), in many cases, served as a reference for many Latin American countries to align their national legal norms with the EU model. One of the notable cases is that of Argentina, one of the first countries to obtain an adequacy decision from the EC under the terms of the old Directive: "*In a way, this certification request aligns us with European legislation and our Law is almost a copy, except for the habeas data part and some other things, because we are a different country from Spain. That is, we are, in fact, a federal country. However, from the Spanish Law, we applied the European criteria to import it into our national criteria. Until our standards were aligned, we did this always looking at European legislation (authors' translation).*"[42]

---

[41] MEX8ACA, in *Pesquisa documental e de campo sobre autoridades de proteção de dados na América Latina: o conceito social e institucional de privacidade e de dados pessoais – Anexo 2 (entrevistas não identificadas) – volume 2*, Alexandre Veronese *et al.* (Brasília: Fapesp, January 31, 2023), 611.

[42] ARG7GOV, in *Pesquisa documental e de campo sobre autoridades de proteção de dados na América Latina: o conceito social e institucional de privacidade e de dados pessoais – Anexo 2 (entrevistas não identificadas) – volume 2*, Alexandre Veronese *et al.* (Brasília: Fapesp, January 31, 2023), 1314.

Still, in the recent discussions regarding the update of Argentina's data protection legislation, the GDPR was also an essential source of inspiration, as explained by one of the interviewees: "*They have always looked at European legislation, trying to update the principles of Directive 95/46, first; and then, once [in Europe], they started discussing the early drafts of the, let us say, General Data Protection Regulation. [They began] incorporating that in 2012. This movement happens by incorporating some of these proposed rules. The bills already included, in some cases, texts that were already in the draft of the General Data Protection Regulation. However, they never came, until now, [to change]. Our Law had no changes. The latest reform projects appear after the entry into force [of the GDPR]. Yes. [They] copy a lot and bring what, in 2017, were the data protection standards. Nevertheless, [they are proposals] that do not expressly bring, for example, the 'right to be forgotten' (authors' translation).*"[43]

From these examples, a key movement in the so-called "*Brussels effect*" is extracted, in which EU legislation goes to other latitudes on various topics, in this case, the right to the protection of personal data. Nevertheless, building a culture of personal data protection within the EU Member States is still a challenge. After all, it is necessary to reduce internal asymmetries and differences in the interpretation and application of Law to increase the potential for external influence. Therefore, the internal dynamics of the concatenation of the policies of the Member States – and their national societies – is also an essential part of this movement of attempted global influence. It is reasonable that the documents of the EC refer to the need to build a culture of personal data protection that encompasses all the Member States that comprise it. From a substantive point of view, it is clear that social, political, and economic processes share a clear connection with the cultural issue. Of course, the documents analysed have both a legal and technical character. However, it is interesting to note that these elements – legal and technical – always refer to the behaviours (actions and reactions) of defined actors (specific state entities and organisations, for example) and undefined actors (citizens, companies, local authorities, local administrations, among others). This movement comes along with the attempt to aggregate a concept of personal data protection legally and culturally into social practices. This dynamic characteristic – an ongoing social process in which there may be different speeds and even setbacks – already demonstrates the difficulty of quantitatively measuring greater or lesser personal data protection. This issue also makes it difficult to differentiate specific cultural patterns or types of personal data protection within the societies of the EU Member States. Although this dilemma is evident, and the EU documents do not resolve the quantification issue, the collected data offer some qualitative suggestions that one can incorporate into a discussion about the culture of privacy protection and personal data, focusing on Latin America. After all, perhaps the most challenging aspect of the social effectiveness of law is strictly dealing with crucial elements that are – in a way – diaphanous, like social beliefs. In a subsequent article, the same subject will come to light from another perspective. The forthcoming article will present more detailed data from field research on the reception and integration of personal data protection and privacy in the researched Latin American countries.

[43] ARG7GOV, in *Pesquisa documental e de campo sobre autoridades de proteção de dados na América Latina: o conceito social e institucional de privacidade e de dados pessoais – Anexo 2 (entrevistas não identificadas) – volume 2*, 1314.