GW Law Faculty Publications & Other Works | Faculty Scholarship

2022

Follow the Leader? Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America

Arturo J. Carrillo
George Washington University Law School, acarrillo@law.gwu.edu

Matias Jackson
Universidad de la Republica - Law School, matiasj23@gmail.com

Follow this and additional works at: https://scholarship.law.gwu.edu/faculty_publications

 Part of the Law Commons

Recommended Citation

Arturo J. Carillo & Matías Jackson, Follow the Leader? Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America, Vienna J. Int'l Const. L. (Forthcoming 2022)

This Article is brought to you for free and open access by the Faculty Scholarship at Scholarly Commons. It has been accepted for inclusion in GW Law Faculty Publications & Other Works by an authorized administrator of Scholarly Commons. For more information, please contact spagel@law.gwu.edu.

Arturo J Carrillo* and Matías Jackson

Follow the Leader? Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America

https://doi.org/10.1515/icl-2021-0037
Published online May 26, 2022

Abstract: In May 2018, the General Data Protection Regulation (GDPR) entered into force in the European Union. As is widely recognized, its impact goes beyond the borders of the old continent, permeating through the regulatory processes of countries all over the world. Nowhere is this more evident than in Latin America, where governments have long emulated European data protection standards. Professor Anu Bradford has famously characterized this phenomenon as a prominent example of 'the Brussels Effect,' defined as Europe's unilateral power to regulate global markets. Other scholars see a more complex dynamic at play. This is especially true in the data privacy context in which the EU has benefited from a highly transplantable legal model and normative innovations that have proved successful in a global marketplace of ideas. This Article joins the debate around the EU's transnational influence on the regulation of personal data by evaluating the *de jure* impact that the GDPR has had in Latin America to date. To this end, the Article addresses three main questions. First, what is the panorama of data privacy legislation across Latin America since the 2016 adoption of the GDPR? Second, how have those countries in the region that have moved first to reform or enact data privacy legislation in light of the GDPR's key innovations done so? And finally, what lessons can be learned from the Latin American experience based on the responses to these questions? In responding, the Article looks first at which countries in the region have introduced or proposed changes to their legislation in the wake of the GDPR's enactment in 2016. It then evaluates the experience of key jurisdictions in greater detail, namely Brazil, Mexico, Chile and Uruguay, to determine what lessons can be drawn from their efforts. By pursuing these inquiries, the authors shed new light on the debate surrounding the nature of the *de jure* dimension of 'the Brussels Effect' in the region.

Keywords: GDPR, data protection, Latin America, human rights, democracy

***Corresponding author: Arturo J Carrillo**, The George Washington University Law School, Washington, DC, USA, E-mail: acarrillo@law.gwu.edu. https://orcid.org/0000-0002-7509-0077
Matías Jackson, Facultad de Derecho, Universidad de la Republica Uruguay, Montevideo, Uruguay

Open Access. © 2021 Arturo J Carrillo and Matías Jackson, published by De Gruyter. This work is licensed under the Creative Commons Attribution 4.0 International License.

1 Introduction

In May 2018, the General Data Protection Regulation (GDPR) came into force in the European Union.[1] As is widely recognized, its impact goes beyond the borders of the old continent, permeating through the regulatory processes of countries all over the world.[2] Among the most notable of its innovations is its extraterritorial reach. Gráinne de Búrca highlighted this feature of the GDPR in an online symposium of the American Journal of International Law:

> Describing itself as a measure intended to harmonize data privacy laws across Europe's single market, the GDPR (…) applies to any organization operating within the EU or offering goods or services to customers or businesses in the EU (…). The key to the way in which the GDPR goes far beyond being a domestic EU-focused legislative measure is in its application to any business or organization *anywhere in the world* that offers good or services to persons within the EU (…).[3]

But the global impact of the EU's latest installment to its data protection regime derives not merely from its extra-territorial jurisdiction. The transnational influence of the European Union's data protection norms dates back at least to the approval of *Directive 95/46/EC of 24th October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data*.[4] Prior to 2016, it was this Directive that set the data privacy standards to follow around the world.[5] Nowhere was this more evident than in Latin America, where governments have long emulated European laws in this arena.[6] Once the GDPR was enacted in April 2016 to replace the Directive, and especially since coming into

1 Paul M Schwartz, 'Global Data Privacy: The EU Way' (2019) 94 NYU L Rev 771, 772; see European Union General Data Protection Regulation 2016/679 [2016] OJ L 119, 1 [hereinafter 'Regulation' or 'GDPR'].

2 Gráinne de Búrca, 'Introduction to the Symposium on GDPR and International Law' (2020) 114 AJIL Unbound 1, 1.

3 Ibid.

4 Graham Greenleaf, *Global Data Privacy in a Networked World*, in Research Handbook on Governance of the Internet 221 (I Brown ed, 2012); Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data [1995] OJ L 281, 31.

5 Ibid.

6 Graham Greenleaf, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108' (2012) 2 Int'l Data Privacy L 68, 77; see also Lee A Bygrave, *Data Privacy Law* (2014) 102; Alberto J Cerda Silva, *Personal Data Protection and Online Services in Latin America*, The Center for Studies on Freedom of Expression and Access to Information (CELE) Of University of Palermo (2011), at 12, 3, 4, <https://www.palermo.edu/cele/pdf/english/Internet-Free-of-Censorship/03-Personal_Data_Protection_Online_Services_Latin_America%20_Alberto_Cerda.pdf> accessed 25 September 2021.

force two years later in May 2018, it has become the standard bearer of European data privacy law, *inter alia*, by imposing stricter requirements on businesses and broadening individuals' rights.[7]

While there is widespread agreement that European legislation in general, and the GDPR in particular, '[have] taken an essential role in shaping how the world thinks about data privacy,'[8] there is some disagreement about how and why that is so. As just noted, the GDPR is widely recognized as 'a significant' extension of the global process of policy convergence and the trading-up of international privacy standards.'[9] Moreover, scholars have pointed out that although '[m]any difficulties remain to be overcome, (…) the GDPR is rapidly evolving into the transnational gold standard of data protection, applicable to all domestic and cross-border transfers of personally identifiable data.'[10] Naturally, this means that the EU Regulation has garnered a fair share of attention, academic and otherwise.

Anu Bradford has famously characterized this phenomenon – the GDPR evolving into a global 'gold standard' – as a prominent example of 'the Brussels Effect,' defined as 'Europe's unilateral power to regulate global markets.'[11] Her idea is that through the use of market mechanisms primarily, Europe has been able to 'unilaterally' export its laws and regulations to other jurisdictions resulting in the '*de facto*' adoption of its regulatory standards by 'export-oriented' companies, as well as the '*de jure*' promulgation of its rules by the similarly motivated legislatures in those other jurisdictions.[12] Other scholars see a more complex dynamic at play, especially in the data privacy context. Paul Schwartz takes issue with Bradford's (and others') one-dimensional formulations of Europe's regulatory influence in this area, affirming that, in addition to market forces, '[the] EU employs a broad set of [negotiation and other] strategies that have encouraged the spread of its data protection laws. Beyond these strategies, the EU has benefited both from elaborating a highly transplantable legal model and from developing concepts that have proved successful in a global marketplace of ideas.'[13]

This Article joins the debate around the EU's transnational influence on data privacy regulation by evaluating the *de jure* impact that the GDPR has had specifically in Latin America to date. It looks at which countries in the region have

7 See (n 2) and (n 3).

8 Schwartz (n 1) 773.

9 Colin J Bennett, 'The European General Data Protection Regulation: An instrument for the globalization of privacy standards?' (2018) 23 Info Polity 239, 244.

10 Michael Rustad and Thomas Koenig, 'Towards a Global Data Privacy Standard' (2019) 71 Fla L Rev 365, 453.

11 Anu Bradford, 'The Brussels Effect' (2012) 107 Nw U L Rev 1, 3, 6.

12 Ibid at 3. See also Schwartz (n 1) 803.

13 Schwartz (n 1) 803.

introduced or proposed changes to their legislation in the wake of the Regulation's enactment in 2016. It also explores the experience of key jurisdictions in greater detail, namely Argentina, Brazil, Chile, Mexico and Uruguay, to determine what lessons can be drawn from their efforts. Although international experts recognize that Latin-American countries have taken steps to modify their data privacy law frameworks since the GDPR was enacted,[14] there has yet been no systematic or wider comparative review of said countries' legislation in this regard; the literature in the field is incomplete and, where it does exist, tends to focus on comparing the Regulation to one country at a time.[15]

In this Article, we begin to close that gap by conducting a comparative law study of the Latin American countries that have contemplated, are contemplating, or have enacted legislative changes to their national legal frameworks for data protection in light of the promulgation and provisions of the GDPR. To this end, the Article addresses three main questions. First, what is the panorama of data privacy legislation across Latin America since the 2016 adoption of the GDPR? Second, how have countries in the region that have moved first to reform or enact data privacy legislation in light of the GDPR done so? And finally, what lessons can be learned, if any, from the Latin American experience based on the initial responses to both prior questions? By addressing these questions, we intend to shed light on the debate surrounding the nature of the *de jure* dimension of 'the Brussels Effect' in the region.

Indeed, there are several virtues to evaluating the Brussels Effect *de jure* in terms of post-GDPR data protection regulation in Latin America. Keeping a more precise tab on how many countries in the region have reacted to the enactment of the Regulation is one. Another is to better understand the extent to which the GDPR is the model that Latin American countries are following as they promulgate new data protection rules. What aspects of the EU Regulation are most commonly reproduced? Which are not? A third virtue is to learn more about how and why the countries most engaged in revamping their legal regimes have made, or are making, such GDPR-inspired changes. Are they following the European model of enacting comprehensive legislation, known as 'omnibus' laws, to promulgate new rules or some other approach? How faithful to the GDPR's letter and spirit are the changes?

It is our hope to begin to identify best practices, pitfalls, and challenges that can inform, and perhaps even guide, other initiatives in countries undergoing

14 Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (2020) 235–264.

15 See, eg, Abigayle Erickson, 'Comparative Analysis of the EU's GDPR and Brazil's LGPD: Enforcement Challenges with the LGPD' (2019) 44 Brook J Int'l L 859; Christian Perrone and Sabrina Strassburger, 'Privacy and Data Protection – From Europe to Brazil' (2018) 6 Panor Braz L 82; Asociación por los Derechos Civiles, *Data Protection in Latin America. Opportunities and Challenges for Human Rights, Volume I* (2017), <https://adc.org.ar/wp-content/uploads/2019/08/Data-Protection-in-Latin-America.pdf> accessed 25 September 2021.

similar reform. All of which contributes to the final insight: elucidating the real-world manifestations in law of the Brussels Effect with respect to data privacy regulation, for one important region of the world.

This Article has four Parts aside from this Introduction. The first provides an overview of the GDPR's newest and most relevant provisions from a Latin American perspective. The second Part surveys the region to determine which national legislations in Latin America have since 2016 adopted modifications or drafted bills to incorporate GDPR provisions into domestic law. Part III features case studies of four strategic jurisdictions in Latin America identified as 'first movers' in terms of GDPR adoption. The four countries are Brazil, Chile, México, and Uruguay. They were chosen, *inter alia*, because of their governments' concerted efforts to modify the respective data privacy law regimes to adapt to the GDPR. While some of them have gone as far as to approve new legislation in this regard (Brazil, Mexico and Uruguay), Chile is still debating a bill that would introduce substantive changes in line with the EU Regulation. The same is true for Argentina, also discussed in 4. Finally, Part IV summarizes our preliminary findings and conclusions with respect to the regional comparative analysis of data privacy regimes post-GDPR with an emphasis on the lessons learned from the four case-studies.

A final caveat is in order. Due to the nature of our touchstone inquiries, any responses we provide will necessarily be preliminary: tracking legal reform is by definition a moving target, as countries continue to debate, legislate and promulgate new laws, rules and regulations governing data protection in their domestic spheres.[16] That said, at first blush, it seems that a significant number of countries in Latin America have considered or enacted changes to their legislations since the approval of the GDPR in 2016. In the ensuing five-year period, 12 countries in the region (of the 20 we studied) have at least debated legislative initiatives related to data protection, if not actually reformed their legal regimes in this respect.[17] At the same time, the approaches taken by these legislative changes vary in certain substantive aspects. For instance, as a rule, not all the key new elements of the Regulation are taken on board by the Latin American legislatures enacting reform, and when GDPR-style provisions are introduced, it is often with key omissions, variations or nuances.[18] Across the board, countries in the region have tended to adopt the elements of the GDPR in a more general way, meaning they prefer higher-level norms with fewer details, which they tend to leave to the regulatory process.[19]

16 See (n 3).
17 See (n 3).
18 See (n 4) and (n 5).
19 See (n 5).

2 Overview of GDPR and Key Elements

In this Part, we provide an overview of the EU's General Data Protection Regulation (GDPR) that focuses on its novel characteristics as well as several of the new provisions it brings to European data privacy law. Doing so allows us to fashion a framework of 'key elements' to use in subsequent Parts to analyze in a more nuanced fashion the extent to which Latin American countries implementing GDPR-style legal reforms have 'followed the leader,' that is, adhered to the Regulation's parameters in carrying out those reforms.

Building as it does on Data Protection Directive 95/46/EC, the GDPR retains much of the basic configuration and content of its predecessor.[20] At the same time, however, the Regulation was enacted because '[p]rivacy issues arising from an exponential growth in consumer and mobile technologies, an increasingly connected planet[,] and mass cross-border data flows (…) pushed the EU to entirely rethink its data protection legislation to ensure that (…) fundamental rights are fully protected in today's digital economy.'[21] It thus expands, deepens, and strengthens numerous aspects of the legal regime created by the Data Protection Directive.[22] This was necessary because, while influential globally, the Directive generated conflicting domestic legal interpretations within the EU, leading to the 'fragmentation' of national data privacy laws.[23]

The GDPR was enacted to harmonize EU law on data privacy and transfers while reinforcing protections for the fundamental rights enshrined in Articles 7 and

20 Kimberly Houser and Gregory Voss, 'GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?' (2018) 25 Rich J L & Tech 1, 26; Mira Burri & Rahel Schär, *The Reform of the EU Data Protection Framework*, 6 J Info Pol'y 479, 489 (2016). See also DLA Piper, *Data Protection Laws of the World* (Full Handbook) 6–21, <https://www.dlapiperdataprotection.com/> downloaded 15 June 2020 (highlighting 'key' differences between the Directive and the GDPR, but noting areas of substantial overlap as well).

21 DLA Piper, supra (n 20), 6–21.

22 Ibid, 6.

23 Ibid; see also GDPR (n 1), recital 9 (stating that '[t]he objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.')

8 of the Charter of Fundamental Rights.[24] As such, it introduces a host of new elements that have transformed it into the most powerful data protection framework in the world.[25] This Part homes in on several of the most innovative aspects of the GDPR, identifying them in the sections below and accompanying Table A as 'key elements.' By compiling a roster of new elements from the GDPR deemed 'key' in this way, we can in the remaining Parts proceed to canvass and compare the data privacy regimes in Latin America with reference to a specialized framework of European legal norms as indicators.

2.1 Key Elements of the GDPR

The GDPR is a piece of legislation that has received a great deal of attention in recent years, especially among those who work on data privacy issues in most any context. Much of the commentary has been centered on the Regulation's two-year anniversary, and the widely held view that it has – and is – transforming data privacy regulation worldwide, mostly for the better.[26] For example, the consensus view of a panel of privacy and international law experts at the American Society of International Law's Annual Meeting, held virtually in June of 2020, was that 'the rising tide' of the GDPR's broad impact on countries outside the EU was 'lifting all boats,' in the sense that it was influencing a trend worldwide towards not just more, but also better, data privacy laws.[27] This is apparently the case to an even greater degree than was true for the Directive, which did not possess the same degree of legal weight, far-reaching data privacy safeguards, or enforceability.[28]

24 DLA Piper (n 20), 6; Charter of Fundamental Rights of the European Union, arts 7, 8 [2012] OJ C 326, 391, 397, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT> accessed 24 September 2021.

25 *GDPR and European Privacy Law Part I: The European System and the Structure of GDPR* (Online course), Privacy + Security Academy, <https://www.privacysecurityacademy.com/online-course-gdpr-1/> downloaded 22 June 2020.

26 See, eg Joe Duball, 'EC Calls for Harmonization, Addresses Data Transfers in GDPR Review' (*IAPP*, June 24, 2020) <https://iapp.org/news/a/ec-calls-for-harmonization-increased-resources-in-gdpr-review/> accessed 24 September 2021.

27 Video: American Society of International Law 2020 Annual Meeting (Virtual), *Promise or Peril: Towards an International Data Protection Regime?* (June 25, 2020) (Arturo J Carrillo, moderator) <https://asil.virtualeventsolutions.com/session/promise-or-peril-towards-an-international-data-protection-regime/> accessed 24 September 2021.

28 See DLA Piper (n 20), 6–21.

In this section, we compile a roster of several of the GDPR's innovative provisions: select features that the Regulation introduces to European data privacy law (and the world). These 'key elements,' as we will call them, are listed below and presented in Table A. Though not an exhaustive list of all the innovations enacted by the Regulation, our roster of key elements includes several that we believe characterize the strengthened European approach to protecting data privacy. In addition to being novel and representative of the GDPR, these elements also tend to be easily verifiable; generally speaking, their implementation can be readily ascertained by establishing whether a specific obligation to do 'X' is reproduced or not in the Latin American domestic legal norms surveyed. It is for these reasons that they were chosen.[29] Moving forward, this list of select elements will serve as the normative framework of benchmarks we will use in subsequent Parts to determine the extent to which the GDPR has been internalized (or not) by Latin American legal systems.

By tracking whether and how the selected key elements from the GDPR are incorporated into Latin American data privacy regimes, we will be able to establish a correlation between the two. Whether or not that correlation also reflects elements of causation is a question to be addressed in 4 and 5. Accordingly, our key elements moving forward, organized under the general headings of the GDPR, are these:

- General Provisions
    - Expanded Scope of Territorial Application
- Rights of the Data Subject
    - Right to be forgotten
    - Right to data portability
- Controller and Processor
    - Heightened standard for processing consent: the ease of withdrawal must match that for giving consent
    - Notification of data breaches
    - Data protection impact assessments (DPIAs)
    - Designation of the Data Protection Officer (DPO)
- Governance and Accountability
    - Remedies and Liability
    - Penalties

Table A graphically organizes this outline structure across the horizontal axis. The vertical axis is comprised of three rows. Row 1 indicates the source articles from the

29 Other new elements of the GDPR that did not make our list include revised definitions of personal data (art 4) and sensitive data (art 9); the concept of pseudonymization (art 4); data protection by design and by default (art 25); and enhanced transparency principles (passim).

GDPR for each element, while Row 2 summarizes the highlighted effects of the cited norms. A more detailed introduction to each key element is outlined below. In addition, Table A includes a third row that presents the corresponding questions to pose in relation to each key element when conducting the survey and case studies to follow in Parts II and III, respectively. Once the operational mapping of these normative benchmarks is completed, we can in the next Part move on to the initial survey of data privacy law reform in the Latin American region since the GDPR burst onto the global scene in 2016.

2.1.1 General Provisions

2.1.1.1 Expanded Territorial Scope

GDPR Article 3 defines the territorial scope of the Regulation, introducing not one but two hugely significant changes *vis à vis* the Directive that we wish to highlight. The first, noted already, is that it applies 'to any business or organization anywhere in the world that offers good or services to persons within the EU (…),'[30] or monitors their behavior.[31] Not surprisingly, the GDPR's new extraterritorial ambit has been a crucial factor in extending the Regulation's influence beyond the borders of the EU.[32] The other innovation to highlight is that, for the first time, European data privacy law expressly covers data processors – suppliers or agents who may be hired by a controller to process personal data on the latter's behalf – and imposes a series of specific obligations on them.[33]

2.1.2 Rights of the Data Subject

The GDPR recognizes two new data subject rights not expressly covered by the Directive: the right to erasure, and to data portability.

2.1.2.1 Right to Erasure (Right to be Forgotten) (Articles 5 & 17)

GDPR Article 17(1) grants a 'right to erasure' to data subjects when their personal data 'are no longer necessary in relation to the original purposes for which they were collected or otherwise processed,' or where 'the data subject withdraws consent on which the processing is based.'[34] In so doing, it gives effect to the

30 Búrca (n 2), 1.
31 GDPR (n 1), art 3(2).
32 Bradford (n 11), 24.
33 GDPR (n 1), art 3, 28; see also DLA Piper (n 20), 7, 9. Some processor specific duties include those to maintain adequate documentation (Article 30), ensure security of personal data (Article 32), and notify of data breaches promptly (Article 33(2)).
34 GDPR (n 1), art 17(1).

principle in Article 5(d) affirming that 'every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.'[35]

The Right to be Forgotten (RTBF) derives from the 2014 judgment of the Court of Justice of the European Union (CJEU) in *Google Spain SL v Costeja*, Case C-131/12 (2014).[36] The CJEU found a 'right to be forgotten' to be implied by the rights to erasure and blocking of data, provided for in Directive 95/46 Article 12(b), and the right to object, provided for by subparagraph (a) of the first paragraph of Article 14.[37] The European Court of Justice determined that if the information at issue is found 'to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine, the information and links concerned in the list of results must be erased.'[38] This interpretation has been expressly imported into the GDPR through Article 17.

Article 17(2) adds a robust notification requirement with respect to the erasure of personal data or similar restriction of the processing. It establishes that '[t]o strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data.'[39]

2.1.2.2 Right to Data Portability (Article 20)

A wholly new right created by the GDPR for data subjects relates to data portability.[40] Article 20 authorizes data subjects to request and receive their personal data from a data controller in a structured, commonly used and machine-readable format, and to transmit it to another data controller without hindrance.[41] Article 20 has two main purposes. From the human rights perspective, it aims to empower data subjects in their relationship with controllers by 'strengthen[ing] the [subject's] control over his or her own data.'[42] From a more economic approach, it can

35 GDPR (n 1), art 5((1)d).
36 See Case C-131/12, *Google Spain SL v Costeja* [2014] ECR 317.
37 Ibid, para 88, 100(3).
38 Ibid, para 94.
39 GDPR (n 1), recital 66 (referring to art 17(2)); see also Voss and Castets-Renard (n 94), 326.
40 DLA Piper (n 20), 16.
41 GDPR (n 1), art 20.
42 See GDPR (n 1), recital 68.

work as a tool to support free flow of personal data and foster competition between controllers by lowering switching costs.[43] Finally, it is important to note that the right to data portability only applies to information which was obtained on the basis of consent or as necessary for the performance of a contract, but not for information obtained on other grounds.[44]

2.1.3 Controller and Processor

2.1.3.1 Heightened Standard for Consent (Withdrawal)

Although the basic normative structure for determining the lawfulness of processing remains largely the same from the Directive to the GDPR, the latter has raised the bar with respect to what constitutes valid consent to the collection and processing of personal data.[45] For example, '[c]onsent must [now] be fully unbundled from other terms and conditions and will not be valid unless freely given, specific, informed and unambiguous (Articles 4(11) and 6(1)(a)).'[46] Moreover, the effects of valid consent under the Regulation have been further limited through the operation of the new data subjects' rights just examined, namely, the right to erasure and to data portability.[47] But, for our purposes in this section, the precise element of the GDPR's reinforced provisions regarding consent to highlight is that relating to its withdrawal.

