United Nations A/HRC/49/55

General Assembly

Distr.: General
13 January 2022
English
Original: Spanish

Human Rights Council
Forty-ninth session
28 February–1 April 2022
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Privacy and personal data protection in Ibero-America: A step towards globalization?

Report of the Special Rapporteur on the right to privacy, Ana Brian Nougrères

Summary

Ibero-America has seen some highly interesting developments in the area of privacy and personal data protection since the start of the twenty-first century.

This report describes the current situation in respect of privacy in Ibero-America, focusing on personal data protection, the historical background and the international approach. The Special Rapporteur analyses the issues through the lens of developments in the Uruguayan system over the last 20 years. She also describes the evolution of personal data protection systems in other Ibero-American countries before, in the final section, considering how these systems have coalesced in recent years to form the Ibero-American personal data protection system.

The Special Rapporteur suggests that the Ibero-American data protection system could provide a model for a way of working collaboratively towards a world where the principles of privacy and personal data protection are mutually agreed upon and respected, leading to the implementation of digital privacy standards, and where integration and harmonization are goals that can be achieved without departing from the ethical principles that guarantee respect for human diversity.

I. Introduction

1. The principles of privacy and personal data protection have developed as a result of growing concerns around advances in information and communication technologies, which provide ever greater possibilities for information management and manipulation but also have the potential to infringe on individuals' lives, freedom and dignity.

2. The evolution of technology has reshaped the world, providing new forms of communication, socialization, education and work and giving rise to new approaches to health care, culture and social development. The principles of privacy and personal data protection, which are fundamental individual rights, are now of greater importance for human dignity than ever before, in that they serve to promote autonomy, decision-making, innovation and, ultimately, the development of the human personality.

3. Artificial intelligence, blockchain technology, information processing speed, virtual reality, augmented reality, biotechnology, robotics, the Internet of things, mass video surveillance and 3D printing are disruptive phenomena that have brought with them profound changes to the way we organize our daily lives.

4. The pandemic has not only accelerated digitization processes; it has also led to technology being ever more closely integrated into our daily lives. While this has great benefits, it also brings serious risks, especially for information security, privacy and personal data processing.

5. In this context, it is important to bear in mind that the individual is at the centre of any regulatory system; that, in democratic societies, the recognition and protection of fundamental human rights is essential for the development of the human personality; and that the purpose of recognizing and protecting fundamental human rights should always be to enrich lives, with the human person being always considered central to the rule of law.

6. Protecting the privacy and personal data of individuals is also about protecting their dignity, equality and freedom and working towards a more egalitarian society in which privacy is not the privilege of a few.

7. The right to privacy and, in particular, the right to personal data protection, are a form of safeguard that gives individuals the means to assert their autonomy and dignity on an equal footing. These rights, like all rights, require effective judicial guarantees. Moreover, insofar as they ensure that people are able to communicate and share with others, they are key factors in the construction and effective functioning of any democratic society.

8. Regulation in this area entails establishing safeguards that guarantee for all persons the exercise of fundamental rights and the means to ensure that their privacy, dignity, equality and freedom are protected. The right to personal data protection, in particular, is essential for the development of personality in democratic societies and for the construction and functioning of these societies. The purpose of personal data protection is to allow for a controlled flow of personal data while also fostering trade.

II. The Ibero-American system: historical background

9. Most Ibero-American countries already had data protection systems in place at the start of the twenty-first century. However, these systems were generally very different from those in place today insofar as they did not expressly recognize the right to personal data protection – although some constitutions, including the Colombian Constitution of 1991, as amended in 2003, did already contain privacy-related provisions.

10. In Uruguay, which has followed the general trend apparent throughout Ibero-America, the fundamental human right to personal data protection has always been a legally prescribed right, but there have been some substantive changes, which will be described in the following sections.

11. In line with a tendency replicated across Ibero-America, the Constitution of Uruguay establishes a system of privacy and personal data protection insofar as it recognizes the non-exhaustive nature of constitutional rights and thus admits that the enumeration of rights,

duties and guarantees contained therein does not exclude others that are either inherent in the human person or derive from the republican form of government.

12. Although the right to privacy is not expressly enshrined in the Constitution of Uruguay, article 7 establishes the right of the country's inhabitants to be protected in their enjoyment of life, honour, freedom, security, labour and property and provides that no one may be deprived of any of these rights except in accordance with laws that may be enacted in the general interest.