Under the Regulation's revised regime, '[i]t shall be as easy to withdraw as to give consent.'[48] Article 7 makes clear that the data subject may withdraw his or her consent at any time.[49] Recital 42 clarifies further that '[c]onsent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse *or* withdraw consent without detriment.'[50] For purposes of the operating methodology as reflected in Table A, then, it is this particular principle – that data subjects must be able to withdraw their consent as easily as they provided

43 See Article 29 Data Protection Working Party, Guidelines on the Right to Data Portability 4 (2016), <https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf> accessed 24 September 2021.
44 See Alex van der Wolk, *The EU General Data Protection Regulation: A Primer for International Business* (2016) 3.
45 DLA Piper (n 20), 10–11.
46 Ibid 11.
47 Ibid.
48 GDPR (n 1), art 7(3).
49 Ibid.
50 Ibid, recital 42.

it – which will serve as the touchstone for purposes of identifying efforts to implement the GDPR's heightened consent requirements. As a practical matter, this element will function as a representative indicator of whether the jurisdiction under study has considered the importance of protecting consent in line with the GDPR's new strictures.[51]

2.1.3.2 Notification of Personal Data Breaches

The establishment of duties to notify data breaches to supervisory authorities and affected persons is one 'of the most profound changes to be introduced by the GDPR.'[52] Articles 33 and 34 refer to the obligations that data controllers have to notify data breaches to supervisory authorities and affected individuals, respectively. The object of these critical new provisions is to mitigate or avoid the 'physical, material or non-material damage to natural persons' that can result from data breaches and/or a failure to report them.[53] Said damage can include loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymization, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.[54]

With respect to the duties under Article 33, controllers must as a general rule notify the supervising authority promptly of any personal data breach; where feasible, they must do so within 72 of becoming aware of it.[55] The controller's notification must provide information on the nature of the breach, the number of subjects affected, the type of data compromised, the likely consequences of the breach, and the measures taken or proposed to be taken, among other things.[56] When the breach compromises information that may result in high risks to the rights and freedoms of individuals, Article 34 stipulates that the controller must also notify the data subjects affected by the breach 'without undue delay.'[57] This is 'in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects.'[58]

---

51 See (n 4) and Table C (Annex).
52 DLA Piper (n 20), 14.
53 GDPR (n 1), recital 85.
54 Ibid.
55 GDPR (n 1), art 33(1).
56 Ibid art 33(3).
57 Ibid art 34.
58 GDPR (n 1), recital 86(2).

2.1.3.3 Data Protection Impact Assessment

Much of the GDPR's import flows from the emphasis on demonstrating compliance with its enhanced data protection principles and promoting greater accountability for the failure to do so.[59] A novel mechanism established to this end is the Data Protection Impact Assessment, or DPIA, which applies to 'new technologies' and any other type of processing 'likely to result in a high risk to the rights and freedoms of natural persons.'[60] The DPIA is 'an assessment of the impact of the envisaged processing operations on the protection of personal data.'[61] It is used 'to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them.'[62] Examples of the types of processing covered are those that involve sensitive personal data or automated 'profiling' of persons; or are carried out *en masse*.[63]

DPIAs are thus an important tool for increasing the compliance of data processors and their accountability with respect to the obligations set out in the Regulation. Among other things, overseeing these impact assessments is one of the primary functions of the newly created Data Protection Officers described in the next sub-section.[64] In this way, the information resulting from the DPIAs can lead to better understandings, and more uniform evaluations, between controllers, processors and the corresponding Data Protection Authorities.[65]

2.1.3.4 Designation of the Data Protection Officer

Still another 'significant new governance' requirement for organizations covered by the GDPR is to appoint a data protection officer, or DPO.[66] Article 37 establishes the obligation for data controllers and processors to designate a DPO inside their organizations when:

- the data processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

---

59 See DLA Piper (n 20), 18.
60 GDPR (n 1), art. 35(1).
61 Ibid.
62 Article 29 Data Prot Working Party (n 43), 4.
63 GDPR (n 1), art 35(3). See also GDPR art 9 for definitions of special categories of data including sensitive personal data.
64 GDPR (n 1), art 39(1)(c).
65 Joshua Blume, 'A Contextual Extraterritoriality Analysis of The DPIA and DPO Provisions In the GDPR' (2019) 49 Geo J Int'l L 1425, 1434.
66 DLA Piper (n 20), 17.

- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale;[67] or
- the core activities of the controller or the processor consist of processing on a large scale sensitive personal data pursuant to Article 9 (special categories of personal data) or personal data relating to criminal convictions and offences referred to in Article 10.[68]

The DPO must possess an expert level of relevant expertise and be designated on the basis of his or her professional qualities.[69] Recital 97 stipulates that said expertise must be related 'to the data processing operations carried out and the protection required for the personal data being processed.'[70] Among the key duties of the DPO are monitoring and providing guidance on Data Protection Impact Assessments.[71] The DPO should also be able to carry out his or her duties 'in an independent manner.'[72] GDPR Articles 38 and 39 expand further on the position and responsibilities of the officer inside the organizations covered. As is the case with the DPIAs, the purpose of this obligation is to promote greater compliance with the provisions of the GDPR and ensure accountability when necessary.[73]

2.1.4 Governance and Accountability

The GDPR's ratcheting up of governance requirements, several of which have been highlighted in the prior paragraphs, have been accompanied by stricter accountability mechanisms, especially the creation of enhanced remedies for individuals to bring private claims and stiffer penalties for non-compliance.[74] Furthermore, the GDPR heightens the responsibility for data controllers and processors by

67 Although the GDPR does not contain a definition of what constitutes 'large-scale,' Recital 91 provides a guidance: 'large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk.' See Article 29 Data Prot Working Party, Guidelines on Data Protection Officers ('DPOs') 7 (2016), <https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf> accessed 24 September 2021.
68 GDPR (n 1), art 37.
69 Article 29 Data Prot Working Party (n 43) 11.
70 GDPR (n 1), recital 97.
71 Article 29 Data Prot Working Party (n 43) 16.
72 Ibid, 14.
73 Ibid, 4.
74 DLA Piper (n 20) 7–8.

requiring them to demonstrate their compliance with all the prescribed principles and norms of data processing.[75]

2.1.4.1 Remedies and Liability

Individuals seeking redress from a controller or processor under the GDPR are guaranteed a range of remedial avenues. They can lodge a complaint with the supervisory authority set up under GDPR Article 51 'if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.'[76] They are similarly entitled to pursue legal action 'before the courts of the Member State' against an offending controller or processor, without prejudice to any other remedies that might be available.[77] Perhaps most significantly, any person who has suffered 'material or non-material damage' as a result of a breach of the Regulation is guaranteed the right to compensation for the harm suffered from the controller or processor.[78] 'The inclusion of 'non-material' damage means that individuals will be able to claim compensation for distress and hurt feelings even where they are not able to prove financial loss.'[79]

2.1.4.2 Penalties

The penalties contemplated by the GDPR are of a magnitude not previously seen in European data privacy law. Fines are divided into two categories depending on the characteristics of the breach. The first corresponds to more severe breaches, which include the non-compliance with data subjects' rights or international transfer restrictions, among others. In these cases, applicable fines rise to 20,000,000 Euros or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher.[80] The second category applies to breaches of obligations set for data controllers and processors, such as those related to security, data breach notifications, certification and monitoring. In these cases, fines go

75 GDPR (n 1), art 5.2.
76 Ibid, art 77.
77 Ibid, art 79.
78 Ibid, art 82(1).
79 DLA Piper (n 20), 8.
80 GDPR (n 1), art 83(5); see also 'Understanding the Scope of Your GDPR Undertaking' (*Ashurst*, July 3, 2018), <https://www.ashurst.com/en/news-and-insights/legal-updates/understanding-the-scope-of-your-gdpr-undertaking/> accessed 24 September 2021 ('[u]ndertaking has the meaning given in Articles 101 and 102 of Treaty on the Functioning of the European Union. In other words, the worldwide annual turnover test is to be applied in a similar way to how fines under European Competition [anti-trust] law are currently assessed. For those unfamiliar with European Competition law principles, the meaning of undertaking has been scrutinised frequently by the courts. The central element is that, if one entity exercises control over another, they both form a single economic entity and are therefore assessed as part of the same undertaking.').

up to 10,000,000 Euros or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher.[81] With these provisions, the GDPR follows the example of anti-bribery and anti-trust laws that tend to set high fines tied to companies' global revenues.[82]

3 Panorama of Data Protection Legislation in Latin America

The objective of this second Part is to review the context and status of legislative initiatives on data protection in Latin America through 2021. To do this, we focused our research on relevant legislation across the region that was introduced or enacted since April 2016, the date the GDPR was approved by the European Parliament and the Council of the European Union. This legal framework entered into force in May 2018, of course; however, governments in Europe and abroad took advantage of the two-year window between the Regulation's adoption and its activation to adapt their domestic regimes and practices to the new rules.[83] For this reason, we will highlight those pertinent legal initiatives starting from the time of the GDPR's approval in 2016.

But first we must set the stage. In Latin America, data protection is uniquely built upon the concept and tradition of *habeas data* as a constitutional right.[84] Since the 1980s, countries in the region have protected privacy and personal data *vis à vis* their governments through a right to *habeas data*, which mirrors the writ of *habeas corpus* but for information.[85] *Habeas data* translates from Latin as 'bring me the data' and implies the right of the data subject to access the information that the State possesses about him or herself.[86] As a constitutional right, it applies to government authorities first and foremost, but has been extended to cover non-state actors as well.[87] A writ of *habeas data* applies to any type of personal data, which the subject is entitled to request and access on demand.[88] It can also include

81 GDPR (n 1), art 83(4).

82 DLA Piper (n 20) 7–8.

83 Mark Foulsham, 'Living with the New General Data Protection Regulation (GDPR)' in Maria Krambia-Kapardis (ed), *Financial Compliance: Issues, Concerns and Future Directions* (2019) 113, 117.

84 Ibid.

85 Ibid.

86 Ibid.

87 Cerda (n 6) 2–4.

88 Sarah L Lode, Note, '"You Have the Data"…The Writ of Habeas Data and Other Data Protection Rights: Is the United States Falling Behind?' (2019) 94 Ind LJ 41, 43.

the rights to rectify as well as sometimes erase personal data held by any public or private third party. [89]

Habeas data was first introduced in the region as a constitutional right enshrined by a number of Latin American countries during the eighties and nineties.[90] It was most recently enacted through a constitutional amendment in Chile in 2018.[91] In this way, Latin American constitutional law became the primary means of protecting personal data through the operation of three key mechanisms: the recognition of *habeas data* as an autonomous fundamental right; the concomitant creation of a specialized constitutional remedy – the writ or action of *habeas data*; and growing recognition of the broad scope of the right and its enforcement with respect to both public and private actors.[92]

After the approval of the EU's Personal Data Directive in 1995, Latin American countries moved towards the enactment of specific data protection laws that complemented the aforementioned constitutional protections. Those new laws tended to follow the European approach of enacting comprehensive 'omnibus' legislation, thus providing more detailed rights and procedures to increase both legal certainty within domestic jurisdictions and harmonization across countries in the region.[93] Commentators have previously divided those legislative initiatives into 'two waves.'[94] The first wave of legislation came immediately after the adoption of the Data Protection Directive in 1995 with the enactment of data protection laws in Chile (1999), Argentina (2000), and Paraguay (2000).[95] It is worth noting here that as part of this first wave, the Ibero-American Data Protection Network was founded in 2003; we discuss this influential organization in more detail below.[96] A second wave of reform came in the following years, with the enactment of new laws in Uruguay (2008), México (2010), Costa Rica (2011), Peru (2011), Nicaragua (2012), and Colombia (2012).[97] To these two we can now add a third wave of ongoing data privacy initiatives, with new or additional laws

89 Ibid, 45.

90 For example, Brazil (1988), Colombia (1991), Paraguay (1992), Peru (1994), Bolivia (1995), Ecuador (1996), and Venezuela (1999); Lode (n 88) 44.

91 See infra (n 271) and accompanying text.

92 Cerda (n 6) 3–4, 12.

93 Ibid 11.

94 W Gregory Voss and Céline Castets-Renard, 'Proposal for an International Taxonomy on the Various Forms of the "Right to be Forgotten": A Study on the Convergence of Norms' (2016) 14 Colo Tech LJ 281, 314.

95 Ibid.

96 See (n 105–108).

97 Voss and Castes-Renard (n 94) 314.

promulgated in Mexico (2017), Uruguay (2018), Brazil (2018), Panama (2019) and Ecuador (2021).[98]

The respective national laws adopted during each of the three historical waves identified share some common characteristics. Latin American countries tend to protect data privacy in comprehensive legislation that expands upon the core right of *habeas data* in their constitutions.[99] Inspired in turn by EU initiatives like the Directive, and now the GDPR, these evolving legal frameworks govern the collection, use and dissemination of personal data by private as well as public parties.[100] In addition, they generally grant at least some if not all of the individual rights known as 'ARCO' rights, for their acronym in Spanish. The ARCO rights of data subjects entitle them to Access, Rectify (correct), Cancel (erase) or Oppose processing personal information that has been collected by government authorities or, more recently, by private companies.[101] If the data is inaccurate, incomplete or outdated, the subject can ask for its rectification; if the data is being processed, he or she can request that it not be.[102] These are all key characteristics of the Latin American approach to protecting personal data.

The comparative study we develop in this Part is primarily descriptive of domestic legislative activity related to data protection. Our intention is to provide a panoramic 'snapshot' of the landscape with respect to data privacy legal reform in Latin America as it stands in 2021, as well as how it is developing at a regional level. Our goal is to gain a comprehensive view of the way Latin American countries have responded to the adoption of the GDPR in 2016. It is worth noting, first, that this research draws heavily from States' official government websites to provide greater certainty about the status of the laws and bills reviewed; and second, that it focuses on the 20 sovereign States geographically located in Central and South America. Thus, territories and dependencies like French Guyana in South America are excluded from our purview, as are all the Caribbean nations, for the most part.[103]

98 See infra (n 155, 177, 122, 164 and 135) and accompanying text.

99 See supra (n 83–85) and accompanying text.

100 Voss and Castes-Renard (n 94) 314.

101 Lode (n 88) 55.

102 Ibid 45.

103 We recognize that a separate study of Caribbean country data privacy reform is warranted. A cursory examination of Caribbean practice in this area through 2021 reveals the following panorama: 15 of the 22 countries in the Caribbean, excluding European-state territories, have a personal data protection regime (Antigua & Barbuda, Aruba, Bahamas, Barbados, Bermuda, BES Islands, British Virgin Islands, Cayman Islands, Curaçao, Dominican Republic, Jamaica, St Kitts & Nevis, St Maarten, St Lucia, and Trinidad & Tobago). Nine of these 15 states possessed such laws prior to the enactment of the GDPR in 2016, while the other six enacted theirs after the GDPR was passed (Barbados, Bermuda, BVI, Cayman Islands, Jamaica, and St Kitts & Nevis). Of the nine countries

Our preliminary findings are summarized in Table B, entitled 'Review of Data Privacy Regulation in Latin America in 2021.' In the first column on the vertical axis, the Table lists all 20 independent countries in Central and South America we surveyed; it then arrays the topics reviewed for each along the top row of the horizontal axis. Those topics are as follows. The second column of Table B reflects whether the particular country studied has a comprehensive data protection law or not. If it does, the Table gives the law's reference number or code along with the date it was enacted; a link is provided to the official version of the law whenever possible. Where such a law exists, its full title translated into English is reproduced in the third column. The fourth column registers whether the country has established a national data protection authority – the 'supervisory authority' originally required by EU Directive 95/46, and subsequently reinforced by the GDPR.[104] The fifth identifies whether the countries have proposed changes to their basic data protection law or some other legislative initiative on data privacy after April 2016, while the sixth column registers whether those proposals have to date been successful or not, ie enacted into law. These 'changes' can flow from either a bill intended to modify the basic data privacy regime identified in the second and third columns, or an entirely new stand-alone law (as in the case of Brazil).

It is worth highlighting here that our set of surveyed nations covers all of the Latin American countries that are part of the Ibero-American Data Protection Network (*Red Iberoamericana de Protección de Datos Personales*),[105] as well as those that are not. As noted, this Network was created in 2003; it was established with the aim of promoting cooperation and policy development among governments with

---

that already had data protection laws in 2016, none to date have proposed new amendments to their existing regimes. Seven Caribbean nations still have not legislated data privacy protections (Cuba, Dominica, Grenada, Guyana, Haiti, St Vincent & the Grenadines, and Turks & Caicos), with only Guyana making efforts to move in that direction. See Bartlett D Morgan, 'Status of Data Privacy Laws in the Caribbean' [Feb 2021] (*bartlettmorgan*, 3 February 2021), <https://www.bartlettmorgan.com/2021/02/03/status-of-data-privacy-laws-in-the-caribbean-feb-2021/> accessed 24 September 2021; see also Cynthia J Rich, 'Assessing the Current and Future Privacy Landscape in the Americas, Morrison Foerster' (*MoFo*, 6 January 2021), <https://www.mofo.com/resources/insights/210106-future-privacy-landscape.html> accessed 24 September 2021.

104 Compare Directive 95/46/EC (n 4), art 28, with GDPR (n 1), art 51 (each mandating the creating of a 'supervisory authority' within the Member States).

105 The Network's member and observer States from Latin America are Argentina, Bolivia, Brazil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, Mexico, Nicaragua, Panama, Paraguay, Peru, Uruguay, and Venezuela. See 'Relación de Entidades Integrantes de la RIPD' (*Red Iberoamericana de Datos*) <https://www.redipd.org/es/la-red/entidades-acreditadas> accessed 1 August 2021.

respect to the regulation of data privacy.[106] Today, it counts with the participation of 10 countries in Latin America and Europe,[107] and has accredited 19 other countries or entities as observers as well, including the Council of Europe's Consultative Committee for the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Convention 108).[108]

Not surprisingly, the Ibero-American Network has actively contributed to the expansion of the European model of data privacy in Latin America, due in large part to Spain's prominent role in the organization.[109] For example, the Network's agenda for 2015–2018 expressly included the promotion of the European data privacy model in Latin American countries, among others, because 'the benefits that such adoption would bring to Spanish companies that desire to transfer an increasing volume of personal data with such countries.'[110] By joining the Ibero-American Network, countries in Latin America have shown a prior interest in, if not commitment to, the European framework and its principles.[111] Almost all of the Latin American participants in the Network, for instance, have an established Data Protection Authority (DPA), which was one of the pillars of the Directive 95/46/EC (Article 28).[112]

In short, the vertical axis of Table B is populated by the 20 Latin American countries in Central and South America, while the top row on the horizontal axis is comprised of the specific topics we reviewed for each of the states surveyed. The final column of Table B is for comments dedicated primarily to highlighting

106 'Historia de la Red Iberoamericana de Protección de Datos [History of the Ibero-American Data Protection Network]' (*Red Iberoamericana de Protección de Datos, RIPD*) <https://www.redipd.org/es/la-red/historia-de-la-red-iberoamericana-de-proteccion-de-datos-ripd> accessed 24 July 2020; see also 'Red Iberoamericana de Protección de Datos', (*Reglamento de la Red Iberoamericana de Protección de Datos [RIPD]*, 2003), <https://www.redipd.org/sites/default/files/2019-11/reglamento-ripd.pdf> accessed 24 September 2021.

107 See Graham Greenleaf, 'Independence of Data Privacy Authorities (Part I): International Standards' (2012) 28 Comput L & Sec Rev 3, 1 ('[the Network] includes in its membership all countries within its community that wishes to be a member, irrespective of whether it has yet adopted data privacy laws or has a DPAs, (Raab, 201: 297-8) so it does not have [formal] accreditation requirements equivalent to the IDPPCC or APPA.')

108 See Red Iberoamericana de Protección de Datos (RIPD) (n 105).

109 See generally Charles D Raab, 'Information Privacy: Networks of Regulation at the Subglobal Level: Information Privacy Networks' (2010) 1 Global Policy 291, 297 ('[a]lthough somewhat modestly called a "network," there is clearly a more formalised set of relationships among the Ibero-American community, with organisational structures as well as common positions and objectives, and based on ties stemming from colonial roots and the Spanish or Portuguese languages.').

110 Bradford (n 14) 153.

111 Raab (n 109) 297.

112 See Table B (Annex).

notable aspects of the selected country's data privacy regime. We note, for example, if a country has a data protection law, as well as any new legislation since 2016 that has referenced the GDPR and/or reflected any of the key elements of that Regulation in a manner attesting to a connection between the two. If no such law exists, we offer a brief commentary on the status of a country's efforts to enact data privacy regulation where pertinent. Finally, we indicate in the Table which countries have obtained an 'adequacy' determination from the European Commission, as well as those that have ratified Convention 108 and its protocols. The summaries captured in that final column read as follows:

- In 2018, **Argentina** proposed a comprehensive draft law to update the omnibus law approved in 2000, with a view to maintaining the 'adequacy' of protections recognized by the European Union. The 2018 draft bill made express reference to the GDPR as the 'international standard' to emulate, and includes almost all the key elements from Table A. Despite this bill losing parliamentary status in 2020,[113] a new proposed law was introduced in March of 2020.[114] Two additional bills were presented in November[115] and December[116] of 2020 and remain in parliamentary debate. These three pending bills have the same general purpose of maintaining the 'adequacy' with the EU and seek to follow the GDPR standards. Argentina ratified Convention 108 in 2018 and signed (but not ratified) the 2018 Protocol updating the convention to 108+.[117] For details, see the Argentina case study, *infra*, 4.1.
- **Belize** lacks a formal data privacy law. Privacy is recognized as a right in the Constitution, and some privacy protections are included in laws which regulate public and private entities that handle personal data.[118]
- **Bolivia** is among the countries that currently lacks a comprehensive data protection framework. In 2018, legislators presented a bill seeking to enact the

113 'Nuevo Proyecto de ley para Reemplazar la Actual Ley de Protección de Datos Personales' (*Marval O'Farrel Mairal*, 21 December 2020) <https://www.marval.com/publicacion/nuevo-proyecto-de-ley-para-reemplazar-la-actual-ley-de-proteccion-de-datos-personales-13873> accessed 24 September 2021.

114 Diputados Argentina, Proyecto 0070-D-2020, <https://www.hcdn.gob.ar/proyectos/textoCompleto.jsp?exp=0070-D-2020&tipo=LEY> accessed 12 May 2021.

115 Diputados Argentina, Proyecto 6234-D-2020, <https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2020/PDF2020/TP2020/6234-D-2020.pdf> accessed 12 May 2021.

116 Senado Argentina, Número de Expediente 2986/20, <https://www.senado.gob.ar/parlamentario/parlamentaria/441614/downloadPdf> accessed 24 September 2021.

117 See (n 208) and accompanying text.

118 Global Advertising Lawyers Alliance, *Privacy Law: A Global Legal Perspective on Data Protection Relating to Advertising and Marketing* (2020), 42 <https://www.bowmanslaw.com/wp-content/uploads/2020/06/Privacy-Law.pdf> accessed 24 September 2021.

'Personal Data Protection Law.'[119] It included some GDPR key elements, such as the right to data portability and data breach notification requirements. The law would have created a DPA with the power to impose sanctions. In 2019, a similar draft bill was presented by Foundation Internet Bolivia.org.[120] Neither was enacted but modified versions of the proposed laws may be considered if re-submitted and endorsed by the new legislature.[121]

- **Brazil** enacted a comprehensive data protection law in 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD), for the first time; it was amended in 2019 to establish the DPA as part of the Executive Branch.[122] The law resembles the GDPR in many important respects, *inter alia*, by having extraterritorial application, promoting stronger data subject rights, and adding a duty for notification of data breaches. However, it differs from European standards on other fronts. The LGPD went into effect in September 2020 due to the pandemic,[123] while enforcement was slated to begin in August 2021.[124] For more information, see the Brazil case study, *infra*, in 4.1.
- In 2017 **Chile's** Congress began consideration of a bill to update the 1999 personal data law and, *inter alia,* create a data protection authority. The proposed law contains some provisions that advance GDPR protections, such as the rights to erasure and data portability, as well as the duty to notify breaches. It ignores several others. The bill remains in parliamentary debate; in January 2021, President Sebastián Piñera submitted an urgent request to expedite the process.[125] Notably, in 2018 Chile adopted Act No 21.096 to amend

---

119 Diputados Bolivia, PL 405-18 Proyecto de Ley de Protección de Datos Personales (on file with author).

120 Ante-Proyecto de Ley ciudadana de privacidad y Protección de Datos Personales, Foundation Internet Bolivia (2019) <http://misdatos.internetbolivia.org/docs/anteproyecto_ley_de_proteccion_datos_personales_InternetBolivia.pdf> accessed 24 September 2021.

121 E-mail from Diandra Cespedes Sagardía, Priv & Data Prot Officer, Bolivia Internet Association, to Arturo Carrillo, Professor of L, Geo Wash Univ L Sch (June 9, 2021, 12:02 PM ET) (on file with author).

122 Mauricio Paez et al., *Companies Are Now Getting Ready for Brazil's New Data Protection Law* (*JonesDay*, September 2019) <https://www.jonesday.com/en/insights/2019/09/brazils-new-data-protection-law> accesssed 24 September 2021.

123 *Brazil*, DLA Piper, Data Protection Laws of the World, <https://www.dlapiperdataprotection.com/index.html?t=law&c=BR> last modified 28 January 2021.

124 Lei No 13.709, de 14 de Agosto de 2018, Diário Oficial da União [DOU] de 15.8.2018 (Braz) http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm#art65; See also Brazil, DataGuidance <https://www.dataguidance.com/jurisdiction/brazil> accessed 20 May 2021.

125 Jaime Urzúa, 'Gobierno Pone Suma Urgencia al Proyecto de Ley de Datos Personales' (*Alessandri*, 15 January 2021) <https://www.alessandri.legal/gobierno-pone-suma-urgencia-al-proyecto-de-ley-de-datos-personales/#:~:> accessed 24 September 2021.

the Constitution to add data protection as a fundamental right with constitutional status.[126] For more information, see the Chile case study, *infra*, in 4.2.

- Since 2016, in **Colombia**, the Congress has discussed various legislative proposals to modify the omnibus Data Protection Law of 2012, though none has yet succeeded. In their introductions, the bills referenced the GDPR as a source of guidance, which is not surprising given that Colombian data protection law is largely based on Europe's.[127] The proposed reforms would have expanded the territorial scope and increased data processors responsibility by introducing duties to realize privacy by design, to prepare impact assessments reports, and establish DPOs.[128] The Colombian DPA is actively enforcing its law against companies that do not comply, like WhatsApp.[129]
- In July 2016, the **Costa Rican** DPA promulgated Executive Decree Nº 40008 to update the country's Data Protection Law by introducing several the GDPR's key elements into the legal regime, such as the right to be forgotten and extended liability regime for both controllers and processors.

---

126 Ley N° 21.096 Consagra Constitucionalmente el Derecho a la Protección de Datos Personales (*Microjuris Inteligencia Jurídica*, 18 June 2018) <https://aldiachile.microjuris.com/2018/06/18/ley-no-21-096-consagra-el-derecho-a-la-proteccion-de-datos-personales/#:~:> accessed 24 September 2021.

127 Juan Pablo Vega B, 'Colombia Tiene un Marco Robusto en Protección de Datos' (*Asuntos Legales*, 16 April 2018) <https://www.asuntoslegales.com.co/actualidad/colombia-tiene-un-marco-robusto-en-proteccion-de-datos-2714309> accessed 24 September 2021.

128 See Proyecto de Ley por medio de la cual se modifica el ámbito de aplicación de la Ley Estatutaria 1581 de 2012 y se facilita a la Autoridad de Protecciónón de Dato para que proteja los derechos de las colombianas y colombianos frente a la recolección y el tratamiento internacional de datos personales, de 6 de agosto de 2016,

<http://leyes.senado.gov.co/proyectos/index.php/proyectos-ley/periodo-legislativo-2014-2018/2016-2017/article/91-por-medio-de-la-cual-se-modifica-el-ambito-de-aplicacion-de-la-ley-estatutaria-1581-de-2012-y-se-facilita-a-la-autoridad-de-proteccion-de-dato-para-que-proteja-los-derechos-de-las-colombianas-y-los-colombianos-frente-a-la-recoleccion-y-el-tratamiento-internacional-de-datos-personales> accessed 24 September 2021.

129 See generally Superintendencia de Industria y Comercio (SIC), 'Decisiones Administrativas' (*Sic.gov*) <https://www.sic.gov.co/tema/proteccion-de-datos-personales/decisiones-administrativas> accessed 24 September 2021; Superintendencia de Industria y Comercio (SIC), '*Superindustria ordena a WhatsApp cumplir con el estándar nacional de protección de datos de sus 39 millones de usuarios en el país*' (*Sic.gov*, 26 May 2021) <https://www.sic.gov.co/slider/superindustria-ordena-whatsapp-cumplir-con-el-est%C3%A1ndar-nacional-de-protecci%C3%B3n-de-datos-de-sus-39-millones-de-usuarios-en-el-pa%C3%ADs> accessed 24 September 2021.

In January 2021, draft law N° 22.388 was introduced to provide a complete reform of the 2011 law,[130] and is currently being debated by the Legislative Assembly.[131] The bill expressly cites the GDPR as its guide to filling the gaps left by the 2011 Law.[132] Among other things, the proposed law would modernize the country's regime of data subject rights and establish the Costa Rican DPA as an independent institution.[133]

- In **Ecuador**, data protection is a fundamental constitutional right.[134] In May 2021 Ecuador's National Assembly enacted its first DP law which specifically recognizes the GDPR's impact.[135] It contains several of the Regulation's key elements. For example, it enshrines the rights to data portability[136], mandates DPIAs[137] and the designation of DPOs,[138] as well as the duty to report data breaches.[139] It also regulates processors' liability for data breaches with enhanced penalties for serious offenses.[140] The original draft included the right to be forgotten but it was eliminated in the approved bill.
- Although **El Salvador's** Legislative Assembly approved a Data Protection Law in April of 2021,[141] it was immediately vetoed by President Nayib

130 AccessNow, *Legislando por la protección de datos personales: Conversatorio entre Europa y América*, YOUTUBE (11 May 2021), 19:58-22:21 <https://www.youtube.com/watch?v=fJyJkw07PlQ&ab_channel=AccessNow> accessed 24 September 2021.

131 Marion Briancesco, 'Costa Rica: Reforma Para Protección de Datos Personales' (*ipandetec.org*, 9 February 2021) <https://www.ipandetec.org/2021/02/09/reforma-datos-personales/> accessed 24 September 2021.

132 Asamblea Legislativa, Proyecto de Ley N° 22.388, 4, 9 <http://www.asamblea.go.cr/Centro_de_informacion/Consultas_SIL/SitePages/ConsultaProyectos.aspx> accessed 2 August 2021; AccessNow (n 130), 22:42-23:00.

133 Asamblea Legislativa (n 132), 9; AccessNow (n 130), 23:10–26:00. A new article on transborder data transfers not in the previous legislation was added.

134 Por una Ley Protección de Datos Centrada en los Derechos del Ciudadano, Notas para la discusión del Anteproyecto de Datos Personales de Ecuador (*Asociación para el Progreso de las Comunicaciones*) <https://www.apc.org/sites/default/files/ProteccionDatosEcuador-Documento.pdf> accessed 5 May 2021).

135 Asamblea Nacional, Ley Orgánica de Protección de Datos Personales N° 459 (26 May 2021) <https://www.asambleanacional.gob.ec/es/leyes-aprobadas?leyes-aprobadas=768&title=datos+personales&fecha=> accessed 24 September 2021.

136 Ibid, art 17.

137 Ibid, art 42.

138 Ibid, art 48.

139 Ibid, arts 43, 46.

140 Ibid, art 68, 70.

141 The law as passed known as 'Decree 875' was removed from the Assembly's website upon the presidential veto; Abdías Zambrano, 'El Salvador Aprueba Su Ley De Datos Personales' (*ipandetec.org*, 22 April 2021) <https://www.ipandetec.org/2021/04/22/el-salvador-aprueba-su-ley-de-datos-personales/> accessed 24 September 2021.

Bukele.[142] A 'National Digital Authority' was also enacted by legislative decree to oversee implementation of the new legislation,[143] and vetoed as well. [144] Thus, El Salvador remains without a comprehensive data protection Law.

- **Guatemala** recognizes a right to privacy for personal communications in its Constitution, which has been developed through rulings of the Constitutional Court.[145] To date, however, there is no data privacy legal regime in place. Although several legislative initiatives promoting data protection and actively supported by civil society have been presented to the Parliament, none have yet been approved.[146]
- **Guyana** has no privacy or data protection law, although it has legislation specific to the financial sector.[147] However, Prime Minister Mark Philips announced an impending data protection law[148] and a request for draft proposals was published in November 2020.[149]
- **Honduras** protects the right to intimacy and confidentiality of communications in its Constitution.[150] Despite the absence of a specific law on data

142 Gobierno de El Salvador, Veto Presidencial (11 May 2021) <https://www.asamblea.gob.sv/sites/default/files/documents/correspondencia/EFBA7BEE-871B-40BE-BD0A-5BD80237CA90.pdf> accessed 24 September 2021; Milton Rodríguez, 'Bukele veta Ley de Protección de Datos Personales y otros decretos' (*elsalvador.com*, 19 May 2021) <https://www.elsalvador.com/noticias/nacional/nayib-bukele-veto-ley-proteccion-datos-personales/839543/2021/> accessed 24 September 2021.

143 María Teresa Gutiérrez, 'Por aprobar Ley de Protección de Datos y Ley de Creación de la Autoridad Nacional Digital' (*La Nueva Asamblea Legislativa*, 9 March 2021), <https://www.asamblea.gob.sv/node/11082> accessed 24 September 2021.

144 Milton Rodríguez (n 142).

145 See Constitución Política de la República de Guatemala [Constitution] 1993, art 24 (Guat), https://www.constituteproject.org/constitution/Guatemala_1993.pdf?lang=en.

146 See Comisión Presidencial de Derechos Humanos del Gobierno de Guatemala, Resolución 68/167 'El Derecho a la Privacidad en la era Digital' 7–8 (2014) <https://www.ohchr.org/Documents/Issues/Privacy/Guatemala.doc> accessed 24 Sptember 2021. See also Sara Fratti, *Estudio Centroamericano de Protección de Datos, Guatemala* (2019), 4.

147 'Guyana' (*DataGuidance*) <https://www.dataguidance.com/jurisdiction/guyana> accessed 15 May 2021.

148 Denis Chabrol, 'New Data Protection Law Coming – PM Philips' (DemeraraWaves, 20 September 2020 9:56 PM) <https://demerarawaves.com/2020/09/20/new-data-protection-law-coming-pm-phillips/> accessed 24 September 2021.

149 Bartlett D Morgan, 'Status of Data Privacy Laws in the Caribbean' (*BarttleMorgan*, 3 February 2021), <https://www.bartlettmorgan.com/2021/02/03/status-of-data-privacy-laws-in-the-caribbean-feb-2021/> accessed 24 Septe,ber 2021; see also Data Protection Bill Consultancy¸ Office of the Prime Minister, Cooperative Republic of Guyana <https://www.bartlettmorgan.com/wp-content/uploads/2021/02/F8E77B7E-899A-4294-BE65-AED7D80C3C1F.jpeg> accessed 20 May 2021.

150 Eduardo Tomé, *Estudio Centroamericano de Protección de Datos, Honduras* (2019) 3 <https://www.ipandetec.org/wp-content/uploads/2019/01/EDP_Honduras.pdf> accessed 24 September 2021.

protection, the country does have a National Commissioner for Human Rights with authority to protect personal data.[151] Furthermore, Honduras in 2015 added the writ of *habeas data* to its constitutional protections.[152] That same year, a bill on personal data protection was introduced in the Honduran Senate that focused on the protection of ARCO Rights and a sanctions regime.[153] Since 2018, Honduras has been debating legal reforms to enact a data privacy law in line with European standards under pressure from civil society actors to do so.[154]

– In 2017, **Mexico** enacted the General Law on the Protection of Personal Data in the Possession of Obligated Subjects, which imposed data privacy duties on public authorities and entities that were not covered by the private actor-focused Federal Data Protection Law of 2010.[155] The new law incorporates several GDPR key elements, including data portability, DPOs and DPIAs.[156] In 2021, the Government approved a controversial legal reform to create a central government database for mobile telephone users of sensitive personal data.[157] The Mexican Supreme Court is hearing numerous challenges to this initiative, not least for violating the Data Protection Law.[158] In the meantime, the Court

151 Ibid 5.

152 Ibid 3.

153 Ibid 10.

154 Oscar Zelaya, 'Honduras-La Proteccion de Datos en Honduras' (*Central-Law.com*, 23 April 2021) https://central-law.com/honduras-la-proteccion-de-datos-en-honduras/ accessed 24 September 2021; Verónica Arroyo and Hedme Sierra Castro, 'Honduras necesita un debate urgente sobre datos personales y libertad de expresión' (*Access Now*, 2019) <https://www.accessnow.org/honduras-igf/ accessed 26 February 2020>.

155 Cesar Cruz et al., 'Mexico' in Alan Charles Raul (ed), *The Privacy, Data Protection and Cybersecurity Law Review 266* (6th ed 2019) <https://www.sidley.com/-/media/publications/theprivacydataprotectionandcybersecuritylawreviewedition6.pdf> accessed 24 September 2021.

156 Ibid.

157 Decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión, Diario Oficial De La Federación [DOF] de 16.04.2021 (Mex), <https://dof.gob.mx/nota_detalle.php?codigo=5616165&fecha=16/04/2021> accessed 24 September 2021; 'Senado Aprueba, en lo General, Crear Padrón Nacional de Usuarios de Telefonía Movil' (*Senado.gob.mx*, 13 April 2021) <http://comunicacion.senado.gob.mx/index.php/informacion/boletines/50696-senado-aprueba-en-lo-general-crear-padron-nacional-de-usuarios-de-telefonia-movil.html> accessed 24 September 2021.

158 'INAI Presentó Ante la SCJN la Demanda de Acción de Inconstitucionalidad Contra el Panaut' (*Forojuridico.mx*, 14 May 2021), https://forojuridico.mx/inai-presento-ante-la-scjn-la-demanda-de-accion-de-inconstitucionalidad-contra-el-panaut/ accessed 24 September 2021; INAI, *Demanda de Acción de Inconstitucionalidad*, 13 May 2021 <https://home.inai.org.mx/wp-content/documentos/AccionesYControversias/Demanda_INAI_PANAUT.pdf> accessed 24 September 2021.

decided to suspend the collection of data due to the legal challenges filed.[159] In 2018, Mexico acceded to Convention 108 as well as the 2001 Additional Protocol on supervising authorities and transborder data flows.[160] For more information, see the Mexico case study, *infra* 4.3.

- **Nicaragua** protects the right to personal data and the *habeas data* action in its Constitution and Law on Protection of Personal Data (Act No 787) of 2012.[161] No legislative proposals for updating the Law have been found.[162] On January 2021, the telecommunication regulatory body (TELECOR) issued an administrative decree on cybercrime which may run counter to its Data Protection Law by granting police or the Public Ministry, subject to judicial approval, the authority to prompt disclosures of personal data within information systems.[163]
- **Panama** adopted its first data protection law in March 2019 soon after the GDPR came into force. The law came into effect in March 2021.[164] However, it acknowledges few of the GDPR's innovations (the right to data portability being one) while omitting most of them. Instead, the new Panamanian data protection regime follows a more sectorial approach like the one prevalent in the United States.[165]

---

159 Nicolas Lucas, 'Suprema Corte concede al IFT una suspensión contra el Padrón Nacional de Usuarios de Telefonía Móvil', *El Economista* (June 15, 2021) <https://www.eleconomista.com.mx/empresas/Suprema-Corte-concede-al-IFT-una-suspension-contra-el-Padron-Nacional-de-Usuarios-de-Telefonia-Movil-20210615-0030.html> accessed 24 September 2021.

160 See (n 320) and accompanying text.

161 Daniel López Carballo, 'Análisis de la Normativa Nicaragüense en Materia de Protección de Datos' (*Homepage of Daniel López Carballo*, 14 March 2019) <http://dlcarballo.com/2019/03/14/analisis-de-la-normativa-nicaraguense-en-materia-de-proteccion-de-datos/> accessed 24 July 2020.

162 Cristina Morales, 'Derechos Digitales en Nicaragua 2018' (*IPANDETEC*, 11 January 2019) <https://www.ipandetec.org/2019/01/11/derechos-digitales-en-nicaragua-2018/> accessed 27 July 2020.

163 Silvia Sanchez, 'Nicaragua y su Normativa de Ciberdelitos' (*ipandetec.org*, 15 February 2021) <https://www.ipandetec.org/2021/02/10/ciberdelito-nicaragua/> accessed 24 September 2021; Ley No 1042, 27 Oct 2020, Ley Especial De Ciberdelitos [Special Law on CyberCrime], ch VI, art 39, La Gaceta, Diario Oficial No 201, 30 Oct 2020 (Nicar) <http://legislacion.asamblea.gob.ni/normaweb.nsf/($All)/803E7C7FBCF44D7706258611007C6D87> accessed 24 September 2021.

164 Rodrigo Noriega, 'Empieza la era de protección de datos personales' (*Prensa.com*, 29 March 2021) <https://www.prensa.com/impresa/panorama/empieza-la-era-de-proteccion-de-datos-personales/> accessed 24 September 2021.

165 Email from Abdias Zambrano, Panamanian Institute for Law and New Technology (IPANDETEC), to Matías Jackson (July 28, 2020) (describing how different types of personal data are regulated by separate laws covering, for example, health or finance related data).

- In May 2021, in **Paraguay**, a comprehensive bill was proposed in Congress to update the country's Data Protection Law across the board[166] and bring it more into line international standards.[167] It seeks to build on the progress made by a similar 2019 legal reform of personal data protections that was restricted to the specific context of financial and credit information.[168] The recent proposed legislation is also modelled on the GDPR and seeks to create a single independent DPA[169] as well as create a right to data portability.[170]
- In **Peru**, the Regulatory Decree that implements the country's Protection of Personal Data Law (2011) was modified in 2017 to strengthen the regime by giving more independence to the DPA and increasing the severity of sanctions.[171] In December 2020, the Ministry of Justice and Human Rights approved an additional resolution adopting a method of calculating sanctions for violations of the Data Protection Law.[172]
- In **Suriname**, the right of privacy has constitutional status despite the lack of a comprehensive data protection law.[173] In May 2018, legislators proposed the Privacy and Data Protection Law, which does not refer explicitly to the GDPR.[174] It does, however, recognize the need to harmonize with international standards, including several of the Regulation's key elements, such as extraterritorial application, the right of erasure, data portability, and the duty

166 'Tras Meses de Estudio, Presentan Proyecto "De Protección de Datos Personales"' (*Honorable Cámara De Diputados*, 7 May 2021) <http://www.diputados.gov.py/index.php/noticias/tras-meses-de-estudio-presentan-proyecto-de-proteccion-de-datos-personales> accessed 24 September 2021.

167 AccessNow (n 130), 29:00–30:20.

168 Ley Nº 6534 de Protección de Datos Personales Crediticios, 17 October 2020 (Para) <https://www.bacn.gov.py/leyes-paraguayas/9417/ley-n-6534-de-proteccion-de-datos-personales-crediticios> accessed 24 September 2021.

169 Honorable Camara De Diputados (n 166); AccessNow, 'Legislando por la protección de datos personales: Conversatorio entre Europa y América' (*YouTube*, 11 May 2021), 32:00–32:57, 35:20–36:02 <https://www.youtube.com/watch?v=fJyJkw07PlQ&ab_channel=AccessNow> accessed 24 September 2021.

170 AccessNow, (n 130), 34:30–34:55 <https://www.youtube.com/watch?v=fJyJkw07PlQ&ab_channel=AccessNow> accessed 24 September 2021.

171 Decreto Legislativo N° 1353, 15 September 2017, Diario Oficial El Peruan 45 (Peru) <https://www.gob.pe/institucion/midis/normas-legales/9641-019-2017-jus> accessed 24 September 2021.

172 Adriana Barrera, 'Registro de Datos Personales: se Aprueba Metodología para el Cálculo de Multas en Materia de Protección de Datos Personales en Perú' (*IAPP*) <https://iapp.org/news/a/registro-de-datos-personales-se-aprueba-metodologia-para-el-calculo-de-multas-en-materia-de-proteccion-de-datos-personales-en-peru/> accessed 21 May 2021.

173 The Constitution of the Republic of Suriname, 1987, art 17 (Surin).

174 Paolo Balboni, 'The New Surinamese Privacy and Data Protection (SPDP) Law' (*PaoloBalboni*, 15 May 2018) <https://www.paolobalboni.eu/index.php/2018/05/15/the-new-surinamese-privacy-and-data-protection-spdp-law/> accessed 24 September 2021.

to notify breaches, among others.[175] It is uncertain whether the bill will be enacted.[176]

- In 2018, **Uruguay** approved changes to its 2008 Law to introduce GDPR key elements.[177] Among these are the notification of data breaches, the duty to carry out impact assessments, and the designation of data protection officers under certain circumstances.[178] The legislature opted not to include other key elements such as the right to be forgotten, the right to data portability or a tougher sanctions regime.[179] In February 2020, however, the Executive issued Decree 64/020 regulating certain aspects of the law relating to data protection officers and impact assessments. This decree further reinforced the liability of entities that treat personal data.[180] It is worth noting that in 2013, Uruguay became the first country outside of Europe to adhere to Convention 108; in 2021, Uruguay became the first Latin American country to fully ratify the 2018 Protocol 'modernizing' the convention.[181] For more information, see the Uruguay case study, *infra*, in 4.4.
- The **Venezuelan** Constitution contains various provisions protecting privacy, which can be enforced directly through the courts.[182] However, Venezuela lacks a data protection law and a data protection authority,[183] with early efforts to create a data protection law ceasing after 2005.[184]

This panoramic view of the region's data privacy regimes allows us to formulate several initial observations, which are the subject of the next sub-section.

---

175 Ibid.

176 Cynthia J Rich, 'Assessing the Current and Future Privacy Landscape in the Americas' (*Morrison Foerster*, 6 January 2021) <https://www.mofo.com/resources/insights/210106-future-privacy-landscape.html> accessed 24 September 2021.

177 Ley No 19670, Oct 15, 2018 (Uru) <https://www.impo.com.uy/bases/leyes/19670-2018> accessed 24 September 2021.

178 Ibid.

179 Florencia Castagnola and María Anza, 'Informe Especial: Cambios a Normativa sobre Protección de Datos Personales' (*Guyer y Regules*) <https://www.guyer.com.uy/en/what_we_do/news-knowledge/on-line-news/informe-especial-cambios-a-normativa-sobre-proteccion-de-datos-personales/> accessed 23 July 2020.

180 Mario Ferrari Rey, 'Protección de Datos Personales: Decreto 64/020' (*PwC*, 6 March 2020), <https://www.pwc.com.uy/es/acerca-de-nosotros/prensa/2020/proteccion-de-datos-personales–decreto-64-020.html> accessed 24 September 2021.

181 See (n 370) and accompanying text.

182 Acceso Libre & Privacy International, *The Right to Privacy in Venezuela (Bolivarian Republic of)* (2016) 5 <https://privacyinternational.org/advocacy-briefing/1062/right-privacy-venezuela-bolivarian-republic> accessed 24 September 2021.