13. On the basis of article 7 of the Constitution, Uruguayan legal doctrine distinguishes between a first class of constitutionally recognized fundamental rights that predate legislation and are inherent in all the inhabitants of the country as human beings (freedom, life, honour, security, labour and property) and a second class of constitutionally protected individual rights, which essentially constitute the right to be protected in the enjoyment of pre-existing rights and are established by the legal regulation of those rights.

14. This distinction is grounded in three articles of the Constitution of Uruguay, namely, article 7, mentioned above, and articles 72 and 332. These articles reflect the natural law philosophy that underpins the Constitution in that they recognize the existence of rights that predate legislation, do not need to be established in enacted law and would not cease to exist if there were no legislation explicitly regulating them – although this lack of specific regulation might be offset through recourse to similar laws, general principles of law and generally accepted legal theories.

15. It is worth mentioning in this connection that the rights of access, privacy and personal data protection were not expressly recognized in legislation at the time.

16. However, individual rights require effective guarantees, and these are not automatically established simply by enshrining the right itself within a regulatory framework.

17. Furthermore, the constitutional prerogative described is limited by the principle of legality, which stipulates that limits may be imposed by legislation enacted in the general interest.

18. While the Constitution of Uruguay enshrines fundamental human rights, this alone did not provide adequate guarantees of protection for the fundamental human rights to privacy, personal data protection and dignity insofar as these rights were not generally and expressly established in national positive law. This situation meant that there were limits on the effective exercise of these rights and the guarantees intended to render them effective.

19. In view of the need to give practical application to the core provisions of the Constitution that enshrine general principles of law, and since these provisions provide for the fundamental human rights to privacy and personal data protection, it is important to analyse the international covenants, conventions and declarations that shape the provisions in question.

20. Although this report does not attempt to provide a detailed study of the relevant international instruments, the most important texts covering this area are the International Covenant on Civil and Political Rights, adopted by the United Nations General Assembly in resolution 2200 A (XXI) of 16 December 1966;[1] the American Convention on Human Rights, also known as the Pact of San José, Costa Rica;[2] the Universal Declaration of Human Rights, adopted by the United Nations General Assembly in resolution 217 A (III) of 10 December 1948;[3] the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted by the Council of Europe in 1981 and updated in 2018; the Organisation for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted in 1980 and amended in 2013; and United Nations General Assembly resolution 45/95 of 14 December 1990, inter alia.

[1] Art. 17.
[2] Art. 11.
[3] Art. 12.

21. Relevant regional instruments in the Americas include the Standards for Personal Data Protection for Ibero-American States adopted by the Ibero-American Data Protection Network in 2017.

22. It is important to consider the hierarchy of international treaties in different legal systems.

23. In Argentina, article 75 (22) of the Constitution grants constitutional rank to international human rights treaties and paragraph 23 of the same article empowers Congress to take affirmative measures to guarantee the full enjoyment and exercise of the rights recognized in international treaties.

24. In Uruguay, instruments that ratify treaties have the rank of law and there is no specific legislation that gives hierarchy to international treaties. However, according to legal doctrine, the rights, duties and guarantees enshrined in international treaties may be incorporated into national law with constitutional rank because they are inherent in the human person or derive from the republican form of government and thus fall within the scope of article 72 of the Constitution. This is an important consideration, since it requires the harmonization of national law with international law in the area of privacy and personal data protection.

25. Many Ibero-American countries based their data protection systems on regulatory provisions complemented by case law that fills gaps and develops essential principles (e.g. Costa Rica), while others based their systems on sector-specific regulations (e.g. Chile[4] and Peru[5]) complemented by framework provisions that regulate personal data protection and the right of access to data with a greater or lesser degree of specificity, depending on the case.

26. Other countries introduced the notion of sensitive data to their regulatory frameworks, as, for example, the Paraguayan legislature did in article 4 of Act No. 1682/2001.

27. Some systems regulate the requirement for express consent. This is the case in Argentina, where the requirement is set out in article 5 of Act. No. 25.326 and article 5 of Decree No. 1558/2001, which provided the sole example of personal data regulation in Ibero-America from 2001 until 2008, when Uruguay introduced its data protection system. Both countries used the European protection system as a model.