183 'Venezuela' (*DLA Piper: Data Protection Laws of the World*, 18 January 2019), <https://www.dlapiperdataprotection.com/index.html?t=law&c=VE> accessed 24 September 2021.

184 Ibid.

3.1 General Findings Regarding the Latin American Panorama

Through the panorama portrayed in Table B, we gain a broad perspective on the status of data privacy regulation in Latin America in 2021, with a focus on the changes introduced since the GDPR's adoption in April 2016. In South America, eight of 12 countries had data protection laws in place at the end of 2021, which is nearly 70% of the continent; in Central America, however, only three of seven countries did, or about 40%. Overall, 12 of the 20 countries we examined in Latin America, which encompasses both South and Central America, had a personal data protection regime, or 60%. Those 12 countries are Argentina (2000), Brazil (2019), Chile (1999), Colombia (2012), Costa Rica (2011), Ecuador (2021), México (2010 & 2017), Nicaragua (2012), Panamá (2019), Paraguay (2000), Perú (2011) and Uruguay (2008 & 2018).

But if you add in the number of countries in Latin America that are currently in the process of debating and/or enacting new data protection laws, that 60% figure for the region improves significantly. Currently, there are legislative initiatives to this end underway in three South American countries that do not have a data protection law – Bolivia, Guyana and Suriname – and in three similarly situated Central American countries: El Salvador, Guatemala and Honduras. This means that 90% of Latin America is either covered by data protection laws or may soon be. Only Venezuela in South America and Belize in Central America have neither data protections laws nor a process to legislate one.

A close examination of Table B points up other interesting insights. If we focus for a moment on the nine countries that already had a general data protection regime prior to 2016, we discover that nearly 80% of them have since updated, or sought to update, their data privacy legislation (Argentina, Chile, Colombia, Costa Rica, Mexico, Paraguay and Uruguay). Specifically, three countries in this latter group have modernized their data protection laws with new GDPR-inspired provisions (Costa Rica, Mexico, and Uruguay), while another four plus Costa Rica have considered or are studying draft laws to amend their existing regime (Argentina, Colombia, Chile, and Paraguay).[185] Two countries – Peru and Nicaragua – have pre-existing data protection laws but have not made major legislative moves to update them, although Peru has made regulatory tweaks to its regime.[186]

---

185 Costa Rica modernized its data protection regime through executive decree in 2016, at the same time that it is currently debating proposed legislation that would further overhaul that regime. See (n 130–133) and accompanying text.

186 In September of 2018, the Peruvian Data Protection Authority issued an Advisory Opinion expressly analyzing the applicability of the GDPR in Peruvian territory. The Peruvian DPA is thus aware of the relevance of the GDPR provisions, although local regulations still prevail. See Carol

In addition, some of the aforementioned governments are reforming their data protection laws with a view to retaining or seeking an adequacy determination under the GDPR. In the region only Argentina and Uruguay have an adequacy determination in place from the European Commission under Directive 95/46.[187] To this end, both countries have been actively revising (Uruguay) or seeking to revise (Argentina) their already 'adequate' data privacy regimes, even as updated adequacy determinations by the European Commission under the GDPR are pending.[188] For instance, Argentina ratified Convention 108 and its additional 2001 Protocol in 2018 and 2019, respectively;[189] in 2018 it signed the Amending Protocol for Convention 108+ as well.[190] Uruguay went further, becoming in April 2021 the first Latin American country to ratify the 2018 Amending Protocol to Convention 108, to which it had already acceded in 2013.[191] There is reason to believe that that ratification of the Council of Europe's Convention 108 and its protocols is a stepping stone towards obtaining a positive adequacy determination,[192] which may explain Mexico's decision in 2018 to ratify Convention 108 and the 2001 Additional Protocol.[193] Other countries such as Brazil, Colombia and Costa Rica are studying the possibility of following suit.[194]

Looking now at the other end of the data protection spectrum, our study also shows that over a third of the countries in Latin America do not yet have a general data protection regime (8 out of 20). In four of them – Bolivia, El Salvador, Guyana, and Suriname – the respective legislatures have at least debated proposed laws since 2016, though without success. In two others – Guatemala and Honduras – civil society groups have been pushing for legislative initiatives that would lead to the adoption of legal frameworks for data privacy that encompass the GDPR's key

Quiroz, 'The impact of the GDPR outside the EU – Peru part' (*Ius Laboris*, 17 September 2019) <https://theword.iuslaboris.com/hrlaw/whats-new/the-impact-of-the-gdpr-outside-the-eu> accessed 24 September 2021.

187 See (n 205 and 366) and accompanying text.

188 See (n 211–216, 371–373) and accompanying text; GDPR (n 1), art 45(9) (establishing that adequacy decisions under Directive 95/46/EC 'shall remain in force until amended, replaced or repealed'); see also Council of Europe, *Adequacy Decisions* <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#relatedlinks> accessed 6 August 2021.

189 See (n 206) and accompanying text.

190 See (n 208) and accompanying text.

191 See (n 369–370) and accompanying text.

192 See Eduardo Bertoni, 'Convention 108 and the GDPR: Trends and perspectives in Latin America' (2021) 40 Computer Law and Security Review, 2.

193 Ibid 3; see also (n 320) and accompanying text.

194 Bertoni (n 192) 4.

elements, also without success.[195] (Belize and Venezuela, as noted, have shown little movement on this front). This suggests that there is still some distance to go in the regional development of data privacy protections generally, and in measuring the GDPR's impact, more specifically.

Finally, it is worth observing that Table B offers qualitative as well as quantitative insights. In particular, it allows us to analyze the types of legislative changes that have taken place between 2016 and 2021. In those five years, for instance, countries undergoing reforms have moved at different paces. Three countries have enacted new laws and/or regulatory reforms to update their pre-existing data protection regime (Costa Rica, Mexico, and Uruguay), while three have enacted entirely new laws (Brazil, Ecuador and Panama) to establish such regimes for the first time. In parallel, seven countries have considered or are studying either the adoption of a new data protection law (Bolivia, El Salvador, Guyana and Suriname), or the reform of their existing data privacy frameworks (Argentina, Chile, Colombia, Costa Rica and Paraguay). Table B provides information on the nature of those legislative initiatives; for example, it distinguishes between efforts that would implement the GDPR's key elements almost in their totality (Argentina) and those that seem to ignore most of the Regulation's innovative features (Panama, El Salvador), as well as everything in-between.

In sum, Table B provides a good overview of the current state of data privacy law in Latin America. We can see that by 2021 most countries in the region – 90% (18 of 20) by our count – have a general data protection law or are trying to enact one. Since 2016, a sweeping 'third wave' of legal reform has spread data protection regimes inspired by the GDPR to several new countries, as well as led several others to update their pre-existing legal frameworks in line with the Regulations' transnational standards. Even so, questions remain about how these Latin American countries embarking on the modernization of their data privacy regimes navigate that course, and the extent to which they choose to follow the example of the GDPR – the acknowledged leader in this field – or not. To address these questions, we deploy case studies in Part III that delve into the details of data privacy reform in four Latin American countries.

4 Country Case Studies

In this Part we move into a detailed exploration of four strategic jurisdictions in Latin America identified as 'first movers' in terms of European norm adoption: Brazil, Chile, México, and Uruguay. Each represents a particular approach to data

195 See (n 146 and 150) and accompanying text.

privacy regulation in the region at present. One objective of this third Part is thus to examine more closely the different types of legislative reforms and updates to Latin American data protection regimes that have been considered and/or approved since 2016 when the GDPR was approved. A second objective, building on the first, is to use the four case studies as inputs for the comparative analysis that underpins the Part IV to better understand the influence that the GDPR is having in the region more broadly. We believe that a closer look at each will allow us to appreciate more fully the nature and extent of the legal reforms in the countries studied. By reviewing the respective experiences since 2016, then, we can better understand not just the legislative initiatives themselves, but also the context and motivations that drive them.

The four case studies – Brazil, Chile, Mexico and Uruguay – were chosen in part because of the respective governments' express efforts to modify their countries' data privacy regimes to respond or adapt to the GDPR. In this regard, they reflect to various degrees the progress taking place regionally in relation to the legal reforms we previewed in 3. Geographically, Mexico is in Central America, while the remaining three countries are in South America. Brazil and Mexico adopted entirely new 'omnibus' legislation, while Uruguay pursued piecemeal reform. Chile represents those countries still in the process of debating legal reform to pre-existing data protection laws. The cohort thus exemplifies to a great extent the range of domestic experiences prevalent in the region, as reflected in Table B. That said, we would be remiss not to recognize a prominent omission from our roster of case studies: Argentina. We chose not to include Argentina due to the fact that its legislative activity at the time of this writing is greatly in flux. Given the importance of discussing the country in relation to the subject matter, however, we have included below a brief overview of data privacy protections and reform in Argentina as part of this introduction to the more in-depth case studies.

A word about methodology. With respect to the case studies for Brazil, Chile, Mexico and Uruguay, we will be tracking in each country's respective legislation the GDPR's key elements as set out in Part I and summarized in Table A. This will allow us to measure the extent to which, objectively, the pertinent norms incorporate the unique GDPR elements identified, or not; the strategic sample provided by the key elements is broad enough to support at least a preliminary analysis of the degree of assimilation present from a technical point of view. But the inquiry does not end there. We have also mined primary and secondary sources for complementary information on the context of the legislative changes proposed or enacted; these sources shed light on the motivations and objectives of the law and policymakers involved. Our overarching goal as noted already is to provide

qualitative insights into the political and social processes behind the legislative initiatives to modernize data protection in these countries.

The results of this initial exercise are captured in Table C, entitled 'GDPR Key Elements as Indicators of Influence.' For each of the four case studies, this Table captures the degree to which the EU Regulation's innovative elements identified in Part I are present in the selected country's proposed or adopted legislation.[196] To achieve this, the horizontal axis of Table C imports verbatim the final row of 'Basic Indicator Queries' for each of the nine key elements identified from Table A. Those then became the questions that guide the process of filling in Table C, because the answer to the indicator query determines whether the referenced GDPR key element is present or not. On the vertical axis of Table A are listed the four countries, along with the pertinent legislation's identification number and hyperlink to the original source. When cross-referenced, the two axes of Table C present a more detailed image of the extent to which the proposed or enacted legislation for these countries incorporates the GDPR's unique features as distilled by the key elements.

The presence of several GDPR key elements in these first mover countries can give rise, at the very least, to the impression of influence by the former on the latter. It is necessary to acknowledge, however, that such correlation does not necessarily signify causation. We know that presumptions of influence are, of course, rebuttable by further investigation producing evidence to the contrary.[197] Graham Greenleaf points out that the question of causation regarding whether the European data protection rules have influenced the adoption of similar provisions by third countries can only be answered by detailed studies that bear down on the particularities of each countries' legal history, as well as the myriad of reasons that go into the adoption of particular legislation.[198] With this important caveat in mind, we developed the case study methodology described above which we believe moves us in the right direction.

We call the GDPR's 'key' elements 'indicators of influence' because the more these elements are present in the legislative acts studied, the stronger one can assume the GDPR's influence to be. That is, the more correlation there is between a

196 See supra 2.2.

197 Greenleaf (n 6), 74. We recognize, for example, that the relationship between the presence of the GDPR key elements in foreign jurisdictions, and recognition as an adequate country, is not straightforward. 'Adequacy assessments take into account different factors, and do not only consider the formal law, but also its implementation in practice. […] [I]t is quite possible that a law with a high number of "European" elements might also have broad exemptions to its principles, and major deficiencies in its enforcement procedures, so […] its numerical summary cannot be simply equated with the "strength" of a data privacy law.' Ibid, 76.

198 Ibid, 74.

country's legislation and the key elements identified, 'the more it is suggestive of a conscious influence of the [European model] in [that] particular country.'[199] Fortunately, in most cases, we do not have to speculate solely on the basis of this technical analysis; legislative history and contemporary press accounts of the legal processes examined will expressly attest to the role of the GDPR in the legislative processes examined. Interpreting both sets of inputs together – textual analysis alongside contemporary accounts – we can fashion a more informed and accurate idea of the nature of the GDPR's influence in that country to date. Before turning to the case studies themselves, however, we should take a look at the evolving panorama in Argentina, which, though not a case study country for the reasons alluded to earlier, has nonetheless been a data protection trailblazer in the region.

4.1 Data Privacy in Argentina

Argentina has long been in the forefront of data protection in Latin America. Like many countries in the region, Argentina built its personal data protection regime on the constitutionally protected right of *habeas data*. Specifically, the 1994 Argentinean Constitution incorporated the right to *habeas data* as part of the section on 'amparo' actions, which are constitutional writs to protect fundamental rights.[200] In 2000, the Argentine Congress approved Law No 25.326 on Personal Data Protection,[201] making it one of the first Latin American countries to adopt omnibus legislation that closely tracked EU Directive 95/46.[202] Along with Chile and Paraguay, it was thus part of the 'first wave' of data privacy legislation that came about in the wake of the Directive's approval.[203]

After approval of the Data Protection Law in 2000, Argentina broadened its alignment with the European approach.[204] In 2003, it became the first country in Latin America to be recognized by the European Commission as having an

199 See ibid 76 (although the author refers to the presence of the Directive's elements as suggestion of conscious influence in a particular country, the same argument can be made for the elements present in the GDPR).

200 Constitución Nacional [Const Nac] (Arg), Art 43, <https://www.constituteproject.org/constitution/Argentina_1994.pdf?lang=en> accessed 24 September 2021; see also Thomas Roberts, 'The Writ of Amparo: A Remedy to Protect Constitutional Rights in Argentina' (1970) 31 Ohio St LJ 831, and Hector Fix Zamudio, 'The Writ of Amparo in Latin America' (1982) 13 U Miami Inter-Am L Rev 361 for more on 'amparo' as constitutional writs.

201 Law No 25326, Oct 30, 2000, BO 2.11.2000 (Arg) <http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm> accessed 24 September 2021.

202 Bradford (n 14) 150.

203 Voss and Castets-Renard (n 94) 314; see also (n 95) and accompanying text.

204 Bradford (n 14) 150.

'adequate' level of protection under Directive 95/36, allowing for the free flow of data with Europe.[205] More recently, in 2019, the Argentine Congress ratified the Council of Europe's 1981 *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* and signed the *Additional Protocol* regarding supervisory authorities and transborder data flows.[206] As such, it is one of the few non-European countries, along with Mexico and Uruguay, to have ratified Convention 108.[207] In September 2019, Argentina signed the Amending Protocol establishing Convention 108+, becoming only the second Latin American country after Uruguay to do so.[208] In 2020, the data protection authorities of Argentina and Uruguay introduced a joint Guide for Impact Assessment for Data Protection aimed at providing a common framework for controllers to follow in both countries.[209] This guide, which expressly cites the GDPR as a source of inspiration, includes a matrix for conducting risk assessments.[210]

Although reforms to the 2000 Data Protection Law are under consideration by the Argentine Congress, the legislative panorama is not nearly as clear or concrete as that in the case study countries selected. In September 2018, then President Mauricio Macri submitted a comprehensive draft law to Congress with the express aim of further modernizing the country's data protection regime and adapting it to 'regulatory changes that have occurred in

205 Commission Decision 2003/490/EC of 30 June 2003 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequate Protection of Personal Data in Argentina, [2003] OJ L 168/19 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003D0490> accessed 24 September 2021.

206 Law No 27483, 2 January 2019, [No 34.025] BO 4 (Arg) <https://www.boletinoficial.gob.ar/detalleAviso/primera/199254/20190102> accessed 24 September 2021; see also Council of Europe, 'Chart of Signatures and Ratifications of Treaty 181' <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=181> accessed 7 August 2021.

207 See Council of Europe, 'Chart of Signatures and Ratifications of Treaty 108', <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=9dwNmX8W> accessed 8 August 2021.

208 'Argentina se Suma al Convenio 108+' (*Argentina.gob.ar*, 20 September 2019) <https://www.argentina.gob.ar/noticias/argentina-se-suma-al-convenio-108> accessed 24 September 2021.

209 'Argentina y Uruguay Lanzan la Guía "Evaluación de Impacto en la Protección de Datos"' (*Argentina.gob.ar*, 28 January 2020) <https://www.argentina.gob.ar/noticias/argentina-y-uruguay-lanzan-la-guia-evaluacion-de-impacto-en-la-proteccion-de-datos> accessed 24 September 2021.

210 Agencia de Acceso a la Información Pública & Unidad Reguladora y de Control de Datos Personales, 'Guía de Evaluación de Impacto en la Protección de Datos' (*gub.uy*, 28 January 2020) <https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-evaluacion-impacto-proteccion-datos> accessed 24 September 2021.

comparative law in recent years,' especially the GDPR.[211] The Macri bill, however, was allowed to lapse during the COVID-19 pandemic[212] and lost parliamentary status in 2020.[213] Nevertheless, towards the end of 2020, Argentine legislators introduced two new bills that substantially reproduce the purpose, focus and content of the Macri bill.[214] These developments, though inchoate, are significant because our analysis of the Macri bill found that it contained nearly all of the GDPR's key elements,[215] as apparently do the subsequent bills that are still pending.[216] All this suggests that the adoption in Argentina of a revised data protection law substantially aligned with the GDPR is merely a question of time.

4.2 Brazil

Brazil offers another sample in regional data privacy regulation that, like Argentina, took place in response to the adoption of the GDPR in Europe; it is notable, however, for another reason: even though Brazil was the first country in Latin America to introduce *habeas data* protection into its Constitution in 1988,[217] it

211 Poder Ejecutivo Nacional, *MEN-2018-147-APN-PTE Mensaje Proyecto Ley de Protección de Datos Personales*, 19 September 2018 (Arg) <https://www.argentina.gob.ar/sites/default/files/mensaje_ndeg_147-2018_datos_personales.pdf> accessed 24 September 2021.

212 See Senado Argentina, 'Datos del Expediente – No 283/18' <https://www.senado.gob.ar/parlamentario/comisiones/verExp/283.18/PE/PL> accessed 24 September 2021; see also Ministerio de Justicia y Derechos Humanos, 'Caducidad de Los Proyectos de Ley en Argentina' <http://www.saij.gob.ar/13640-nacional-caducidad-proyectos-ley-lns0001967-1949-09-30/123456789-0abc-defg-g76-91000scanyel> accessed 24 September 2021.

213 'Nuevo Proyecto de Ley para Reemplazar la Actual Ley de Protección de Datos Personales' (*Marval O'Farrell Mairal*, 21 December 2020) <https://www.marval.com/publicacion/nuevo-proyecto-de-ley-para-reemplazar-la-actual-ley-de-proteccion-de-datos-personales-13873> accessed 24 September 2021.

214 Diputados Argentina, 'Proyecto 6234-D-2020' <https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2020/PDF2020/TP2020/6234-D-2020.pdf> accessed 12 May 2021; Senado Argentina, 'Número de Expediente 2986/20' <https://www.senado.gob.ar/parlamentario/parlamentaria/441614/downloadPdf> accessed 24 September 2021.

215 See Poder Ejecutivo Nacional (n 211), art 4 (expanding territorial scope), art 31 (expanding users rights to include the Right to Erasure), art 38 (requiring privacy by design measures, art 40 & 42 (requiring impact assessments).

216 Diputados Argentina, 'Proyecto 6234-D-2020' <https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2020/PDF2020/TP2020/6234-D-2020.pdf> accessed 12 May 2021; Senado Argentina, 'Número de Expediente 2986/20' <https://www.senado.gob.ar/parlamentario/parlamentaria/441614/downloadPdf> accessed 24 September 2021.

217 See Constituição Federal [CF] [Constitution] art 5 (Braz).

had no general data protection law at all until 2018.[218] It was in August of that year that Brazil approved the General Personal Data Protection Act (*Lei Geral de Proteção de Dados Pessoais* or LGPD), which was originally scheduled to go into effect in August of 2020.[219] Although the government of Jair Bolsonaro tried to delay by a year the LGPD's entry into force due to the pandemic,[220] the Law ultimately took effect on September 18th, 2020.[221] Its enforcement of the sanctions regime established, however, did not become active until August 2021.[222]

The Brazilian General Personal Data Protection Act follows the GDPR not just in name, but in substance as well. Although it did not come with an official message expressly referencing its European inspiration and counterpart, the Brazilian statute was overtly intended not just to establish a data protection regime for the first time, but to do so in line with the prevailing international standards set by Europe.[223] As the discussion below will show, almost all of the GDPR's key elements appear in the LGDP, which consciously follows in the EU Regulation's footsteps in terms of format, logic and structure.[224] That said, even though the LGPD tracks the GDPR closely, it is not identical in every respect.[225] One example of this variance is the establishment of a data protection agency, the *Autoridade*

218 Lei No 13.709, de 14 de Agosto de 2018, Diário Oficial da União [DOU] de 15.8.2018 (Braz) <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> accessed 24 September 2021.

219 Ibid.

220 Art 20, Lei No 14.010, de 10 de Junho de 2020, Diário Oficial da União [DOU] de 12.6.2020 (Braz) <https://legis.senado.leg.br/norma/32250736> accessed 24 September 2021.

221 'Brazil' (*DLA Piper, Data Protection Laws of the World*, 28 January 2021) <https://www.dlapiperdataprotection.com/index.html?t=law&c=BR> accessed 24 September 2021.

222 Lei No 13.709, de 14 de Agosto de 2018, Diário Oficial da União [DOU] de 15.8.2018 (Braz) <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm#art65> accessed 24 September 2021; See also 'Brazil' (*DataGuidance*) <https://www.dataguidance.com/jurisdiction/brazil> accessed 20 May 2021.

223 See Christian Perrone and Sabrina Strassburger, 'Privacy and Data Protection – From Europe to Brazil' (2018) 6 Panorama Braz L 82, 98. See also Carol Siqueira, 'Deputados Defendem Projeto sobre Proteção de Dados Pessoais' (*Câmara dos Deputados*, 29 May 2018) <https://www.camara.leg.br/noticias/539247-deputados-defendem-projeto-sobre-protecao-de-dados-pessoais/> accessed 24 July 2020; Janary Júnior, 'Marco Legal da Proteção de Dados Pessoais é Sancionado; Lei Entra em Vigor em 2020' (*Câmara dos Deputados*, 14 August 2018) <https://www.camara.leg.br/noticias/543434-marco-legal-da-protecao-de-dados-pessoais-e-sancionado-lei-entra-em-vigor-em-2020/> accessed 29 July 2020; Paula Soprana, 'Saiba o que Muda com a Lei Geral de Proteção de Dados Pessoais' (*Folha de São Paulo*, 15 August 2018) <https://www1.folha.uol.com.br/mercado/2018/08/saiba-o-que-muda-com-a-lei-geral-de-protecao-de-dados-pessoais.shtml> accessed 29 July 2020.

224 Perrone and Strassburger (n 223) 98.

225 Michael Baxter, 'Brazil's General Data Protection Law isn't quite GDPR' (*PrivSec Report*, 21 August 2018) <https://gdpr.report/news/2018/08/21/brazils-general-data-protection-law-isnt-quite-gdpr/> accessed 21 February 2020.

Nacional de Proteção de Dados (ANDP), as part of the Executive, rather than as the fully independent authority mandated by article 51 of the GDPR.[226]

In any case, Brazil checks nearly every box in Table C's accounting of GDPR key elements. Beginning with the General Provisions, the LGPD adopts a broad baseline scope with both extraterritorial reach and application to data processors (*operadores*) that seeks to protect Brazilian resident's personal data regardless of where its processing is carried out.[227] The extra-territorial provisions activate when one of two conditions are met: where the processed data belongs to persons residing in Brazilian territory, or where the purpose served by the processing is to offer such persons goods or services online.[228] Moreover, data processors must comply with all the duties and responsibilities that data controllers have.[229]

In addition to enacting a scope of application similar to the GDPR's, the Brazilian law likewise adopts a panoply of data subject rights that includes those to erasure and to data portability. So, on the one hand, the LGPD grants individuals the right to ask for erasure of personal data when it is inaccurate or out of date.[230] The legislators chose not to use the exact term 'right to be forgotten' because of the challenges noted surrounding the term in the Latin American context, as well as the related clashes with freedom of expression.[231] Although some Brazilian commentators include it in the long list of substantive similarities between the LGPD and the GDPR,[232] it is at best unclear what the operative effect would be.

---

226 The process behind the creation of an independent DPA in Brazil has not been straightforward. After Congress approved LGPD, then President Michel Temer vetoed the section that would have created an independent national agency as required by the GDPR. This veto was later reversed by executive order to create the *Autoridade Nacional de Proteção de Dados* (ANDP) under control of the President's office. This means that, although independent in name, many believe that the ANDP's dependence on the executive power may negatively impact its autonomy. See Abigayle Erickson, 'Comparative Analysis of the EU's GDPR and Brazil's LGPD: Enforcement Challenges with the LGPD' (2019) 44 Brook J Int Law 859, 861.

227 Lei No 13.709 (n 218), art 3; see also Perrone & Strassburger (n 223) 97.

228 Lei No 13.709 (n 218), art 3; see also Perrone & Strassburger (n 223) 97.

229 Lei No 13.709 (n 218), art 42.

230 Ibid, art 16 and 18.

231 See Rafaella Couto Ferreira, 'O Alcance do Direito Ao "Esquecimento" no Ordenamento Juridico Brasileiro em Relação ao Controle de Dados Das Pessoas Físicas Na Internet' (2020) 4 Rev Iniciaç Científica E Ext Fac Direito Franca, 870; see also Júlia Costa de Oliveira, *Direito ao esquecimento e seus mecanismos de tutela na internet: Como alcançar uma proteção real no universo virtual?* (2020).

232 See, eg, Baxter (n 225); Lucas Souza, 'A Lei Geral de Proteção de Dados Pessoais: Um Novo Desafio para o Varejo' 5 <https://www.migalhas.com.br/arquivos/2020/1/46525417897C00_Aleigeraldeprotecaodedadospess.pdf> accessed 24 September 2021; Sandra Martini and Lais Bergstein, 'Aproximações entre o Direito ao Esquecimento e a Lei Geral de Proteção de Dados Pessoais (LGPD)' (2019) 1 Disruptiva; Anderson Schreiber, 'Proteção de Dados Pessoais no Brasil e

On the other hand, the LGPD similarly recognizes the right to data portability.[233] Although Brazilian legislation previously only contemplated the right to portability with respect to personal data held by telecommunications companies, the new provision in the LGPD is a general right applicable to any kind of data controller.[234] The Law requires a controller to send personal data to another service or product provider upon request 'in accordance with the regulations of the national authority, subject to commercial and industrial secrets.'[235] In this regard, the new law does not provide details on how it is to be implemented. But it does seem to be in tension with GDPR art. 20's dictate that the transfer of personal data between controllers upon request by the data subject must be 'without hindrance.'[236]

Having constructed its data protection regime upon the same principles as the GDPR, it is no surprise to find that the LGDP followed the European model of enshrining consent as the main basis for legitimate processing.[237] Of note is that Article 8 of the Brazilian Law establishes that consent may be revoked at any time upon the express manifestation of the holder, through a free and facilitated procedure.[238] However, there are some differences in the concept of consent when compared with GDPR; for example, the LGPD goes further in requiring 'specific and highlighted consent' from the data subject for international transfers of their personal data.[239] Another variance from the European norm of relevance to this discussion is the lack of express language to the effect that consent must be 'as easy to withdraw as to give.'[240] For this reason, we do not register the LGPD as meeting that key element with respect to consent in Table C.

With respect to the GDPR's other key elements of personal data breach notification, impact assessments and protection officers, the LGPD is largely, but not perfectly, in harmony with its European counterpart. For instance, the Brazilian Law mandates that data controllers report data breaches to both national authorities and affected data subjects *only* when those breaches may cause related risks or damage to the latter.[241] Another variance in this regard is that the Law does

---

na Europa' (*Carta Forense*, 5 September 2018) <http://www.cartaforense.com.br/conteudo/colunas/protecao-de-dados-pessoais-no-brasil-e-na-europa/18269> accessed 30 July 2020.

233 Lei No 13.709 (n 218), art 18 (V) & (IX).

234 Perrone & Strassburger (n 223) 92.

235 Lei No 13.709 (n 218), art 18 (V).

236 See GDPR (n 1), art 20.

237 Lei No 13.709 (n 218), art 7 (I). See also Perrone and Strassburger (n 223) 89.

238 Lei No 13.709 (n 218), art 8.

239 Compare Lei No 13.709 (n 218), art 33 (VIII) with GDPR (n 1), art 49(1) (requiring 'explicit consent'); see also Perrone and Strassburger (n 223), 90.

240 GDPR (n 1), art 7(3).

241 Lei No 13.709 (n 218), art 48.

not impose a time restriction for breach notifications, only requiring that notice be given 'within a reasonable period, as defined by the national [data protection] authority.'[242] The GDPR, of course, requires that the supervisory authority be notified of any breach of personal data with 72 h, regardless of whether it poses a 'high risk' of harm to data subjects.[243]

There are likewise significant divergences around data protection impact assessments (DPIAs) and the designation of data protection officers (DPOs). With respect to the former, the LGPD defines the DPIA as a 'report (…) of the controller that contains the description of the processes for processing personal data that may generate risks to [users'] civil liberties and fundamental rights (…).'[244] However, it does not make them mandatory for controllers as does the GDPR where said risks are 'high';[245] instead, the Brazilian Law authorizes the ANPD, the new national data protection authority, to request that controllers (public or private) conduct DPIAs under certain circumstances.[246] For instance, the circumstances that may lead the ANPD to exercise its discretion in this regard include data processing that takes place because it is 'necessary to serve the legitimate interests of the controller,' except where the prevailing fundamental rights and freedoms of the data subjects require the protection of their personal data.[247] In that case, the ANPD may, but is not required to, commission a DPIA from the controller.[248]

As concerns the designation of data protection officers, the LGPD obligates only controllers to comply with this duty, although it is defined more broadly than in the GDPR.[249] The European Regulation goes further in requiring that both controllers and processors name a DPO if they are a public authority, are processing sensitive personal data, or engage in the 'regular and systematic monitoring of data subjects on a large scale.'[250] But, on the other hand, the Brazilian Law requires all controllers to name a 'person in charge' of the data processing whose duties are similar to those of the European DPOs.[251] Those duties include accepting complaints from and communicating with data subjects, facilitating communications with the DPA, providing guidance to the controllers' employees

242 Perrone and Strassburger (n 223) 93.
243 GDPR (n 1), art 33, 34.
244 Lei No 13.709 (n 218), art 5(XVII).
245 GDPR (n 1), art 35(1).
246 Lei No 13.709 (n 218), art 10, 32, 38. See also Perrone and Strassburger (n 223) 94.
247 Lei No 13.709 (n 218), art 7(IX).
248 Ibid, art 10(II) § 3.
249 Ibid, art 41.
250 GDPR (n 1), art 37.
251 Lei No 13.709 (n 218), art 41; see also Abigayle Erickson, 'Comparative Analysis of the EU's GDPR and Brazil's LGPD: Enforcement Challenges with the LGPD' (2019) 44 Brook J Int'l L 859, 884.

and contractors about the practices to be taken in relation to personal data, and performing other attributions determined by the controller or the ANPD.[252] In this sense, the Brazilian Data Protection Authority can calibrate different levels of compliance according to the nature and size of the entity or the volume of data processing operations.[253]

Finally, regarding accountability, there is again a partial following of the European model. On the one hand, just as the GDPR mandates, the ANPD will have the authority to impose administrative sanctions on 'data processing agents,' ie both controllers and processors.[254] Those sanctions can take the form of fines that can scale up to 2% of revenues generated in Brazil, with a maximum possible of 50 million reais (approximately USD 9,200,000).[255] There is no differentiation between serious and other breaches of the LGPD; the ANPD is given broad leeway to calculate the fines and other sanctions.[256] This means that while Brazilian legislators followed the criteria embraced by the GDPR of setting hefty fines on the basis of an organization's revenues, they made no express distinction for grave breaches and chose to limit their revenue baseline to domestic production only, ie those of the 'private company, group or conglomerate in Brazil in its last year.'[257] So, while still imposing significant sanctions, the LGPD declined to make them as potentially onerous as those enabled under the European Regulation, which (in)famously based its fines on an offending enterprise's global revenue stream.[258]

Since the LGPD entered in force, the Brazilian authorities have taken significant steps to further develop the new data protection regime. In August 2020, President Jair Bolsonaro issued executive Decree No 10,474 establishing the regulatory structure of the new data protection authority, the ANPD; this decree also 'provides details on the appointment of members of the ANPD, as well as administrative and internal procedures for [the agency's] functioning.'[259] The ANPD in turn has actively engaged with its mission, not least by publishing in

252 Lei No 13.709 (n 218), art 41; see also Rodrigo Dias, 'Considerações sobre a Figura do Encarregado pelo Tratamento de Dados Pessoais na lei Geral de Proteção de Dados' (*Escola Superior de Advocacia da seccional Rio de Janeiro da Ordem dos Advogados do Brasil*, 2020) <http://esa.oabrj.org.br/consideracoes-sobre-figura-do-encarregado-pelo-tratamento-de-dados-pessoais-na-lei-geral-de-protecao-de-dados/> accessed 29 July 2020.

253 Lei No 13.709 (n 218), art 41.

254 Ibid, art 52; see also Erickson (n 251) 885.

255 Lei No 13.709 (n 218), art 52.

256 See, eg, Lei No 13.709 (n 218), art 52 (XI) § 4.

257 Lei No 13.709 (n 218), art 52(II).

258 GDPR (n 1), art 83; see also Perrone and Strassburger (n 223) 96.

259 'Brazil: President signs decree approving structure of data protection authority' (*DataGuidance*, 27 August 2020) <https://www.dataguidance.com/news/brazil-president-signs-decree-approving-structure-data-protection-authority> accessed 24 September 2021.

January 2021 its operating strategy for 2021–2023.[260] In July 2021, in anticipation of the entry into effect of its enforcement powers a month later, the ANPD issued regulations governing the imposition of sanctions under the LGPD after conducting public hearings.[261]

There have also been challenges to the new data privacy regime established by the LGPD, primarily emanating from the Executive. Most notably, President Bolsonaro in October 2019 issued an executive decree creating a Citizen Database (*Cadastro Base do Cidadão*) to 'consolidate and improve the information inside government about each citizen.'[262] Enacted seemingly without regard for the newly-minted LGPD, this decree has been heavily criticized as a threat to citizens' privacy.[263] Unsurprisingly, numerous Brazilian civil society actors have challenged its constitutionality before the Supreme Court of Brazil, including the Federal Counsel of the Brazilian Bar Association.[264] A similar measure which obliged telecom operators to share the personal data of more than 140 million mobile service users with the Brazilian Institute for Geography and Statistics was declared unconstitutional by the Brazilian Supreme Court in May 2020 on a number of grounds, including privacy and due process.[265]

---

260 'Brazil's Data Protection Law: A Brief Overview' (INPLP, 2 March 2021) <https://inplp.com/latest-news/article/brazils-data-protection-law-a-brief-overview/> accessed 24 September 2021.

261 'ANPD Publica Portaria Que Define os Procedimientos de Regulamentação da Autoridade' (*National Authority of Data Protection*, 9 July 2021) <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-portaria-que-define-os-procedimentos-de-regulamentacao-da-autoridade> accessed 9 July 2021; 'A ANPD informa que realizará audiência pública sobre norma de fiscalização' (*National Authority of Data Protection*, 2 July 2021) <https://www.gov.br/anpd/pt-br/assuntos/noticias/a-anpd-informa-que-realizara-audiencia-publica-sobre-a-norma-que-dispora-sobre-os-procedimentos-de-fiscalizacao-e-sancao-da-autoridade-no-dia-08-07-2021-de-10h-as-12h-e-de-14h-as-18h> accessed 7 July 2021.

262 'Cadastro Base do Cidadão' (Governo Digital, 29 April 2020) <https://www.gov.br/governodigital/pt-br/governanca-de-dados/cadastro-base-do-cidadao-cbc> accessed 24 September 2021 [translation by the authors].

263 Rafa Santos, 'Cadastro Base do Cidadão destoa da LGPD e divide especialistas' (Consultor Jurídico, 20 November 2019) <https://www.conjur.com.br/2019-nov-20/cadastro-base-cidadao-apresenta-dissonancias-lgpd> accessed 24 September 2021; see also 'O Cadastro Base do Cidadão' (*AARB*, 17 February 2020) <https://www.aarb.org.br/o-cadastro-base-do-cidadao-e-a-lgpd/> accessed 24 September 2021.

264 'Data Privacy Brasil Afirma que Cadastro Base do Cidadão fere "direito fundamental à proteção de dados"' (*Observatorio Privacidade*, 9 April 2021) <https://www.observatorioprivacidade.com.br/2021/04/09/data-privacy-brasil-afirma-que-cadastro-base-do-cidadao-fere-direito-fundamental-a-protecao-de-dados/> accessed 24 September 2021.

265 Laure Schertel Mendez and Clara Iglesias Keller, 'A New Milestone for Data Protection in Brazil' (*Internet Policy Review*, 13 May 2020) <https://policyreview.info/articles/news/new-milestone-data-protection-brazil/1471> accessed 24 September 2021; see also Supremo Tribunal

Challenges notwithstanding, the LGPD is undisputedly landmark legislation that alters the landscape of data protection in Latin America. It was clearly inspired by the GDPR, which it generally emulates in key respects. At the same time, numerous variations – on the duties of processors, for instance, as well as around the notification of breaches, the conduction of DPIAs, and the establishment of a supervising authority housed in the Executive – significantly alter the tenor of the law, giving it a distinctly more restrictive 'Brazilian flavor'.[266] While it shares a basic structure and guiding principles with its European counterpart, the LGPD leaves many of the regulatory details to the ANPD, which raises concerns about future implementation of key elements such as those relating to data portability and DPOs.[267] Although the ANDP recently has taken positive steps towards implementing the LGPD, challenges to the new regime remain.

4.3 Chile

Chile was among the first countries to enact a data protection regime in Latin America when the National Congress passed the Law for the Protection of Private Life in 1999.[268] Traditionally in Chile, the right to privacy was derived exclusively from Article 19(4) of the Constitution, which guarantees 'the respect and protection of private life and the honor of the person and his family'.[269] The mechanism for guaranteeing the exercise of Article 19(4) was the constitutional writ to protect all fundamental rights authorized by Art 20 of the Constitution.[270] This approach was modified significantly in 2018, however, when the Constitution was amended to expressly add personal data protection in Article 19(4) as a constitutional right.[271]

The first attempt to codify data protection *per se* came in 1993 when Chilean legislators considered a draft law for the 'protection of data of a personal

Federal, 'Ação Direta de Inconstitucionalidade ADI 6387' <http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165> accessed 22 July 2021.

266 Perrone and Strassburger (n 223) 98.

267 Ibid.

268 Law No 19628, Ley sobre Protección de la Vida Privada, Agosto 18, 1999, Diario Oficial [DO] (Chile) <https://www.leychile.cl/Navegar?idNorma=141599> accessed 24 Septe,ber 2021; see also Voss and Castets-Renard (n 94) 314.

269 Constitución Política de la República de Chile [CP] art 19(4) <https://www.constituteproject.org/constitution/Chile_2012.pdf> accessed 24 September 2021.

270 See ibid, art 20; see also Pablo Viollier, *El Estado de la Protección de Datos Personales en Chile* (2017) 7 (2017).

271 Pablo Contreras, 'El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena' (2020) 18 Estudios constitucionales 87–120.

character.'[272] At the time, they looked for inspiration to the laws of various European countries, including Spain, France, and England.[273] After six years of congressional debate, the current data protection law (Act No 19.628) was promulgated in August of 1999; it was, however, almost immediately considered 'insufficient' because it failed to adequately regulate third party (private) processing of personal data.[274] In particular, the 1999 Law did not create a data protection authority, regulate cross-border data transfer flows, or sufficiently protect consent; nor did it provide for remedies or effective sanctions for violations.[275]

Efforts from 1999 forward to modernize the Protection of Private Life (Data Protection) Law made little progress until 2017, when the government of President Michelle Bachelet sent a comprehensive reform bill to the Senate entitled 'Regulation of the protection and processing of personal data and creation of the Personal Data Protection Agency.'[276] Up to that point, the 1999 Law had been amended piecemeal, primarily to protect persons from discriminatory treatment by private companies, for example, in the employment, financial and commercial sectors.[277] In 2014, Bachelet's government conducted public consultations on a draft statute intended to help harmonize Chilean law with international standards on data protection, including EU Data Protection Directive 45/96 and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, among other comparative law sources.[278] The government's online description of its draft law adds that 'the text of the European Union Regulation [then] under study was also taken into account,' meaning the GDPR.[279] For reasons that are

272 See Law No 19628 (n 268).

273 Viollier (n 270), 8.

274 See Viollier (n 270) 7; see also Manuel Vergara, 'Chile: Comentarios Preliminares al Proyecto de Ley que Regula la Protección y Tratamiento de Datos Personales y Crea la Agencia de Protección de Datos Personales' (2017) 6 Rev Chil Derecho & Tecnol 135, 136.

275 See Viollier (n 270), 47; see also Vergara (n 274) 136.

276 Proyecto de Ley, iniciado en mensaje de S E la Presidenta de la República, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, Marzo 15, 2017 (Chile), <https://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=11144-07> accessed 24 September 2021.

277 Viollier (n 270) 18–19.

278 'Ante proyecto de Ley Protección de las Personas del Tratamiento de Datos Personales' (*Ministerio de Economía, Fomento y Turismo*, 2014) <http://www.participacionciudadana.economia.gob.cl/consultas-ciudadanas-virtuales/ante-proyecto-de-ley-proteccion-de-las-personas-del-tratamiento-de> accessed 24 September 2021; Org for Econ Coop & Dev [OECD], *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) <https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> accessed 24 September 2021; see also Voss and Castets-Renard (n 94) 317.

279 Ministerio de Economía, Fomento y Turismo (n 278).

unclear, this ambitious initiative never progressed past the consultation phase and was ultimately unsuccessful.[280]

What is certain is that the draft law President Bachelet presented to Congress in March 2017 reflected a different approach to reforming the Chile's data privacy regime than its defunct predecessor of 2014.[281] According to the President's introductory message in the bill, one objective of the reform proposed is to establish a 'modern and flexible' legal framework in line with 'international norms and standards' on the subject of the protection and processing of personal data.[282] Pointedly, however, the drafters of that message left out of their lengthy exposition any reference to the law of the European Union, preferring to anchor the reform's normative model primarily in the standards and recommendations of the OECD, a transatlantic club of countries dedicated in large part to economic development, of which Chile is a member.[283] It should also be highlighted that this legislation is configured as a series of amendments to the Protection of Private Life (Data Protection) Law of 1999, not a stand-alone omnibus law like the ones proposed in Argentina and enacted in Brazil. From December 2020 to May 2021, the Government sent no fewer than seven messages to the Chilean Congress urging approval of the pending proposed law.[284] However, as of July 2021, the Bachelet bill was still under consideration in the Senate.[285]

The absence of any express reference to the GDPR in the proposed legislative reform's introductory section is made all the more curious by the inclusion in the text of several of the Regulation's key elements. For example, Table C reflects how the draft law would create new rights for the data subject, including the rights to erasure and data portability. One can also see how it would similarly mandate data controllers and processors to report data breaches while strengthening sanctions in case of violations. That said, it is just as important to observe which

280 Viollier (n 270) 33 ('as happened with the public consultation process, although the modifications made to the preliminary draft were discussed, they were not made available either to those involved in the table, or to the public') (translated by the authors).

281 Proyecto de Ley (n 276); see also Vergara (n 274).

282 Proyecto de Ley (n 276) 5.

283 Ibid; see also 'Where: Global reach, OECD' (*Organisation for Economic & Co-operation and Development*) <https://www.oecd.org/about/members-and-partners/> accessed 11 August 2020.

284 See 'Boletín 11144-07' (*Senado República de Chile*, 2017) <http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=11144-07> accessed 31 May 2021.

285 See 'Boletín 11144-07' (*Senado República de Chile*, 2017) <http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=11144-07> accessed 17 July 2020. It is likely that this delay is due at least in part to the constitutional reform process underway in the country at the time of this writing. See 'Chile Constitution: Sweeping changes possible as independents win' (*BBC*, 17 May 2021) <https://www.bbc.com/news/world-latin-america-57142087> accessed 24 September 2021.

of the GDPR's key elements the Chilean Executive chose not to include in its proposal: for instance, Table C reveals how the bill would retain the underlying data protection law's more limited territorial scope and would forego impact assessments altogether. Let us now take a look at the treatment of the key elements in a bit more detail.

Though never mentioned expressly as a model or source of inspiration, the GDPR infuses several of the most important updates to be enacted through the legal reform process. While the drafters of the bill preferred not to give the current data protection law extraterritorial reach,[286] they did expand the scope of its provisions to cover all public or private persons or organizations 'responsible for data,' a new term defined to cover both controllers and processors.[287] Likewise, with respect to the rights of data subjects, the President's introduction to the bill confirms that the inclusion of the new right to data portability in Section 4 is in keeping with 'the latest regulatory trends,'[288] which surely encompass the GDPR. Like its counterpart in the EU Regulation, the new provision in the Chilean bill would ensure that data subjects can ask either for a copy of their personal data in a structured format or request the transfer of their personal data to another controller.[289]

In this same vein, Section 4 of the reform bill further sets out the rights to 'rectification, cancellation and opposition.'[290] Its drafters explain how the new right to 'cancellation,' which mandates the suppression of personal data under certain circumstances, should in particular operate to guarantee 'the so-called 'right to be forgotten' in relation to data produced as a consequence of any criminal, civil, administrative and disciplinary offenses.'[291] In other words, the inclusion of the article authorizing cancellation, which does not expressly mention the 'right to be forgotten', was nonetheless intended to emulate the corresponding provision of the GDPR in form and function.[292] Like in Europe, this approach was deemed necessary for Chile to balance the rights of individuals to reduce public access to damaging information with the right to access information in the public interest.[293]

Similarly, in keeping with the European model, the Chilean reform would reinforce the data protection law's reliance on consent as the primary ground for

286 Proyecto de Ley (n 276) § (1) (not modifying the territorial scope of the underlying law).
287 Proyecto de Ley (n 276) § (2)(b); see also Vergara (n 274), 145.
288 Proyecto de Ley (n 276) 7.
289 Ibid § (4).
290 Ibid.
291 Ibid 7.
292 See GDPR (n 1), art 17.
293 Proyecto de Ley (n 276) 7.

lawful processing. The bill's proposed Article 12 sets out the rules for what should constitute valid consent and how to withdraw it.[294] According to this provision, the subject can revoke his or her consent at any time without cause 'using similar or equivalent means to those employed for granting it.'[295] This phrasing, we believe, substantially meets the key element listed in Table C for withdrawing consent, even though it does not track the precise language of GDPR Art 7(3).