28. The remedy of habeas data is explicitly enshrined in some Ibero-American constitutions, including those of Brazil,[6] Paraguay[7] and Ecuador,[8] while, in Portugal[9] and Colombia,[10] the availability of this remedy is tacitly recognized in other elements of the personal data protection framework. The right of access to data is recognized in Brazil[11] and Mexico.[12]

29. Although a number of more effective, up-to-date systems of guarantees came into being with the introduction of the remedy of *habeas data*, generally speaking, these have all been gradually superseded by the new Ibero-American personal data protection system that has been taking shape in recent years.

30. Generally speaking, as will be explained subsequently with reference to Uruguay, it had already been established under the regulatory systems of Ibero-American countries in place in the late twentieth century that, even in the absence of provisions expressly regulating privacy, personal data protection and *habeas data*, the fundamental human rights to privacy and personal data protection were adequately enshrined at the constitutional level owing to

[4] Organic Act establishing the Framework of the State Administration and Law-ranking Decree No. 1/19.653 of 2001 of the Office of the Minister and Secretary General of the Office of the President of Chile.

[5] Act No. 27489/2001 of June 2001 on Private Risk Information and Data Owner Protection Centres.

[6] Constitution of the Federative Republic of Brazil of 1988, art. 5 (LXXII).

[7] Constitution of the Republic of Paraguay of 1992, art. 135.

[8] Constitution of Ecuador of 2008, art. 92

[9] Constitution of Portugal of 1976, art. 35

[10] Constitution of Colombia of 1991, art. 15.

[11] Act No. 9.507 of 1997 of Brazil.

[12] Federal Act on Transparency and Access to Public Government Information of 11 June 2002 of Mexico.

the natural law approach to human rights that underpins national constitutions and the philosophy underlying the provisions analysed above.

31. However, the systems of several countries proved deficient when it came to giving effect to the core provisions of their national constitutions and attempting to apply provisions that enshrined general principles of law in a manner that took account of the human rights to dignity, personal data protection and privacy.

32. In addition, some countries adopted sector-specific regulations applicable to specific types of data, such as health-related data, statistical data, child-related data, credit records and professional secrecy, inter alia, only.

III. The Ibero-American system: milestones in the process of change

33. Three milestones marked the process of change that culminated in the development of Ibero-American legislation on personal data protection.

34. The first milestone was the declaration adopted at the thirteenth Ibero-American Summit of Heads of State and Government, held in Santa Cruz de la Sierra, Bolivia, in November 2003. In preambular paragraph 45, this declaration states: "We recognize that personal data protection is a fundamental right of individuals and stress the importance of the Ibero-American regulatory initiatives aimed at protecting the privacy of citizens contained in the Declaration of Antigua, which established the Ibero-American Data Protection Network, open to all the countries of our Community."

35. The final declaration adopted at the twenty-seventh International Conference of Data Protection and Privacy Commissioners, held in Montreux, Switzerland, in September 2005, also recognized, in similar terms, the importance of the activities of the Ibero-American Data Protection Network at the global level.

36. The second milestone was the Declaration of Antigua, Guatemala, adopted at the second Ibero-American Meeting on Personal Data Protection, held in June 2003, by the representatives of Argentina, Brazil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Spain, Guatemala, Mexico, Nicaragua, Paraguay, Peru, Portugal and Uruguay. This declaration is particularly relevant insofar as its signatories declare that they:

> "1. Welcome the growing interest, concern and commitment that has been shown in Ibero-American countries with regard to the protection of personal data.
>
> 2. Reiterate that they consider personal data protection to be an authentic fundamental right of individuals, especially with regard to respect for data privacy and the power to access and control data about them.
>
> ...
>
> 5. Note the need to foster the adoption of measures that guarantee a high level of data protection and the importance of establishing national regulatory frameworks that, inspired by common legal traditions, respect for fundamental rights and the interests of their respective countries, guarantee adequate protection in all Ibero-American countries. These regulatory frameworks should take into consideration the essential data protection principles recognized in national instruments. In this regard, the regulatory initiatives that have been implemented in various Ibero-American countries are considered a very positive development.
>
> 6. Highlight the importance of strengthening experience-sharing initiatives that facilitate exchanges between Ibero-American countries by providing permanent channels for dialogue and cooperation in the field of data protection.
>
> 7. To this end, and in order to reinforce the mutual, ongoing cooperation between them, moving forward on the basis of the Permanent Forum established on the occasion of the First Meeting, institute the Ibero-American Data Protection Network ... open to the representatives of all Ibero-American countries.