In similar fashion, the bill imposes greater duties for compliance on those organizations deemed to be 'responsible for data,' which, as noted, means both controllers and processors.[296] Like GDPR Art 33 and 34, proposed Article 14 would require, on the one hand, that those 'responsible' give notice 'in the most expeditious way possible and without undue delay' to the Personal Data Protection Agency to be created when a data breach happens;[297] on the other, where the breach concerns 'sensitive data' or that pertaining to 'economic, financial, banking or commercial obligations,' it would also require the party responsible for the data to notify all affected persons in this same way.[298] Unlike the GDPR, however, the reformed law would not fix a deadline for making the required notifications (72 h), leaving it to the regulator to determine what is reasonable under the stated standard.[299]

Not all key elements in the Chilean reform bill match those of the GDPR as closely as the foregoing. One example is the naming of data protection officers (DPOs). While the designation of a DPO is recognized as an important option for controllers and processors to have at their disposal as part of a suite of preventative measures, it is not mandatory.[300] This means that the decision to appoint an internal data privacy expert responsible for promoting and monitoring compliance with the law is left to the sole discretion of the controller or processor in charge of the database.[301]

Sanctions is another area in which certain aspects of the key element are incorporated but others are not. Unique to all the regimes we studied, the reform would introduce a novel three tier system – lesser, grave and very grave offenses – for imposing penalties on data controllers and processors that breach its provisions.[302] In this regard, it takes the GDPR's dual tier approach even

294 Proyecto de Ley (n 276) § (5).
295 Ibid.
296 Proyecto de Ley (n 276) § (2)(b).
297 Proyecto de Ley (n 276) § (5).
298 Ibid.
299 Compare GDPR (n 1), art 33(1), with Proyecto de Ley (n 276) § (5).
300 See Proyecto de Ley (n 276) § (10); see also Vergara (n 274) 146.
301 Vergara (n 274) 146.
302 Proyecto de Ley (n 276) § (5).

further.[303] According to proposed Article 39, the tier-three fines for the most serious offenses can reach a maximum of five thousand 'monthly tax units,' (*unidades tributarias mensuales* or *UTM*) which equals approximately USD $336,000.[304] This means that although drafters significantly increased the types and amounts of sanctions relative to the prior framework, they preferred to tie fines to monthly tax units and not company's revenues as the GDPR does, thus lessening the potential onus on larger multinational companies.[305]

In conclusion, the Chilean Executive's initiative to reform the Protection of Private Life (Data Protection) Law draws heavily from the innovations of the GDPR without ever referencing it directly. In this respect, the pending bill would add a series of novel articles to the existing law to expand coverage to processors, create new data subject rights, require notification of data breaches, and impose heavier sanctions on offenders following a tiered scale of breaches. However, several of the GDPR's key elements – mandatory DPOs and impact assessments, as well as extraterritorial scope, to name a few – are largely ignored or substantially modified.

4.4 Mexico

Mexico's approach to data privacy is unique in that it has adopted separate laws to govern private and public actors, respectively. The rules and regulations governing private enterprise are anchored in a law enacted in 2010 to this end,[306] while public authorities engaged in data processing at all levels of government are the subject of more recent legislation from 2017.[307] 'This differentiation is explained by the

303 Compare GDPR (n 1), art 33(1), with Proyecto de Ley (n 276) § (5).

304 Proyecto de Ley (n 276) § (5). The 'monthly tax unit' is an indexed unit of accounting updated monthly by the Internal Tax Service (Servicio de Impuestos Internos). In August 2020, the unit value was $ 52.213 Chilean pesos. See 'UTM – UTA – IPC 2021' (*Servicio de Impuestos Internos*) <https://www.sii.cl/valores_y_fechas/utm/utm2021.htm> accessed 8 May 2020. On 5 August 2020, one US Dollar equaled $ 775.54 Chilean Pesos according to Central Bank of Chile (Banco Central de Chile). See 'Tipos de Cambio' (*Banco Central de Chile*) https://si3.bcentral.cl/Bdemovil/BDE/IndicadoresDiarios accessed 8 May 2020.

305 Universidad de Chile et al, 'Diálogo 2: Proyecto de Ley que Regula la Protección y el Tratamiento de Datos Personales' (2019) 3 RDA 1, 30; Proyecto de Ley (n 276) § (5).

306 Ley Federal de Protección de Datos Personales en Posesión de los Particulares (2010) [LFPDPP], <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf> accessed 24 September 2021; see also Reglamento de la Ley Federal de Protección de Datos Personales in Posesión de los Particulares (2011) [Regulation of the LFPDPP], <http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf> accessed 24 September 2021.

307 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (2017) [LGPDPPSO] <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf> accessed 24 September 2021.

introduction into the [Mexican] legal system of [data protection] under the umbrella of the right to access public information, whose application referred to the public sector exclusively.'[308] This approach created a bifurcated framework for data privacy that introduces a level of complexity to the analysis not present in the other case studies. For instance, most overviews of Mexican data protection law for consumption outside the country focus on the former set of rules – those regulating private parties – which, it is worth noting, were 'clearly influenced' by EU Directive 95/46.[309]

In this study, however, we will focus on the data protection regime established by the later law directed at public authorities and entities because it was promulgated after the GDPR-centered reference date of 2016. This perspective will provide us with insight into the extent to which the more recent Mexican legislation incorporates the key elements of EU Regulation 2016/679. We will, where relevant, comment as well on the corresponding norms from the parallel regime under the 2010 law and its regulations. In addition, we will highlight a recent challenge to the country's constitutional and legislative data protection regime as it pertains to public entities.

Regardless of which data protection framework we are discussing, its foundation is the Mexican Constitution. Indeed, the country's singular approach to the topic can be understood as the outcome of a series of constitutional reforms. In 2007, Article 6 was amended to declare that 'information related to a person's private life and personal data shall be protected in the terms and with the exceptions provided by law,'[310] which at the time still only applied to the public sector. In 2009, a fundamental normative shift occurred when Mexican legislators amended Article 16 of the Constitution to recognize 'every person's right to protection of their personal data, to access, rectify, and cancel [said data], as well as to

308 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, *Comentada* (2018) 9, [translation by authors] <https://www.infoem.org.mx/es/contenido/iniciativas/biblioteca/ley-general-de-protecci%C3%B3n-de-datos-personales-en-posesi%C3%B3n-de> accessed 24 September 2021.

309 LGPDPPSO, *Comentada* (n 308), 11; See eg 'Mexico: Data Protection Laws and Regulations 2021' (*ICGL.com*, 6 July 2021) <https://iclg.com/practice-areas/data-protection-laws-and-regulations/mexico> accessed 24 September 2021; 'Mexico – Data Protection Overview' (*DataGuidance*) <https://www.dataguidance.com/notes/mexico-data-protection-overview> accessed 24 September 2021; GDPR matchup: Mexico's Federal Data Protection Law Held by Private Parties and its Regulations' (*iapp*, 8 June 2017) <https://iapp.org/news/a/gdpr-matchup-mexicos-federal-data-protection-law-held-by-private-parties-and-its-regulations/> accessed 24 September 2021.

310 Political Constitution of the United States of Mexico [Constitución Política de los Estados Unidos Mexicanos], Art 6 <http://www.ordenjuridico.gob.mx/Constitucion/cn16.pdf> accessed 24 September 2021 [translation by authors].

manifest their opposition' to its processing (the ARCO rights).[311] In so doing, they elevated the concept of data protection to the status of a constitutional norm to be protected in the private as well as the public sphere.[312] A third wave of relevant constitutional reform took place in 2014 dedicated to increasing transparency in government; this process was driven in large part by the 'need to establish uniform standards for data protection' throughout the country and create the authorities and procedures required to enforce those standards.[313]

The progressive constitutional reform just described ushered in a series of correlative congressional initiatives to modernize data privacy rights in Mexico. The first legislative brick laid in the wall of Mexican data protection law after 2009 was the Federal Law for the Protection of Personal Data in the Possession of Private Parties (*Ley Federal de Protección de Datos Personales en Posesión de los Particulares*).[314] Promulgated in 2010, the Private Sector Law, as we will call it for short, looked to protect users' privacy *vis à vis* private companies in line with international standards and EU Directive 95/46; it excluded public authorities from its scope because those were already regulated under the pre-existing regime of access to public information.[315] Notably, the 2010 Law set up the National Institute for Transparency, Access to Information and Personal Data Protection (INAI) to be the country's data protection authority.[316] The administration of then President Felipe Calderón subsequently issued in 2011 a detailed Regulation to implement the 2010 Law and reinforce its protections for personal data in the hands of the private sector.[317]

In the wake of the seminal constitutional reforms of 2009 and 2014, Mexican authorities took active measures to revise its data protection regime even further. Consequently, Congress approved in 2016 the General Law on Protection of Personal Data in Possession of Mandated Subjects (*Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*), which came into force in 2017.[318] 'The mandated subjects to which the Public Sector Law applies at the federal, state, and

311 Ibid, Art 16; see also (n 101) and accompanying text (describing the ARCO rights).

312 LGPDPPSO, *Comentada* (n 308) 11.

313 Ibid [translation by authors].

314 Ley Federal de Protección de Datos Personales en Posesión de los Particulares (2010) [LFPDPP] <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf> accessed 24 September 2021.

315 Olivia Andrea Mendoza Enríquez, 'Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México:desafíos y cumplimiento' (2018) 12 Rev IUS 267, 281; LFPDPP (2010) art 2.

316 LFPDPP (2010), art 38–39; César Cruz, Diego Acosta and Marcela Flores, 'Mexico', in Alan Charles Raul (ed), *The Privacy, Data Protection and Cybersecurity Law Review* (2019) 266–281, 267.

317 Mendoza Enríquez (n 315) 282; see also Reglamento de la Ley Federal (n 306).

318 Cruz, Acosta-Chin and Flores (n 316) 267.

municipal levels are any authority, entity, body and agency of the executive, legislative and judicial branches, autonomous [government] bodies, political parties, [public] trusts and public funds.'[319] Subsequently, Mexico acceded in 2018 to the Council of Europe's *Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data* as well as the 2001 Additional Protocol regarding supervisory authorities and transborder data flows.[320] It is clear from the foregoing that Mexico, in its own unique way, 'has followed, along with other Latin American countries, the international trend of ensuring the protection of personal data.'[321]

Be that all as it may, our goal here is not to map the entire panorama of Mexican data privacy law to date; rather, it is to trace the extent to which the main post-2016 legislative initiative – the Public Sector Law – embraced the key elements of the GDPR. We know that this Law grew out of the constitutional reform process just described, and that it was subject to 'clear influence of the elevated standards of protection adopted by the European Union, which strengthens the very foundations of [the Law's] construction and incorporates important innovations that invigorate the legitimate and proper processing of personal data.'[322] It remains to be seen which of those innovations translated into concrete changes in the data protection regime and what the impact of those changes has been.

This is because the 2017 Public Sector Law, while recognizing the GDPR's importance, is distinct in a number of important ways. For one, it reflects Mexico's dual track approach to regulating data privacy, which, for the reasons discussed already, is unique in the region: it differs from the comprehensive (omnibus) legal regimes traditionally deployed not only in Europe, but in Latin America as well.[323] This makes comparison with the GDPR challenging because, by definition, the

319 Adolfo Athié Cervantes, 'Mexico – Data Protection Overview' (*OneTrust Dataguidance*, December 2020) <https://www.dataguidance.com/notes/mexico-data-protection-overview> accessed 24 September 2021.

320 Estados Unidos Mexicanos. – Presidencia de la República, 'DECRETO Promulgatorio del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal' (2018) <https://www.dof.gob.mx/nota_detalle.php?codigo=5539473&fecha=28/09/2018> accessed 20 July 2020. See also Council of Europe, 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data', opened for signature 28 Jan, 1981, ETS No 108 (entered into force 10 January 1985) <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108> accessed 24 September 2021, and CoE, 'Additional Protocol to Convention 108' <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=181> accessed 24 September 2021.

321 Cervantes (n 318).

322 LGPDPPSO, *Comentada* (n 308) 12 (2018) [translated by authors].

323 Ibid 09 (2018). See also (n 92) and accompanying text; Tables B and C (Annex).

Public Sector Law governs only the conduct of 'mandated subjects,' that is, Mexican public authorities and entities.[324] Restricting our analysis to one sector reduces its impact somewhat. Thus, for example, our inquiry into whether or not the Law's territorial scope has been expanded to reach actors or activities beyond the country's borders is, for better or for worse, not applicable in this case given the nature of the 'mandated subjects.'

Imperfect as the exercise may be, it is still worth highlighting the other aspects of the Public Sector Law that do lend themselves to comparison with the GDPR. One can observe, for instance, that the Law applies to processors (*encargados*) as well as controllers (*responsables*), and imposes significant duties on the former.[325] Regarding the rights of data subjects, the Law introduces the right to data portability for the first time.[326] Article 57 grants data subjects the right to obtain a copy of their personal data in a structured and commonly used electronic format for their own use or for 'transfer (…) to another system.'[327] As was the case in other countries – Chile, for example – this norm was lifted directly from the text of what became the GDPR.[328]

In contrast, the other of the Regulation's innovations (and key element) in terms of data subject rights, the right to be forgotten [erasure], has not been as widely or wholly embraced. 'In [Mexico], the right to be forgotten only achieved implicit recognition in the regulation of the right to object to the processing of personal data by the [Public Sector Law].'[329] We saw similar approaches in Chile and Brazil.[330] An authoritative commentary to the Law stresses the substantial differences in legal, social and political context between Europe, on the one hand, and Latin America and especially Mexico, on the other, to explain why the 'misnamed right to be forgotten' has not taken root *per se* in the country.[331] To illustrate, consider the case from 2016 in which a Mexican court found that the national regulator, the INAI, had erroneously enforced a 'non-existent right to be forgotten' against Google Mexico,[332] which the regulator had argued was premised on the constitutional rights to cancel the holding and use of one's personal data by

324 See (n 319) and accompanying text.
325 LGPDPPSO (2017), art 3 (XV & XXVIII) & Title IV.
326 Ibid, art 57; Mendoza Enríquez (n 315) 284.
327 LGPDPPSO (2017), art 57.
328 LGPDPPSO, *Comentada* (n 308) 161–163 (2018).
329 Ibid 161.
330 See (n 231 and 292) and accompanying text.
331 LGPDPPSO, *Comentada* (n 308) 128, 126–130.
332 Ibid 124.

controllers, as well as to object to its processing.[333] While those rights contemplate a degree of control by the data subject over their personal information in terms of erasure, said rights will under certain circumstances be outweighed by countervailing values that require preserving access to information and freedom of expression in the public interest.[334]

The remaining key elements reflected in the 2017 Public Sector Law are likewise a hodge-podge of norms that nonetheless follow the GDPR model to a significant extent. So, for instance, while consent is affirmed to be a central pillar for lawful data processing in Articles 16 and 21, no express provision or procedure for withdrawing it other than those envisioned by the ARCO rights is included.[335] Significant as well is the fact that the Law allows for 'tacit' consent, which is 'when the privacy notice [explaining the data processing to occur] has been put at the disposal of the data subject [and] he or she does not express any disagreement with it.'[336] Tacit consent is expressly prohibited by the GDPR.[337] In other respects, the Law tracks the GDPR more closely. Thus, controllers are obliged to inform data subjects and the INAI 'without undue delay' of any breaches that 'significantly' affect the affected subjects' rights in terms similar to those fixed by the Regulation;[338] processors are in turn bound to report data breaches to the controllers.[339]

The correlation between the two sets of norms extends to the obligation to conduct data protection impact assessments and, with a Mexican twist, the designation of data protection officials, at least with respect to controllers. With respect to the first, the Public Sector Law adopts criteria substantially similar to those in the GDPR for triggering DPIAs: such assessments are required whenever controller processing involves sensitive or special data, the transfers of personal data, or otherwise poses a risk to the rights and freedoms of the persons affected

333 See '¡GANAMOS! TRIBUNAL ANULA RESOLUCIÓN DEL INAI SOBRE EL FALSO «DERECHO AL OLVIDO»' (*R3D*, 24 August 2016), <https://r3d.mx/2016/08/24/amparo-inai-derecho-olvido/> accessed 20 July 2020; Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (2017) (n 307), art 46 and 47.

334 LGPDPPSO, *Comentada* (n 308) 128–131.

335 See LGPDPPSO Obligados (2017), art 16, 21, 43–47, and Chapter II (Exercise of ARCO Rights). Interestingly, the language of the key element regarding withdrawal of consent, which should be 'as easy as giving it,' does seem to appear in Article 21 of the 2011 Regulation to the LFPDPP, which states that revocation of consent must be permitted 'at least through the same means as it was given.' Regulation to the LFPDPP (n 306), art 21 [translation by the authors].

336 LGPDPPSO (2017), art 21, 26.

337 Ibid; GDPR (n 1), art 7(1) and recital 32. 'Silence, pre-ticked boxes or inactivity should not […] constitute consent'.

338 Compare LGPDPPSO (2017), art 40 with GDPR (n 1), art 33(1), 34(1).

339 LGPDPPSO (2017), art 59(IV).

due to the nature of the data.[340] As regards the second, the Law follows the GDPR in function, if not form, with respect to a duty on controllers to designate a DPO. It obligates the public sector controllers to create an internal 'Transparency Committee' that is to operate as 'the maximum authority with respect to the protection of personal data.'[341] This Committee's primary function is internal and centered on directing the controller's efforts to implement and comply with the Law.[342] At the same time, the controllers are obligated to establish a public-facing 'Transparency Unit', whose primary role is to 'support and guide the data subject who requires it in relation to the exercise of their right to personal data protection'.[343] Together, these two mandated entities carry out the equivalent functions of the GDPR's data protection officers, whose designation is mandatory for public bodies.[344]

Confusingly, however, the Mexican Law allows for, but does not require, the naming of an actual 'data protection official' within the Transparency Unit whose job would be to operate as a 'special adviser on personal data for the management of data processing, the adoption of security measures, the handling of ARCO rights, etc'.[345] This means that although DPOs as a formal matter are optional under the Law, their functional equivalents – the Transparency Committee and Unit – are not. For that reason, we register it as meeting the corresponding key element as well.

Finally, the accountability regime set up by the Public Sector Law, though not fully comparable to that of the GDPR due to the variance in focus discussed, does, in our opinion, meet the criteria corresponding to the key elements of processor liability and enhanced sanctions. First, the Law establishes shared liability between the 'mandated subjects' (the controllers) and those put in charge of personal data processing (processors).[346] The latter can be held directly responsible for failures to comply with the obligations imposed by the Law and the controllers.[347] Second, the Law creates an entirely new system of sanctions that 'are independent of those civil, criminal or any other legal order that might derive from the same facts'.[348] Like that of the GDPR, it operates on two tiers: ordinary infractions, and those offenses 'considered grave for purposes of their administrative sanction'.[349]

---

340 Compare LGPDPPSO 74 with GDPR (n 1), art 35(1) & (3).
341 LGPDPPSO (2017), art 83.
342 Ibid, art 84.
343 Ibid, art 85(I).
344 See GDPR (n 1), art 37(1)(a), 38–39.
345 LGPDPPSO (2017), art 85; LGPDPPSO, *Comentada* (n 308) 276.
346 LGPDPPSO (2017), art 60; see also LGPDPPSO, *Comentada* (n 308) 433.
347 LGPDPPSO (2017), art 60.
348 Ibid, art 163–165.
349 Ibid, art 163.

Included among the grave offenses are any acts undermining the exercise of ARCO rights by data subjections.[350] Failure to comply with the orders of the INAI or other supervisory body can result in enforcement measures directed at the offending officials in their personal capacity; these officials can be required to pay fines determined according to a variable unit of measure.[351] In any event, said fines would not exceed $7000 USD. Inclusion of these measures is considered at once 'novel [and] of extreme transcendence' for the Mexican data protection regime.[352]

In April 2021, Mexico enacted new legislation that challenges the foundations of the Public Sector Law.[353] Intended as an anti-crime measure, the new law amending the Federal Telecommunications and Radiofusion Law mandates the creation of a centralized government database for all mobile telephone users, commonly referred to by its Spanish acronym, PANAUT (*Padrón Nacional de Usuarios de Telefonía Móvil*).[354] The database would compile the personal information of users, including not just their name, nationality, and national ID number, but also biometric data.[355] The PANAUT would be managed by the Federal Institute for Telecommunications (*Instituto Federal de Telecomunicaciones*), the IFT, a government agency.[356] Given that it seems to fly in the face of the Public

350 Ibid, art 163(I, II).

351 Ibid, art 152–154. The fines can be between 150 and 1500 times the Unidad de Medida y Actualización, or the Unit of Measure and Update, which can mean a maximum of $ 6.700 USD. The value of the Unit is annually set by the National Institute of Statistics and Geography (INEGI) and is used to quantify legal obligations. For 2021 the Unit value equals $ 89.62 Mexican Pesos. Source: 'UMA' (*inegi*) https://www.inegi.org.mx/temas/uma/ accessed 8 November 2020. By 5 August 2021, 1 US Dollar equals $ 19.89 Mexican Pesos according to the Mexican Bank. Source: 'Tipos de cambio diarios – (CF102)' (*Sistema de Informacion Economica*) <https://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?sector=6&accion=consultarCuadro&idCuadro=CF102&locale=es> accessed 8 May 2021.

352 LGPDPPSO, *Comentada* (n 308) 417–418.

353 Stephany Daphne Méndez Pérez, 'El Padron Nacional de Usuarios de Telefonía Móvil y su impacto en la protección de datos personales' (*IAPP*, 8 June 2021), <https://iapp.org/news/a/el-padron-nacional-de-usuarios-de-telefonia-movil-panaut-y-su-impacto-en-la-proteccion-de-datos-personales/> accessed 24 September 2021.

354 'Decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión' (*Diario Oficial De La Federación*, 1 April 2021), <https://dof.gob.mx/nota_detalle.php?codigo=5616165&fecha=16/04/2021> accessed 24 September 2021; 'Comunicación de El Senado, Senado aprueba, en lo general, crear Padrón Nacional de Usuarios de Telefonía Movil' (*Senado.gob.mx*, 13 April 2021), <http://comunicacion.senado.gob.mx/index.php/informacion/boletines/50696-senado-aprueba-en-lo-general-crear-padron-nacional-de-usuarios-de-telefonia-movil.html> accessed 24 September 2021.

355 'Decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión' (Diario Oficial De La Federación, 16 April 2021, Art 180 Ter, I–IV, <https://dof.gob.mx/nota_detalle.php?codigo=5616165&fecha=16/04/2021> accessed 24 September 2021.

356 Méndez Pérez, 'El Padron Nacional de Usuarios de Telefonía Móvil' (n 353).

Sector Law in several respects, this new legislation has been the object of multiple constitutional and legal challenges, not least by the INAI, Mexico's data protection authority, and the IFT itself.[357] Interestingly, in its complaint to the Supreme Court, the INAI drew comparisons between Mexico and the European Union where a similar law came into effect and was likewise challenged.[358] In June 2021, the Supreme Court suspended the implementation of the controversial new law at the request of the IFT for fiscal and constitutional reasons.[359]

In conclusion, Mexico's bifurcated data privacy regime presents unique challenges to understanding how the GDPR has influenced data protection law and practice in that country. But our review of the Public Sector Law confirms the notion that the Law's drafters were 'clearly influenced' by the GDPR (among others international standards in the field).[360] Nearly all of the Regulation's key elements are reflected, one way or another, in the multiple innovations embodied in the Law: the right to data portability; the duties to notify breaches, conduct DPIAs, and implement a robust internal data protection mechanism to function like a data protection officer on steroids; and the 'transcendent' new sanctions regime. These features all testify to that influence. And at least two of the missing key elements – territorial scope, revocation of consent – can be explained as casualties of the sectorial focus of the Public Sector Law.[361] The recent creation of the PANAUT and the serious challenge it poses to the integrity of this Law remain an ongoing – and as yet unresolved – legal saga. We now proceed to the final case study country,

357 Ibid see Foro Jurídico, 'INAI presentó ante la SCJN la demanda de acción de inconstitucionalidad contra el Panaut' (*Forojuridico.mx*, 14 May 2021), <https://forojuridico.mx/inai-presento-ante-la-scjn-la-demanda-de-accion-de-inconstitucionalidad-contra-el-panaut/> accessed 24 September 2021; see also Instituto Federal de Telecomunicaciones, *La Suprema Corte de Justicia de la Nación concede al Instituto Federal de Telecomunicaciones suspensión dentro la Controversia Constitucional 71/2021 promovida en contra del Padrón Nacional de Usuarios de Telefonía Móvil.* (Comunicado 55/2021), 15 June 2021, <http://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/la-suprema-corte-de-justicia-de-la-nacion-concede-al-instituto-federal-de-telecomunicaciones> accessed 24 September 2021.

358 'Demanda de Acción de Inconstitucionalidad' (INAI, 13 May 2021), 23–24 <https://home.inai.org.mx/wp-content/documentos/AccionesYControversias/Demanda_INAI_PANAUT.pdf> accessed 24 September 2021.

359 Instituto Federal de Telecomunicaciones (n 357); see also Nicolas Lucas, 'Suprema Corte concede al IFT una suspensión contra el Padrón Nacional de Usuarios de Telefonía Móvil' (*El Economista*, 15 June 2021), <https://www.eleconomista.com.mx/empresas/Suprema-Corte-concede-al-IFT-una-suspension-contra-el-Padron-Nacional-de-Usuarios-de-Telefonia-Movil-20210615-0030.html> accessed 24 September 2021.

360 See (n 322) and accompanying text.

361 See eg (n 335) and footnote text.

Uruguay, before turning our attention to the comparative analyses and concluding observations contained in 5.

4.5 Uruguay

Uruguay has forged a functional approach to data protection that takes European standards as its starting point. It is one of the few countries in the region that does not have a *habeas data* provision in its Constitution.[362] Despite this, the 1966 Constitution protects the right to privacy and intimacy in articles 7, 10 and 72.[363] It was not until 2008, however, that data protection and *habeas data* were first introduced to the Uruguayan legal framework with the approval of Personal Data Protection Law Nº 18.331 ('PDPL'), a comprehensive (omnibus) piece of legislation that regulates data processing in both the 'public and private spheres'.[364]

Uruguay deliberately followed the prevailing European framework as it sought to harmonize its regime with the EU's to the greatest extent possible.[365] The PDPL was modeled on EU Directive 95/46 and expressly motivated by the prospect of an adequacy determination, which became reality in 2012.[366] The 2008 Law established the Unit for the Regulation and Control of Personal Data (*Unidad Reguladora y de Control de Datos Personales*, also known as URCDP) and invested it with full supervisory powers over the data privacy regime.[367] The URCDP is set up as an autonomous part of the Executive Branch.[368] It is worth recalling that in 2013, Uruguay became the first country outside Europe to adhere to Convention 108 and the Additional Protocol regarding supervisory bodies and transborder data

362 Carlos Saltor, *La Protección de Datos Personales: Estudio Comparativo Europa-America con especial Énfasis de la Situación Argentina* (2013) 347.

363 Constitución de la República, art 7, 10, 72 (Uru), <https://www.constituteproject.org/constitution/Uruguay_2004.pdf?lang=en> accessed 24 September 2021; see also ibid 348.

364 Ley No 18331 de Protección de Datos Personales, Agosto 11, 2008, art 3 (Uru), <https://www.impo.com.uy/bases/leyes/18331-2008> accessed 24 September 2021.

365 Bradford (n 14), 150; José Vera, 'El Nuevo Reglamento Europeo de Protección de Datos (GDPR) en Uruguay' (*El Observador*, 4 May 2018), <https://www.elobservador.com.uy/nota/el-nuevo-reglamento-europeo-de-proteccion-de-datos-gdpr-en-uruguay-20185412140> accessed 24 September 2021.

366 Commission Decision 2012/484/EU [2012] OJ L 227/11, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32012D0484> accessed 24 September 2021.

367 Article 29 Data Protection Working Party, Opinion 6/2010 on the Level of Protection of Personal Data in the Eastern Republic of Uruguay 15 (2010), <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp177_en.pdf> accessed 24 September 2021.

368 Ibid.

flows.[369] Just as notable is the fact that in April 2021, the country ratified the 2018 Amending Protocol as well, becoming the first (and only) Latin American State party to Convention 108+.[370]

Uruguay holds the distinction of being the first Latin American country to reform its data protection laws expressly to make them conform to the newly enacted GDPR. In so doing, the Uruguayan authorities chose not to replace the PDPL with new legislation, but to amend it through a series of legislative acts. Thus, five months after the GDPR came into force in Europe, the Uruguayan Parliament approved Budget Act Nº 19.670 (15th October 2018), which included a number of specific amendments to the PDPL.[371] Deliberations in the chambers of Parliament left no doubt that these changes were being pursued expeditiously in order to integrate the 'good' parts of the GDPR while adapting them to local 're-alities.'[372] In addition, Regulations decreed in 2020 to implement the PDPL as amended by the Budget Law likewise recognize that the latter's reform took into account 'the most recent provisions and doctrines,' expressly referencing the GDPR among other European standards.[373] As it stands, these three legislative acts working together comprise Uruguay's data protection regime.

Not surprisingly, this legal regime accounts for many – though not all – of the GDPR key elements, including a new extraterritorial scope and increased duties on both controllers and processors. The reforms expanded the territorial scope of the Personal Data Protection Law in the same direction as the GDPR.[374] Before the reform, the PDPL applied exclusively to processing carried out inside the country's borders. Since 2018, Uruguayan law encompasses processing activities regardless of where they are conducted so long as the controllers' are offering of goods and services to the inhabitants of the country.[375] Regarding processors, Uruguay was ahead of the curve in subjecting them to regulation: the original PDPL of 2008

369 'Personal data protection: Uruguay becomes first non-European state to accede to "Convention 108"', (*Council of Europe*, 12 April 2013), <https://www.coe.int/en/web/portal/-/personal-data-protection-uruguay-becomes-first-non-european-state-to-accede-to-convention-108-> accessed 22 July 2020.

370 Ley No 19.948 de Aprobación Del Protocolo de Enmienda del Convenio para la Protección de las Personas con Respecto al Tratamiento de Datos Personales, suscrito en Estrasburgo, (2021), <https://www.impo.com.uy/bases/leyes/19948-2021> accessed 24 September 2021.

371 Ley No 19670 (n 177).

372 División Procesadora de Documentos Nº1564 de 2018, Cámara de Representantes (Uru), <http://www.diputados.gub.uy/wp-content/uploads/2018/05/VT-1564.pdf> accessed 24 September 2021.

373 Decreto No 64/020, Reglamentación de los Art 37 a 40 de la Ley 19.670 y Art 12 de la Ley 18.331, Referente a la Protección de Datos Personales, 17 February 2020 (Uru), <http://www.impo.com.uy/bases/decretos/64-2020> accessed 24 September 2021.

374 Ley No 19670 (n 177), art 37; see also Castagnola and Anza (n 179).

375 Ibid, art 37.

distinguished between those entities '[r]esponsible for the data and its processing' (*Responsable de la base de datos o del tratamiento*) and those '[i]n charge of processing' (*Encargado del tratamiento*),[376] and imposed duties on both.[377] And, just to underscore this fact, the 2018 amendments to the PDPL expressly affirmed that liability for breaches of its provisions extends to processors as well.[378]

In this same manner, most of the GDPR's key elements on the responsibilities of data controllers and processors have been updated in Uruguayan law to better align them with the European Regulation. The amendments broadened the responsibility of both controllers and processors by enacting additional proactive protection measures.[379] One of these measures is a new requirement that they conduct data protection impact assessments (DPIAs) under certain circumstances.[380] These arise whenever controllers or processors work with sensitive or specially protected data, and whenever they engage in personal profiling, target vulnerable groups, carry out big data processing or send the data to a non-adequate country.[381] Interestingly, the GDPR mandates DPIAs when processing 'is likely to result in a high risk to the rights and freedoms of natural persons,' taking into account the nature, scope, context and purposes of that processing.[382] In contrast, the Uruguayan regulation fixes a set of broad criteria that could effectively lower the bar for when DPIAs will be required.[383] In this sense, Uruguay sets its own standards and differentiates somewhat from the GDPR.

Furthermore, in its reform of the PDPL, Uruguay codified for the first time the duty to notify data breaches to the URCDP as well as the individuals affected.[384] While the 2018 Budget Law only set the obligation to notify data breaches 'immediately,' the 2020 Regulation went further by adopting the GDPR's 72 h time maximum time frame for effectuating notification.[385] Some Uruguayan commentators consider this to be the most significant change among the many

376 Ley No 18331 (n 364), art 4(H) & (K).

377 See, eg, Ley No 18331 (n 364), art 4(H) & (K); see also infra (n 396) and accompanying text.

378 Ley No 19670 (n 140), art 12.

379 Ley No 19670 (n 140), art 39.

380 Agencia de Acceso a la Información Pública & Unidad Reguladora y de Control de Datos Personales, (n 210) (expressly citing the GDPR as a source of inspiration).

381 Ley No 19670 (n 177), art 4 (E): Sensitive data: personal data that reveal racial and ethnic origin, political preferences, religious or moral convictions, union affiliation and information regarding health or sexual life. Ley No 19670 (n 177).

382 GDPR (n 1), art 35(1).

383 See Decreto No 64/020 (n 373), art 6.

384 Ley No 19670 (n 177), art 38.

385 Decreto No 64/020 (n 373), art 4.

introduced through the amendment process.[386] In the same vein, the reforms also imported the duty of all public entities and some private organizations to designate data protection officers, a mechanism that did not exist under the original PDPL regime.[387] According to the URCDP, DPOs under the new provision must have knowledge in human rights with a focus on data protection, as well as the controller or processor's core business.[388] The private entities subject to the duty to designate a DPO are those that have as their core business the treatment of sensitive personal information (health, sexual, political) or the management of large volumes of data.[389]

The foregoing testifies to the positive impact of the GDPR on Uruguay's reform of its data protection law. But equally relevant is what was not changed. The amended legal regime does not track the GDPR's key elements in three important respects. The first is that, despite the preeminence of consent as a pillar of personal data processing in the 2008 PDPL, the Uruguayan authorities did not see the need to add any language on how and when consent could be withdrawn.[390] Accordingly, it is not clear what mechanisms would be necessary or valid for a data subject to withdraw or cancel his or her consent to have their personal data processed by a controllers.[391] Second, the post-2018 reform process did not modify any of the key elements concerning the rights of the data subject, most importantly with respect to data portability. For reasons not entirely clear, this hallmark GDPR innovation recognized by every other case study country was not part of the normative harmonization process in Uruguay. One can speculate about how in a small country like Uruguay, where State agencies are the main controllers and processor of personal data, portability of said data may not be high on the list of priorities.[392] But it does seem nevertheless to be a curious omission in light of the context described.

---

386 M Da Silva and P Mesa, 'Sepa Cuáles son los Cambios Recientes en la Protección de los Datos Personales' (*El País*, 8 March 2020) <https://negocios.elpais.com.uy/sepa-son-cambios-recientes-proteccion-datos-personales.html> accessed 23 July 2020.

387 Ley No 19670 (n 177), art 40.

388 Unidad Reguladora y de Control de Datos Personales, Resolución No 32/020 (2020) <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-32020> accessed 24 September 2020.

389 Ley No 19670 (n 177), art 40.

390 See Ley No 18331 (n 364), art 4(c), 5, 8, 9, 11, 17, 18, 21, 23, and 25.

391 Decreto No 414/019, Reglamentacion de la Ley 18.331, Relativo a la Proteccion de Datos Personales, 31 August 2009 (Uru), art 5–6 <https://www.impo.com.uy/bases/decretos/414-2009> accessed 24 September 2021.

392 Until June 2020, Uruguay was, along with Venezuela, one of the only countries in the region that did not have adopted telephone number portability. This means that mobile phone users could not change from one provider to another without changing their telephone number. By

Third, and more in line with regional practice, is the absence of express reference to the right to be forgotten. As is the case in the other countries studied, the Uruguayan authorities did not feel the need to expand on the existing data subject rights already guaranteed under the local ARCO regime.[393] Thus, for example, the URCDP issued an opinion in 2016 affirming that the 'right to be forgotten can be considered as the projection of other rights, among others, (…) the right to deletion [*supresión*].'[394] This is defined as applying only where there is 'an error, falsehood or exclusion' in the personal data of the subject requesting it, which suggests that it would not reach as far as the European understanding of the right to be forgotten.[395]

Last but not least, there is the sanctions regime. On the one hand, as we saw already, processors have been liable for breaches of their duties since 2008 under the original Data Protection Law.[396] On the other hand, legislators made no other changes to the accountability provisions of that law, which established a tiered approach to sanctions based on degree of 'gravity, repetition, or recidivism' with respect to the offenses committed.[397] Among other penalties, potential fines were set at up to 500,000 'Indexed Units,' which in Uruguay refers to a unit of measure adjusted daily by inflation.[398] Under prevailing levels, this translates into a maximum fine of USD 57,220.[399] So, while penalties were not 'enhanced' as part of

mid-2020 the government of Luis Lacalle Pou approved the legal modification to allow mobile users to change their company while maintaining their phone number, although technical implementation among providers is still pending. Although tangentially related to data portability in GDPR terms, this distinct approach to the portability of personal data generally might help explain the absence of this key element in the country. See 'Ursec postergó llamado para administración de portabilidad numérica, tras recursos de tres empresas que fueron descalificadas' (*La Diaria*, 17 May 2021) <https://ladiaria.com.uy/politica/articulo/2021/5/ursec-postergo-llamado-para-administracion-de-portabilidad-numerica-tras-recursos-de-tres-empresas-que-fueron-descalificadas/> accessed 5 July; 'De "Arrendatarios" a Dueños del Número de Teléfono Celular' (*El Observador*, 25 January 2020) <https://www.elobservador.com.uy/nota/de-arrendatarios-a-duenos-del-numero-de-telefono-celular-202012420107> accessed 13 August 2020.

393 See Ley No 18331 (n 364), Chapter III (Rights of Data Subjects).

394 Ley No 18331 (n 364), art 13(E), 15.a; see also Unidad Reguladora y de Control de Datos Personales, 'Dictamen 17/2016' (2016), <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/dictamen-172016> accessed 24 September 2021.

395 Ibid. For discussion of Europe's 'right to be forgotten,' see (n 36–38) and accompanying text.

396 Ley No 18331 (n 364), art 35.

397 Ibid.

398 'Unidad Indexada' (*Instituto Nacional de Estadística*), <http://www.ine.gub.uy/ui-unidad-indexada> accessed 14 August 2020.

399 Ley No 18331 (n 364), art 35. The value of the Unit is set daily by the National Institute of Statistics (INE). On 5 August 2021 the Unit value equaled $5.00 Uruguayan Pesos. Source: 'Boletin Tecnico' (*ine*, 4 August 2021) <https://www.ine.gub.uy/documents/10181/30921/UI+Agosto+2021/

the data protection law reform, and thus we do not check that element's box in Table C, it must be recognized that an advanced accountability mechanism was already in place at the time of that reform and continues to this day.

In conclusion, Uruguayan data protection law tracks its European counterpart deliberately in many respects – extraterritorial scope, data breach notification, processor liability, to name a few – but not all. Some elements, notably data portability, were omitted; others, like those for DPIAs and DPOs, were modified to lower their respective thresholds. These differences can be attributed to modifications to the norms enacted by legislators to make them mesh better with local 'realities.' At the same time, we would be remiss if we did not point out that there are several other innovative GDPR elements not captured by our methodology that Uruguay has adopted, such as making privacy by design and by default obligatory.[400] Overall, the country – one of only two in the region with a recognized adequacy determination from the European Commission – continues to embrace European data protection standards, in particular the GDPR, even as it adapts them to its particular circumstances. Whether it does so sufficiently to warrant a new adequacy decision remains to be seen.

5 Observations and Conclusions

We began this Article by posing three overarching questions. The first asked what the panorama of data privacy legislation across Latin America looked like since the 2016 adoption of the GDPR. The second question explored how those countries in the region that moved first to reform or enact data privacy legislation in light of the GDPR have done so. And the third inquired as to the lessons to be learned from the Latin American experience based on our responses to the first o questions. By addressing each of these queries in turn, it has been our goal to shed light on the debate referenced in the Introduction surrounding the nature of the *de jure* dimension of the most recent 'Brussels Effect' in the region. The results of the quantitative and qualitative studies of data privacy legislation across Latin America in Parts II and III confirm that Europe's normative influence in the region has not only continued but deepened as well. Insofar as data protection is concerned, a substantial number of countries, including all of the most developed

8dfe2f0c-7921-40d1-980a-cc4fa3d7dbbf> accessed 8 May 2021. On 5 August 2021, 1 US Dollar equals $43.69 Uruguayan Pesos according to the Central Bank. Source: 'Cotizacion de monedas' (*Banco Central del Uruguay*) <https://www.bcu.gub.uy/Estadisticas-e-Indicadores/Paginas/Cotizaciones.aspx> accessed 5 August 2021.

400 Ley No 18331 (n 364), art 8 & 9.

ones in economic terms,[401] have indeed chosen to 'follow the leader;' that is, they have elected to emulate many key aspects of the EU's revamped regime under the GDPR by incorporating them into domestic law.

Indeed, the results of our panoramic survey of the region in Part II suggest that a 'third wave' of EU standards-driven legislative reform is still underway.[402] By the end of 2021, most countries in the region – 90% (18 of 20) by our count – had a general data protection law or were trying to enact one.[403] And of those jurisdictions possessing data protection laws prior to 2016, nearly 80% have since either approved or proposed substantive reforms to their legislation.[404] Three successfully updated their pre-existing legal regimes with new GDPR-inspired provisions (Costa Rica, Mexico, and Uruguay), while four others have considered or are still studying similarly inspired draft laws (Argentina, Colombia, Chile, and Paraguay).[405] In addition to updates it made in 2016, Costa Rica is currently in the process of debating a new draft law, which looks certain to be approved, [406] checking both boxes simultaneously. In addition, since 2016, Brazil, Ecuador and Panama have promulgated entirely new data protection laws for the first time; Brazil and Ecuador in particular provide clear examples within the 'third wave' cohort of the GDPR's *de jure* impact on domestic jurisdictions in Latin America.[407] That said, it is important to note that not all 'third wave' initiatives have taken the form of 'omnibus' laws, as the aforementioned three countries did, and as was primarily the case for the first two waves of reform that took place in the wake of Directive 96/45.[408] Uruguay and Chile, for example, have opted to enact or propose amendments to their original laws already in place.[409]

The panorama painted in Part II heralds the advent of a 'third wave' of reform after the approval of the GDPR in 2016; prior to 2016, it was EU Directive 95/46 that set the data privacy standards to follow in Latin America and the world.[410] Since 2016, with the GDPR firmly in place on the regulatory horizon, 16 of the 20 countries

401 The five biggest economies in Latin America by GDP by power purchasing parity (PPP) are Brazil, Argentina, Mexico, Colombia and Chile. International Monetary Fund, 'World Economic Outlook Database' (April 2020 Edition) <https://www.imf.org/external/pubs/ft/weo/2020/01/weodata/index.aspx> accessed 16 August 2020.

402 See (n 94–98) and accompanying text (discussing the three 'waves' of data protection legislation in Latin America).

403 See supra 3.1 and Table B.

404 See supra 3.1 and Table B.

405 See supra 3.1 and Table B.

406 See (n 185) and accompanying text.

407 See (n 135) and accompanying text; 4.1 (Brazil case study).

408 See (n 94–97) and accompanying text.

409 See supra 4.2 (Chile case study) and 4.4 (Uruguay case study).

410 See (n 4–6) and accompanying text.

surveyed adopted or debated new standards for data protection within their existing domestic legal framework, and in several cases enacted an entirely new law to that same end.[411] In the majority of those 'third wave' countries, the GDPR's influence is palpable, if not express, with few exceptions (eg Panama and El Salvador).[412] This wave can be further differentiated from the previous ones in at least one other respect. Several countries that already possessed a data protection law sought amendments or reforms to that law rather than enacting entirely new 'omnibus' legislation, which continued to be the preferred route for countries enacting data privacy legislation for the first time. Uruguay, Chile and Colombia are examples of the former group, while Brazil, Ecuador and Panama exemplify the latter. For the reasons we go into below, these trends are likely to continue and strengthen in the region.

The initiatives by most countries described in Parts II and III to align their law with the GDPR are part and parcel of a broader context of interrelationship between Europe and Latin America. The post-2016 trend of following the GDPR has been accompanied by Argentina and Mexico's adherence in parallel to Convention 108 and the Additional Protocol regarding supervisory authorities and transborder data flows.[413] Consequently, there are now three countries in the region – the other is Uruguay – that are parties to the first and only data protection treaty in effect and its additional protocol. In addition, Argentina has signed the Amending Protocol updating the treaty as Convention 108+, while Uruguay has ratified it; other countries look to follow suit.[414] All this testifies to the broad attraction that European approaches to data privacy regulation have on Latin American lawmakers. Another example of this connection is Chile's strong affinity for the OECD's data protection framework, which it chooses to emphasize as its primary reference in the ongoing reform process.[415]

Conversely, not all aspects of the GDPR or Europe's approach to data protection are equally popular in the region. This is especially true in relation to the mechanism for granting adequacy status to non-EU countries, which initiated under the EU Directive and continues under the GDPR.[416] Since 1995, only Argentina and Uruguay have received an adequacy determination from the European Commission, and maintaining that status has been a source of inspiration

411 Those 16 countries are Argentina, Brazil, Bolivia, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Guyana, Honduras, Panama, Paraguay, Mexico, Suriname, and Uruguay. See supra 3.1 and Table B.

412 See 3.1 and Table B.

413 See (n 207) and accompanying text.

414 See (n 192–194 and 206–208) and accompanying text.

415 See (n 278, 283) and accompanying text.

416 Directive 95/46/EC (n 6), art 25(2); GDPR (n 1), art 45(2).

for the legislative reform efforts since 2016 in both countries.[417] But, as far as we know, no other Latin American country has applied to obtain adequacy status, despite widespread admiration for European standards and the fact that two other countries – Japan and the United Kingdom – have recently achieved that recognition under the Regulation.[418] More and broader research into this issue is required. Our preliminary exploration of these topics, however, seems to support the novel proposition that the Europe's adequacy mechanism may not be the incentive for governments that some might think it is, at least in Latin America.[419] This is true even where most countries in the region are actively seeking to update their national data protection regimes in light of the GDPR.

The foregoing observations respond to the first question regarding what the panoramic overview of regional practice since 2016 shows us. To answer the other two queries – what have first-mover States done and what lessons can we derive overall from the research – we have to parse the particular practice of the four countries profiled in Part III's case studies. In this respect, a number of sub-queries suggest themselves: What key elements of the GDPR are most commonly reproduced? Which are not? What might explain the difference? What legislative strategies have they followed to enact or promote such changes? And are there any other patterns, trends or other observations worth highlighting out of a comparative evaluation of the case studies? Keeping in mind that we are describing 'a moving target,'[420] our initial set of observations in response to these queries are drawn largely from Table C, which summarizes the 'score' for each country studied in terms of GDPR key elements present in the legislation analyzed. At the same time, there are other important characteristics of the referenced laws or draft laws not reflected in Table C, including legislative history and context, that we draw upon from the case studies.

We have seen how the history and context of the countries studied allows us to frame the correlation between their respective legislative reforms and the GDPR's key elements in terms of influence.[421] By influence we mean the extent to which any correlation in key elements between the Regulation and the national legislation contrasted can be said to be due to the effect of the former on the latter. The

417 See supra 4 (Introduction) and 4.4 (Uruguay case study).

418 See eg Japan adequacy decision of 23 January 2019, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.076.01.0001.01.ENG&toc=OJ:L:2019:076:TOC> accessed 24 September 2021.