...

8. Are aware that the right to personal data protection strengthens the rule of law and serves to reinforce democracy in Ibero-American countries as well as their standing and credibility in a globalized world. To this end, within the legal and institutional framework of their respective countries and according to their respective competencies, they will make the necessary efforts to ensure that personal data protection is promoted within the Ibero-American Conference, in the knowledge that doing so will promote the dissemination and raise awareness of this important fundamental right."

37. The third milestone was the 2004 Declaration of Cartagena, Colombia, in which, recognizing the important informational function of the Ibero-American Data Protection Network and its usefulness as an aide for understanding how data protection operates in each country, the signatories decided to take a more proactive approach, in pursuit of more tangible progress in the exchange of relevant information, the establishment of a permanent committee on mutual assistance, and cooperation in the drafting of common documents and proposals. This declaration led in the following years to the publication of papers on the following topics: data protection in the financial sector (Cartagena, 2004); European and Ibero-American perspectives on international data transfers (Cartagena, 2004); the telecommunications sector, the Internet and attacks on privacy (Cartagena, 2004); the commercial sector and the use of information for marketing purposes (Cartagena, 2004); the feasibility of establishing supervisory authorities in Latin America (Mexico, 2005); e-government and telecommunications (Mexico, 2005); access to public information and data protection (Mexico, 2005); the development of regulations and harmonization (Santa Cruz de la Sierra, 2006); the online network (Santa Cruz de la Sierra, 2006); self-regulation instruments (Santa Cruz de la Sierra, 2006); health data processing in relation to medical records (Santa Cruz de la Sierra, 2006); and guidelines for the harmonization of data protection regulation in the Ibero-American community (Cartagena, 2007). The Ibero-American Network continues to publish documents of this kind. Its more recent papers, all of which can be consulted on its website, include: Recommendations of the Ibero-American Data Protection Network on the Processing of Personal Health Data during Pandemics (2021); Recommendations on the Processing of Personal Data through Cloud Computing Services (2021); Declaration of the Ibero-American Data Protection Network on Digital Violence against Women and Girls (2021); General Recommendations on Data Processing and Artificial Intelligence (2019); Specific Guidelines on Compliance with the Principles and Rights Governing the Protection of Personal Data in Artificial Intelligence Projects (2019); and Personal Data Protection Standards for the American States (2017).

IV. The Ibero-American system: evolution

38. The legal systems governing personal data protection are composed of a set of principles designed to safeguard privacy and provide adequate means of protecting personal data without neglecting the importance of fostering economic flows. They regulate the rights and conduct of data subjects, issues of consent and responsibility, differential protection, security, the data protection authorities and sanctions, inter alia.

39. The different elements are organized in different ways depending on the system. Some systems are based on self-regulation and others on sector-specific standards. Some systems are supported by protection authorities, while in other systems there is no proactive preventive authority of this kind. There are also co-regulation models where companies, industries, commerce, the State, users and supervisory agencies work together to facilitate sectoral analysis and optimal decision-making.

40. The right to privacy is enshrined as a fundamental right in the constitutions of most Ibero-American countries, as detailed in section II above.

41. As for personal data protection, which is also a fundamental human right, much progress has been made over the past two decades towards the enactment of laws based on the European data protection system.

42. The European model requires the establishment of a general law on personal data protection, a series of principles to be respected – including the principle of consent, which provides the lawful basis for data processing, and the principle of purpose, which places limits on legal consent – and a set of obligations, rights and responsibilities for the various stakeholders. It also requires the existence of a supervisory authority, which should exercise its functions independently, either ex ante, for preventive purposes, or ex post, by imposing sanctions in the event of non-compliance. It is also usual for data protection systems to include legal instruments that guarantee rights both administratively and judicially, and will normally be supplemented by information security mechanisms.

43. At the end of the previous century, few Ibero-American countries had passed general legislation on personal data protection. The exceptions were Chile (Act No. 19.628 of 1999) and Argentina (Act No. 25.326 of 2000), and Spain and Portugal, which were spearheading the process of change from within the European Union. Personal data protection in other Ibero-American countries was derived from the natural law philosophy underpinning their national constitutions, with safeguards for the right to personal data protection requiring an interpretation of these constitutions that was aligned with international treaties and the applicable provisions of national law. Various countries had also adopted sector-specific provisions that complemented their personal data protection regimes.

44. Gradually, the shift in favour of the model proposed in 2003 at the thirteenth Ibero-American Summit of Heads of State and Government in Santa Cruz de la Sierra and in the Declaration of Antigua became a focus of analysis and awareness-raising for the Ibero-American Data Protection Network, eventually coming to constitute the general trend.

45. The Ibero-American countries that thus began adopting general laws providing comprehensive protection for personal data included Uruguay, as of 2008;[13] Mexico, as of 2010;[14] Peru[15] and Costa Rica,[16] as of 2011; Nicaragua[17] and Colombia,[18] as of 2012; Panama, as of 2019;[19] Brazil,[20] as of 2018; and Ecuador,[21] as of 2021.

46. With regard to data protection authorities, the body established under Brazilian law is an agency of the autonomous federal administration grouped under the Office of the President of the Republic.[22] In Ecuador, the Personal Data Protection Authority is established under article 75 of the Organic Act on Personal Data Protection as an independent public body responsible for monitoring the application of the law. In Nicaragua, articles 28 and 29 of Act No. 787/2012 provided for the establishment of the Directorate for Personal Data Protection under the Ministry of Finance and Public Credit with a mandate to monitor, supervise and protect personal data held in public and private databases. In Paraguay, the law on the protection of personal credit data[23] grants powers in this area to two authorities, the Central Bank and the Ministry for Consumer and User Protection. In Uruguay, the corresponding authority,[24] namely, the Personal Data Regulation and Monitoring Unit, is a decentralized unit of the country's e-government agency, which is an executive unit of the Office of the President. The Panamanian data protection authority, namely, the National Authority for Transparency and Access to Information, reports to the Council for the Protection of Personal Data, which is a multisectoral body composed of nine members. In Colombia,[25] the Personal Data Protection Authority under the Office of the Superintendent of Trade and Industry is

[13] Act No. 18331 of August 2008.

[14] Federal Act on the Protection of Personal Data held by Private Parties, Federal Act on Transparency and Access to Public Information, General Act on the Protection of Personal Data held by Public Sector Bodies and General Act on Transparency and Access to Public Information.

[15] Act No. 29733/2011.

[16] Act No. 8968.

[17] Law No. 787/2012.

[18] Act No. 1266/2008 and Statutory Act 1581/2012.

[19] Act No. 81/2019 on Personal Data Protection.

[20] Act No. 13709.

[21] Organic Act on Personal Data Protection.

[22] General Act on the Protection of Personal Data, art. 55, as amended by Act No. 13.853/2019.

[23] Act No. 6534/2020.

[24] Act No. 18331 of August 2008, art. 31

[25] Statutory Act No. 1581/2011, art. 19.

the body responsible for monitoring respect for the principles, rights, guarantees and procedures established by law in the processing of personal data.

47. All these supervisory bodies enjoy functional autonomy from State structures to a greater or lesser degree, but they do not have budgetary autonomy.

48. The situation in Argentina currently differs from elsewhere in Ibero-America. A personal data protection authority attached to the Ministry of Justice was established in 2000 but, in 2017, its degree of autonomy was changed by emergency decree and the Office of Chief of the Cabinet of Ministers took over the task of guaranteeing the effective exercise of the right of access to public information and monitoring the application of the Personal Data Protection Act. In the same year, the Agency for Access to Public Information was established with a remit to oversee the comprehensive protection of personal data and thus uphold individuals' right to honour and privacy.[26] Since 2017, all data protection-related activities have thus been subsumed under the Agency for Access to Public Information.

49. In principle, international data transfers are prohibited under the European personal data protection system. However, since the European system is the strictest, "adequacy" status may be accorded to certain third countries if their regulations, and the practical application of those regulations, are in line with the European system. Countries that meet these requirements are declared adequate in accordance with article 25 (6) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Being admitted to this international system of countries recognized as providing adequate protection for personal data has important implications, since it allows for the free exchange of data between recognized countries and is consequently an important facilitator for the conduct of e-commerce in a safe and secure environment.

50. In Ibero-America, two countries have this legal status: Argentina, as of 2 July 2003, (Decision 2003/490/EC) and Uruguay, as of 12 October 2012 (Implementing Decision 2012/484/EU). In its decisions to grant adequacy status to Argentina and Uruguay, the working group established under article 29 of Directive 95/46/EC emphasized that it would be monitoring developments in data protection in the two countries and the manner in which their respective data protection authorities applied the data protection principles advocated by the European system. It is thus interesting to note that, since the level of protection ensured by third countries is subject to change and the Commission must periodically check whether its adequacy decisions are objectively and legally justified, in 2016, pursuant to Commission Implementing Decision (EU) 2016/2296 of 16 December 2016, amendments were made to both Commission Decision 2003/490/EC and Implementing Decision 2012/484/EU, among other decisions relating to the adequate protection of personal data by various countries in application of article 25 (6) of Directive 95/46/EC of the European Parliament and of the Council.

51. It is also noteworthy that, in 2000, Argentina was the first country in South America to pass a law consistent with the European personal data protection model. The law in question, Act No. 25.326, governs the protection of the personal data of natural and legal persons held in files, records, databanks and other technical means of data processing managed by public or private entities.

52. Act No. 25.326 provides for the use of the constitutional remedy of *habeas data* to ensure that data subjects have access to their personal data and can request the correction or deletion of data that either are inaccurate or are used for discriminatory purposes.

53. The general principles of data protection established in Act No. 25.326 are lawfulness, purpose, data quality, consent, proportionality, information, data categorization, sensitive data identification and data security.

54. The Argentine system also protects the rights of access to and correction or deletion of data and the right to information in respect of public databases.

[26] Decree No. 899/2017.

55. Uruguay was the next to take up the European model when, in August 2008, it passed Act No. 18331, a general law applicable to the data of natural and legal persons held on any medium, whether in the public or private domain, with some exceptions.

56. The Uruguayan data protection system is based on the principles of consent as the lawful basis for data processing, purpose limitation, legality, quality and proportionality, transparency and security. The principles of good faith, accountability and minimization are also legally recognized.

57. The Uruguayan data protection system also upholds the rights of access, correction, update, inclusion and deletion that data subjects enjoy, provided that the requirements established in the applicable regulations are met, in accordance with the European data protection system.

58. All databases must be registered under Uruguayan law, which in this respect remains in line with regulatory provisions that are starting to become obsolete as provisions providing for mandatory registration give way to systems of proactive accountability.

59. Uruguayan legislation provides for both administrative remedies and an expedited judicial remedy to be available to data subjects.

60. This approach to personal data protection has had repercussions in Ibero-America, leading to laws based on the European system being passed in other countries. This occurred in Colombia, Costa Rica, Mexico, Nicaragua and Peru between 2010 and 2013, at which point in time the establishment of an Ibero-American data protection system was already coming to be seen as the way forward.

61. Ibero-America was not only constructing its own personal data protection system; it was also developing a model that promoted harmonization and cooperation with the European Union and sought to improve economic flows while protecting the fundamental human rights to privacy and personal data protection.

V. The Ibero-American system: current situation

62. The European Union General Data Protection Regulation (GDPR) 2016/679, which was adopted in 2016 and entered into force in 2018, had a major impact worldwide, including in Ibero-America.

63. The changes necessitated by the Regulation included the establishment of a data protection system with a more proactive accountability system that does away with registration obligations, privacy-by-design and privacy-by-default procedures, regulations on impact assessments and the right to data portability, an obligation to report security system breaches, and more severe sanctions for non-compliance.

64. Although Ibero-America is gradually bringing its legislation into line with GDPR provisions, no Ibero-American country has passed legislation that fully incorporates all European standards and few Latin American countries have incorporated the innovations introduced by the Regulation into their laws.

65. Nonetheless, the data protection laws passed after the Regulation’s entry into force in 2018 follow its general outline and are gradually being brought into line with the current European Union system. This is the case in Brazil (2018), Panama (2019), Andorra (2021) and Ecuador (2021). The positive legal systems of other Ibero-American are also being gradually brought into line with GDPR provisions.

66. Thus, on 26 May, Ecuador adopted Organic Act No. 459 on Personal Data Protection, which adheres to GDPR principles, especially those that guarantee fundamental rights such as the rights of access, correction, deletion and opposition, the right to data portability and proactive accountability.

67. On 26 March 2019, Panama adopted Act No. 81, which came into force in March 2021 and was supplemented by an implementing decree in May 2021. Among other innovations, Act No. 81 enshrines the principle of data portability.

68. Other countries, including Uruguay, have harmonized their regulations with GDPR provisions, particularly those that govern the role of data protection officers, the appointment of which is mandatory in some cases. The remit of a data protection officer is to issue recommendations on the formulation of data protection measures, supervise compliance with such measures, propose new measures and liaise with the supervisory authority. Uruguayan legislation has also established an obligation to assess the impact of personal data processing when the applicable legal conditions are met. Provisions regulating the principle of security were updated by Act No. 19.670 and Decree No. 64/2020, which likewise adhere to the GDPR provisions, in this case those enshrining the principles of proactive accountability and privacy by design and by default.

69. In Costa Rica, the legislature is currently considering bill No. 22388, which would overhaul the Personal Data Protection Act (No. 8968). The bill includes provisions regulating the role of data protection officers, introduces an obligation to conduct privacy impact assessments, amends the provisions of the previous law that regulate the registration of databases, sets new rules for the consent of minors and establishes privacy-related provisions based on considerations similar to those that underpin the Regulation.

70. Some of the specific elements that make certain data protection and privacy systems, including the European system, more exacting, and the extent to which these elements have been incorporated into Ibero-American legislation, are considered below.

71. In Ecuador, article 85 of the recently adopted Organic Act on Personal Data Protection provides for the appointment of a data protection officer. In Brazil, the role of data protection officer is provided for in article 23 of the General Act on Data Protection while, in Uruguay the role is regulated in great detail in article 40 of Act No. 19.670 and Decree No. 64/2020. In Mexico, the role of personal data protection officer is governed by article 85 of the General Act on the Protection of Personal Data held by Public Sector Bodies, and, in Colombia, by article 23 of Decree No. 1377/2013.

72. In Ecuador, the issue of security breaches is addressed in article 79 of the Organic Act on Personal Data Protection. In Brazil, this same issue is addressed in article 48 of the General Act on Data Protection, in Uruguay in chapter II of Decree No. 64/2020, and in Mexico in articles 38 et seq. of the General Act on the Protection of Personal Data held by Public Sector Bodies. Argentina has no regulations covering security breaches, but has adopted a series of non-binding recommendations on information security.[27] In Costa Rica, security breaches are addressed in article 38 of the regulation on the Personal Data Protection Act. In Colombia, security breaches are addressed in article 17 of Statutory Act No. 1581/2012 and, in Panama, in article 2 (5) of Act No. 81 of March 2019. In Nicaragua, article 11 of Act No. 787/2012 establishes an obligation to report information security breaches to the army or the national police. The relevant regulations provide that the data protection authority and/or the person to whom the personal data refers must be notified that the data in question has been compromised by a security incident, in some cases by a specific deadline.

73. In Brazil, personal data protection impact assessments are regulated in the General Data Protection Act,[28] while, in Mexico, they have been mandatory since 2017,[29] in certain special circumstances. In Uruguay,[30] personal data protection impact assessments are a requirement only when the law so provides, and, in Ecuador, they are governed by the Organic Act on Personal Data Protection of 2021.[31] Impact assessments are not mandatory in Argentina, Colombia, Costa Rica and the Dominican Republic.

74. The recognition of the right to data portability is another of the changes ushered in by the European Union Regulation. In Ecuador, the right to data portability is enshrined in the recently adopted Organic Act on Personal Data Protection, which provides that: “Data subjects have the right to be provided with access to their data by the data controller in a compatible, updated, structured, common, interoperable and machine-readable format that

[27] Decision No. 47/2018.
[28] Article 10 (3).
[29] General Act on the Protection of Personal Data Held by Public Sector Bodies, art. 74.
[30] Royal Decree No. 64/2020, art. 6.
[31] Art. 42.

preserves the data's characteristics, and the right to have their data transmitted to other data controllers."[32] Panama has also enshrined the right to data portability.[33] In Brazil, the right to data portability is enshrined in the General Data Protection Act,[34] as is the case in Chile.[35] El Salvador,[36] Honduras[37] and Uruguay[38] have enacted specific regulations on data portability. In Paraguay,[39] the right to data portability is protected only in respect of credit data.

75. These changes mark a further advance for the system in that Ibero-American countries are not only following the traditional European model but are also updating their regulations in line with this model with a view to improving cooperation between Ibero-America and the European Union.

VI. Conclusions

76. **The purpose of individual rights must always be to enhance the dignity, autonomy, equality and freedom of the human person and to facilitate social and political coexistence, the individual being both the origin and the object of all legal and political organization.**

77. **Even in the absence of provisions that expressly regulate privacy, personal data protection and *habeas data*, these fundamental human rights are protected in accordance with the natural law philosophy that was imbued in the constitutions of Ibero-American countries until the end of the last century.**

78. **There were three milestones in the evolution of the Ibero-American personal data protection system. The first was the declaration adopted at the thirteenth Ibero-American Summit of Heads of State and Government held in Santa Cruz de la Sierra in November 2003. The second was the Declaration of Antigua of June 2003. The third was the Declaration of Cartagena of 2004.**

79. **The constitutions of most Ibero-American countries establish the right to privacy as a fundamental human right.**

80. **The protection of personal data is also considered to be a fundamental human right, even if not explicitly enshrined in national constitutions. In the first fifteen or so years of the twenty-first century, the tendency in Ibero-American countries was to enact laws based on the European personal data protection system to supplement the core provisions of their respective constitutions.**

81. **Personal data protection systems require the existence of a general law that comprehensively regulates all aspects of personal data processing.**

82. **These laws establish a series of principles that must be honoured and respected, specify the obligations, rights and responsibilities of the various stakeholders, and provide for the establishment of independent personal data protection supervisory authorities empowered to take preventive action and act a posteriori by imposing sanctions for non-compliance. Data protection systems should also offer legal remedies for upholding the various rights at stake, whether through administrative or judicial channels.**

83. **The above analysis of the extent of these principles' application in Ibero-American countries today reveals the existence of a personal data protection system that provides a model for harmonization and cooperation, specifically with the European Union, pursuing a healthy balance between the protection of fundamental**

[32] Art. 17.
[33] Act No. 81/2019, art.15 (5).
[34] Art. 18 (V), as amended by Act No. 13.853/2019.
[35] Act No. 19.628 of 18 August 1999, art. 9, as amended in 2018.
[36] Act No. 19889 of 9 July 2020, art. 471.
[37] Act on Data Portability of 30 April 2014.
[38] Legislative Decree No. 142 of 6 November 1997 on Telecommunications and Energy, art. 19 (e), as amended in 2008.
[39] Act No. 6534/2020 on the Protection of Personal Credit Data, art. 8.

human rights and the free circulation of goods, persons, services and capital, and thus fostering healthy economic and social integration.

84. **The adoption and entry into force of the European Union General Data Protection Regulation (GDPR) 2016/679 had significant repercussions in Ibero-America, with countries in the region adopting the various solutions proposed therein for issues including the need to appoint a data protection officer in every organization, communicating and dealing with security incidents, proactive accountability measures, the assessment of potential risks at different stages of the data life cycle and the right to data portability.**

85. **Based on the understanding that cooperation is an essential element of personal data protection, the builders of the Ibero-American data protection system have sought to harmonize their regulations with the European model and thus to achieve a higher level of integration with Europe in this area.**

86. **While the analysis presented in this report shows that not all data protection standards and institutions are incorporated in the legislation of the various countries of Ibero-America, the examples mentioned are clear evidence of an increasingly marked trend towards the comprehensive protection of privacy and personal data, with clear European influences, that has culminated in the formation of the Ibero-American personal data protection system.**

VII. Outlook

87. It is clear from the foregoing that Ibero-America is moving towards a personal data protection system based on European personal data protection principles. As a result of this trend, a very useful mechanism for cooperation between Ibero-America and Europe is taking shape that has been developing and extending over an increasingly large area of Latin America for the past two decades.

88. This way of working could serve as a model for the development of privacy and data protection principles in the global context, provided that the integration it involves is achieved harmoniously, on the basis of reciprocal respect, with less discrimination and greater justice, and in a world conducive to the economic development of peoples in which democratic principles prevail. Only with a common understanding of the principles as the point of departure can disruptive technologies such as artificial intelligence, virtual reality, biotechnology, the Internet of things and mass video surveillance be leveraged in a manner that favours privacy.

89. The objectives are attainable: integration and harmonization should be our goals, but we must also endeavour to assist the most disadvantaged groups, in accordance with ethical standards and with respect for diversity.