419 See Bradford (n 14), 262; see also Michael D Birnhack, 'The EU Data Protection Directive: An Engine of a Global Regime' (2008) 24 Comput L & Security Rev 508, 516.

420 See (n 16) and accompanying text.

421 See (n 199) and accompanying text.

case studies confirm how in every jurisdiction legislators were aware of the GDPR and its role as 'standards bearer;' in nearly all – Brazil, Mexico, and Uruguay – its role in shaping the national legislation reviewed was explicit or manifest.[422] In Chile, the EU Regulation's role was minimized: the introductory chapter of the Chilean draft law submitted by the Executive pointedly omits any direct reference to EU standards, much less the GDPR itself.[423] Yet even in that case, the GDPR's fingerprints appears repeatedly, as when Chile seeks to codify data portability, a hallmark innovation of the GDRP.[424]

Turning now to the review of the GDPR's key elements in Table C, there are a few that stand out due to their (near) ubiquity across the countries studied: data portability, data breach notification, the application of the data protection law to processors as well as controllers, and enhanced sanctions. Although assigned different labels by different regimes (eg *operadores* vs *encargados*), processors have been or would be made regulated subjects of the respective data protection laws in all the jurisdictions studied, most for the first time, and all have or would be held liable for failure to comply with the law. The duties imposed on processors, however, tend to vary from place to place; for instance, in Uruguay and Mexico, they are required to appoint DPOs, but not in Brazil or Chile.[425] One thing that is nearly uniform across the region is increased sanctions, although in no case do they rise to the level of those contemplated by the GDPR.[426] With the exception of Uruguay, which already had a strong sanctions regime in place, the other countries enacted or would enact a stricter penalties framework *vis à vis* its predecessor, though in some cases even those have been criticized for not going far enough.[427]

The two elements that most strongly correlate across jurisdictions are the right to data portability and the duty on controllers to report data breaches. The former in particular is a hallmark innovation of the GDPR regime; as such, it is a strong indicator of influence.[428] The consistent acceptance of data portability as a new right of users in every case study regime but one speaks to the transferability of the idea behind it (the exception, oddly enough, is Uruguay). The duty to notify breaches is similarly illustrative, even as it is rapidly becoming the global standard: witness its introduction into conventional international law in the

422 See 4.1, 4.3 and 4.4 (case studies for Brazil, Mexico and Uruguay).
423 See supra 4.2 (Chile case study).
424 See (n 288) and accompanying text.
425 See Table C.
426 Ibid. See also (n 80–82) and accompanying text.
427 See, eg, 4.4 (Brazil case study).
428 See (n 199) and accompanying text.

modernizing of Convention 108.[429] The laws examined in Brazil, Chile, Mexico and Uruguay all establish or would require the communication of personal data breaches to both the data protection authority and the affected users; those laws similarly establish or would dictate the minimal content of the reports to be notified (eg nature of incident, type of data compromised, and security measures taken).[430] Uruguay, which enjoys an adequacy decision from the European Commission, took the additional step of imitating the GDPR model even more closely by establishing a time limit of 72 h for reporting a breach.[431]

Another element that correlates strongly, though not always in the positive sense, is the right to erasure and 'the right to be forgotten.' On the one hand, the Latin American legal tradition reflected in the figure of *habeas data*, and the ARCO rights derived therefrom, provide fertile ground for the integration of these rights – in particular the right to erasure [*cancelar*] – across legal systems.[432] All of the laws studied purport to do so – either in the pre-existing regime or as part of the updates after 2016.[433] On the other hand, no State was willing to adopt explicitly the more expansive European concept of the 'right to be forgotten,' which was read into the rights to erasure and to object to processing by the European Court of Justice.[434] While the two concepts – erasure and RTBF – are closely related they are not exactly the same. The right to be forgotten is not so much a right in itself as an extension of the right to erasure that transforms it, in the view of Latin American critics, into a 'mechanism for censorship.'[435] All the countries studied enacted or proposed provisions codifying the right to erasure; at the same time, however, when addressing the RTBF dimension, legislators and commentators alike emphasized the importance of the countervailing rights to access information and freedom of expression 'in both its individual and social dimensions.'[436]

As noted already, this regional reluctance to import the full meaning of the right to erasure from the GDPR can be explained by the fact that there are aspects of Latin American law and culture that diverge from Europe's, specifically in terms of

429 Council of Europe, 'Modernizing of the Data Protection "Convention 108"' <https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet> accessed 16 August 2020.

430 See supra 4. See also Poder Ejecutivo Nacional, (n 135), art 20; Law N° 13.709, (n 230), art 48; Proyecto de Ley (n 276); LGPDPPSO (n 309), art 40; Ley No 19.670 (n 174), art 38.

431 See (n 385) and accompanying text.

432 See (n 84–92) and accompanying text.

433 See (n 84, 90) and accompanying text.

434 See (n 36–37) and accompanying text.

435 LGPDPPSO, Comentada (n 308) 128.

436 Ibid. See also 4 country case studies.

what is understood by the term 'right to be forgotten.'[437] The region has a long tradition of protecting freedom of expression and the right of access to information that collides with the broad application of the 'right to be forgotten' as defined in European law.[438] For example, the Special Rapporteur for Freedom of Expression of the Organization of American States (OAS) has categorically affirmed that Inter-American human rights law does not protect or recognize the so-called 'right to be forgotten' in the terms outlined by the CJEU in the *Costeja* case.[439] The Rapporteur has emphatically stated that '[p]eople [in Latin America] want to remember and not to forget'.[440] This is because, more so than in Europe, the Latin America political and legal context, shaped by its history, favors the right to truth and access to information in furtherance of the public interest as essential components of freedom of expression.[441]

Even when a key element is not universally shared – extraterritorial scope, say – much can be learned from examining how the States that implement it do so. Thus, for instance, the two countries that include an expansive jurisdiction over data protection activities (Brazil, and Uruguay) tie it to the purpose of offering or providing goods or services to person residing in their respective territories.[442] In this sense, the countries added the 'targeting criterion' which is one of the key provisions introduced by the GDPR to expand its territorial scope.[443] Another example is the designation of data protection officers. All the countries examined introduced the designation of DPOs into their domestic legal regimes in some form; most made it a requirement.[444] Even so, there are variances: Brazil requires it only for controllers, but not processors; Chile makes it optional for both, and Mexico reconfigured the concept by requiring 'Transparency Units' that would function in much the same way as a DPO in other contexts.[445]

These are the preliminary observations we have been able to identify on the basis of the studies conducted in 3 and 4. But there are other, methodological

437 See Daphne Keller, 'Europe's 'Right to Be Forgotten' in Latin America' in Agustina del Campo (ed), *Towards an Internet Free of Censorship II Perspectives in Latin America* (2017) 151–174, 155.
438 Ibid 174.
439 Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, *Standards for a free, open and inclusive Internet* (2017) 52 <http://www.oas.org/en/iachr/expression/docs/publications/INTERNET_2016_ENG.pdf> accessed 24 September 2021.
440 Ibid 53.
441 See, eg, LGPDPPSO, *Comentada* (n 308), 123.
442 See supra 4.1, 4.2 and 3.5 (case studies of Argentina Brazil and Uruguay).
443 See GDPR (n 1), art 3(2).
444 See Table C.
445 Ibid. See also 4.1, 4.2 and 4.3 (case studies for Brazil, Chile and Mexico).

questions we have had to grapple with that are worth surfacing here because they explain in more detail how the aforementioned observations were formulated. For example, with respect to the Brussels Effect itself, how do you go about measuring *de jure* influence generally, and of the GDPR in particular? How do you determine the extent of such impact where the parts of the legislative acts contrasted – much less the whole – do not always match up exactly? In the terms established by our methodology, the question posed would be this: how many key elements need to be 'present' in a law to support an affirmation of *de jure* effect? What form must those key elements take to find a match or correlation?

In our methodology, we took a functional approach. It rapidly became clear to us that whenever countries adopted key elements from the GDPR, they do not do so verbatim. Rather, national legislators consistently chose to adapt the language of the source provisions to their particular context, often leaving out details or adding new ones. So, on the one hand, a sanctions regime featuring revenues-based fines, one of the main enforcement innovations of the GDPR, is followed only partially by Brazil's law, despite the range of reforms of establishing or reinforcing penalties in other jurisdictions.[446] The same goes for data breach notification: although imported into all case study jurisdictions, only Argentina and Uruguay copied the 72 h timeframe into their law.[447] Others like Chile have left the meaning of giving notice 'without undue delay' to the regulatory process.[448] In other words, in these and many other instances, the substance or 'spirit' of the referenced GDPR provisions was followed, if not the 'letter' or text of the Regulation's provisions *per se*. We thus full credit to countries in such scenarios, emphasizing function over form in the application of our methodology to the legislative acts reviewed.

On the other hand, some States – most notably Chile and Mexico – chose different models when regulating data protection in their jurisdiction, which made it even more challenging to compare and contrast with the GDPR. Chile's comprehensive overhaul of its deficient data protection law through a series of detailed amendments referenced OECD standards rather than those of the GDPR.[449] Mexico built upon its bifurcated data privacy regime by adopting a detailed law focused exclusively on public sector data processing, which led to specialized frameworks, for example, for remedies. Regardless, in both cases, what

446 See Table C.
447 See (n 431) and accompanying text.
448 See (n 297) and accompanying text.
449 See (n 415) and accompanying text.

we saw were extreme examples of the principle that countries in the region have tended to adapt rather than copy key elements of the GDPR, shaping them to fit national realities and regulatory capacities. Depending on the country context and approach taken, this could result in higher-level norms with fewer details in some circumstances, as in Brazil, or more distinctive and extensive normative frameworks in others, like in Mexico. Here, again, we credited the substance and function of the norms, rather than the form they took.

Methodological challenges notwithstanding, we are confident in our finding of a post-2016 'active influence' on Latin American data protection law emanating from the GDPR.[450] We can, of course, point to express references to the GDPR as a primary source of inspiration or model made by legislators in Argentina, Colombia, Uruguay and Mexico.[451] In the case of Argentina and Brazil, the parallels in form as well as function between their respective legislation and the GDPR speak volumes: imitation is, after all, the greatest form of flattery. But it is one thing to highlight an obvious connection between two sets of norms, and quite another to try to map the degree of influence one has had on producing the other, if by influence we mean how one source contributed to or caused the second. We understand that our work in this respect only scratches the surface of understanding the evolution of data protection law in Latin America, not least because the legislative processes at issue are notoriously complex, and each country is a universe unto itself.

It is for these reasons that we developed the comparative law methodology employed in this Article to allow us to at least begin to address the challenges identified with some degree of rigor, logic and consistency. The case studies in Part III have, among other things, provided us with a lens into the practice of the States selected that complements the more quantitively-focused research analyzed in 3. By combining the two we are able to formulate the foregoing observations, such as they are, about the *de jure* influence of the GDPR in the region. Which leaves just the question of why: if, as we saw, achieving adequacy status does not seem to be the ultimate goal for most of the countries in the region, why then do their governments maintain the tradition of implementing or adapting European data protections standards like those in the GDPR? Even accepting we can trace an 'active' *de jure* influence in the way we purport to, this only begs the question of *why* it continues to transpire in the first place.

We think the answer to the question of why the GDPR has been as influential as it has includes at least the following dimensions, the least of which is related to

450 See Graham Greenleaf, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108' (2012) 2 Int'l Data Privacy L 68, 74.

451 See supra 4.1, 4.3 and 4.4 (case studies of Brazil, Mexico and Uruguay).

market forces. First, most Latin American countries are animated by constitutions that through *habeas data* and other provisions enshrine access to data, privacy and more recently, data protection, as fundamental rights.[452] Though it emanates from different sources and legal traditions, this perspective – indeed, philosophy – nonetheless dovetails seamlessly with Europe's tradition of treating data privacy protection in terms of human rights.[453] Uruguay's Data Protection Law most clearly reflects this synchronicity when it affirms unequivocally in Article 1, entitled 'Human Right,' that 'the right to the protection of personal data is inherent in the human person.'[454] Similarly, Mexico's constitution was amended in 2009 to recognize 'every person's right to protection of their personal data.'[455] This reality cannot come as a complete surprise given the historical ties between the two regions, and the fact that most Latin American legal systems were founded on European models.[456]

Second, Europe's regulatory innovations in the 1995 Directive and now the GDPR appeal to Latin American legislators precisely because they represent a rights-based approach to ensuring the effective protection of personal data in a globalized and highly interconnected world.[457] In other words, several features of the European model, if not the entire model itself, are widely considered the best formulation of data protection regulations currently available; these are truly 'concepts that have proved successful in [the] global marketplace of ideas.'[458] Data breach notification; data portability; processor liability; robust preventive measures such as DPIAs and DPOs; these are the GDPR innovations that sell it – individually and collectively – as a legal paradigm. They further represent a roster of normative innovations that other countries can pick and choose from as they adopt and adapt the European standards to their domestic legal regimes.

And, of course, there are market forces at play, but these are less dispositive relatively speaking than in other regions of the world. Such forces are often assumed to be the reason most countries follow the GDPR, and they certainly do have a role to play, even in Latin America, where the primary trading partners of

452 See (n 99–101) and accompanying text.

453 See Paul M Schwartz and Karl-Nikolaus Peifer, 'Transatlantic Data Privacy Law' (2017) 106 Geo LJ 115, 119; see also Paul M Schwarz and Daniel J Solove, 'Reconciling Personal Information in the United States and the European Union' (2014) 102 Calif L Rev 877.

454 Ley No 18331 (n 364), art 1.

455 See (n 311) and accompanying text.

456 Matthew C Mirow, Latin American law: a history of private law and institutions in Spanish America (1st ed, 2004) 108.

457 See (n 21) and accompanying text.

458 Schwartz (n 8) and accompanying text.

the countries we studied tended to be each other, the United States, and only occasionally, a European country.[459] It is certainly no coincidence that the largest economies in Latin America – Brazil, Argentina, and Mexico in particular – are active implementers of GDPR key elements. Argentina for the time being continues to enjoy its adequacy determination,[460] while Mexico and Brazil are thinking of pursuing their own.[461] But in terms of trade in goods and services, Europe figures barely at all among the top trade partners for each of these countries.[462] Although economic integration is referenced in general terms, the primary reason cited by most Latin American legislators and commentators for Europe's influence has been that its standards are the most modern and protective of personal data.[463] This perspective tends to confirm that history, tradition and sector-leading innovations are what most draw Latin American legislators to the GDPR when it comes time to update or reform their data protection laws.

459 In 2018, Argentina's major trading partner countries for exports were Brazil, United States, China, Chile and Vietnam, and for imports they were Brazil, China, United States, Germany and Paraguay; World Bank, 'Country Profiles: Argentina' (*World Integrated Trade Solutions*) <https://wits.worldbank.org/CountryProfile/en/Country/ARG/Year/LTST/TradeFlow/EXPIMP> accessed 24 September 2021. In 2018, Brazil's major trading partner countries for exports were China, United States, Argentina, Netherlands and Chile and for imports they were China, United States, Argentina, Germany and South Korea; World Bank, 'Country Profiles: Brazil' (*World Integrated Trade Solutions*) <https://wits.worldbank.org/CountryProfile/en/Country/BRA/Year/LTST/TradeFlow/EXPIMP> accessed 24 September 2021. Mexico's major trading partner countries for exports were United States, Canada, China and Germany, and for imports they were United States, China, Japan, Germany and South Korea. World Bank, 'Country Profiles: Mexico' (*World Integrated Trade Solutions*) <https://wits.worldbank.org/CountryProfile/en/Country/MEX/Year/LTST/TradeFlow/EXPIMP> accessed 24 September 2021.

460 List of 'adequate' countries as of July 2021: Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United Kingdom as providing adequate protection. See 'Adequacy Decisions' (*European Commission*) <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> accessed 8 July 2021.

461 See 'Interview with: Dr Francisco Javier Acuna Llamas' (*DataGuidance*) <https://www.dataguidance.com/opinion/interview-dr-francisco-javier-acu%C3%B1a-llamas-president-national-institute-transparency-access> accessed 24 September 2021; https://finance.yahoo.com/news/more-countries-seek-gdpr-adequacy-053224360.html.

462 See (n 459) and accompanying text.

463 See (n 223, 278, 321, 372) and accompanying text.

Annex

Table A: Select 'key' elements introduced by GDPR.

	General provisions	Rights of the data subject		Controller and processor				Governance and accountability	
	Scope of territorial application	Right to erasure ('right to be forgotten')	Right to data portability	Heightened standard for processing with consent	Notification of a personal data breach	Data Protection Impact Assessment (DPIA)	Designation of the Data Protection Officer (DPO)	Remedies & liability	Penalties
GDPR	– Art 3 (1) & (2) – Art 28	– Art 5(1)(d) – Art 17 – Art 19	– Art 20	– Arts 7(3)	– Art 33 – Art 34	– Art 35	– Art 37	– Art 82	– Art 58 – Art 83
Highlighted focus of selected elements	Extraterritorial application to businesses and organizations operating in EU Applies to processors of data as well as controllers	Right to accuracy and erasure as data principles Controllers must erase inaccurate, unnecessary, & unconsented to data without undue delay when requested by data subject ('right to be forgotten')	Right to receive data in 'structured, commonly used and machine-readable format,' and to transmit it to another data controller 'without hindrance'	Data subjects must be able to withdraw consent as easily as they give it	Data controllers must notify data breaches to the supervisory authorities and, in certain cases, the affected individuals, 'without undue delay,' and where feasible, not later than 72 h after becoming aware of the breach	Controllers must carry out DPIAs anytime their data processing is likely to result in 'high risk to rights and freedoms of persons.' – DPOs must at least 'monitor' the performance of any DPIA	Controllers and processor must designate DPOs when processing personal data 'on a large scale,' especially if they are public authorities and/or processing sensitive data	Individuals are guaranteed a range of administrative and legal remedies for 'material or non-material damage' suffered at the hands of data processors	Heavy fines are imposed for serious breaches of either data subject rights, among others, or of the duties of controllers and processors
Base indicator queries	– Does country's data privacy (DP) law apply extraterritorially? – Does it apply to processors as well as controllers?	– Is the 'right to be forgotten' *per se* protected in the DP law? – How is it defined?	– Is the right to data portability protected in the DP law? – How is it defined?	– Is a rule that withdrawal of consent must be as easy as giving it, recognized in the DP law?	– Does DP law require controllers to report data breaches? – If so, when and to whom?	– Does the law require DPIAs to be conducted for high-risk data processing? – If so, how?	– Does the DP law require controllers & processors to appoint a DPO? – if so, under what circumstances?	– Are processors liable for breaches of the DP law?	– Does the DP law impose enhanced penalties for serious breaches?

Table B: Review of data privacy regulation in Latin America in 2021.

Country	DP law identification & date of approval	Title of the DP law	DPA	Draft law or decree proposed after May 2016 (Y/N)	Approved changes to DP legal regime after May 2016 (Y/N)	Comments on GDPR influence
Argentina[a]	Act No 25.326 10.4.2000	Personal Data Protection Act	Y	Y March (2020) November (2020) December (2020)	N	In 2018, Argentina proposed a comprehensive draft law to update the omnibus law approved in 2000, with a view to maintaining the 'adequacy' of protections recognized by the European Union. The 2018 draft bill made express reference to the GDPR as the 'international standard' to emulate, and includes almost all the key elements from Table A. Despite this bill losing parliamentary status in 2020, a new proposed law was introduced in March of 2020. Two additional bills were presented in November and December of 2020 and remain in parliamentary debate. These three pending bills have the same general purpose of maintaining the 'adequacy' with the EU and seek to follow the GDPR standards.
Belize	N/A	N/A	N	N	N	Belize lacks a formal data privacy law. Privacy is recognized as a right in the Constitution, and some privacy protections are included in laws which regulate public and private entities that handle personal data.
Bolivia	N/A	N/A	N	Y November 2019[b] May 2019[b]	N	Bolivia is among the countries that currently lacks a comprehensive data protection framework. In 2018, legislators presented a bill seeking to enact the 'Personal Data Protection Law.' It included

Table B: (continued)

Country	DP law identification & date of approval	Title of the DP law	DPA	Draft law or decree proposed after May 2016 (Y/N)	Approved changes to DP legal regime after May 2016 (Y/N)	Comments on GDPR influence
						some GDPR key elements, such as the right to data portability and data breach notification requirements. The law would have created a DPA with the power to impose sanctions. In 2019, a similar draft bill was presented by Foundation Internet Bolivia.org. Neither was enacted but modified versions of the proposed laws may be considered if re-submitted and endorsed by the new legislature.
Brazil	Act No 13.709 14.8.2018	General Data Privacy Law	Y	Y	Y Link	In 2018 Brazil adopted a comprehensive data protection law, the *Lei Geral de Proteção de Dados Pessoais* (LGPD), for the first time; it was subsequently amended in 2019 to establish the DPA as part of the Executive Branch. The law resembles the GDPR in many important respects, *inter alia*, by having extraterritorial application, promoting stronger data subject rights, and adding a duty for notification of data breaches. However, it differs from European standards on other fronts. The LGPD went into effect in September 2020 due to the pandemic, while enforcement was slated to begin in August 2021.

Table B: (continued)

Country	DP law identification & date of approval	Title of the DP law	DPA	Draft law or decree proposed after May 2016 (Y/N)	Approved changes to DP legal regime after May 2016 (Y/N)	Comments on GDPR influence
Chile	Act No 19.628 8.28.1999	Privacy Law	N	Y Link	N	In 2017 Chile's Congress began consideration of a bill to update the 1999 personal data law and, *inter alia,* create a data protection authority. The proposed law contains some provisions that advance GDPR protections, such as the rights to erasure and data portability, as well as the duty to notify breaches. It ignores several others. The bill remains in parliamentary debate; in January 2021, President Sebastián Piñera submitted an urgent request to expedite the process. Notably, in 2018 Chile adopted Act No 21.096 to amend the Constitution to add data protection as a fundamental right with constitutional status.
Colombia	Act No (1581) 10.17.2012	Data Protection Law	Y	Y Link	N	Since 2016 the Colombian Congress has discussed various legislative proposals to modify the omnibus Data Protection Law of 2012, though none has yet succeeded. In their introductions, the bills referenced the GDPR as a source of guidance, which is not surprising given that Colombian data protection law is largely based on Europe's. The proposed reforms would have expanded the territorial scope and increased data processors responsibility by introducing duties to

Table B: (continued)

Country	DP law identification & date of approval	Title of the DP law	DPA	Draft law or decree proposed after May 2016 (Y/N)	Approved changes to DP legal regime after May 2016 (Y/N)	Comments on GDPR influence
						realize privacy by design, to prepare impact assessments reports, and establish DPOs. The Colombian DPA is actively enforcing its law against companies that do not comply, like WhatsApp.
Costa Rica	Act No (8968) 06.27.2011	Protection of Persons Subject to Personal Data Processing	Y	Y Link	Y Link	In July 2016, the Costa Rican DPA promulgated Executive Decree No 40008 to update the country's Data Protection Law by introducing several the GDPR's key elements into the legal regime, such as the right to be forgotten and extended liability regime for both controllers and processors. In January 2021, draft law N22.388 was introduced to provide a complete reform of the 2011 law, and is currently being debated by the Legislative Assembly. The bill expressly cites the GDPR as its guide to filling the gaps left by the 2011 Law. Among other things, the proposed law would modernize the country's regime of data subject rights and establish the Costa Rican DPA as an independent institution.
Ecuador	Official Register N.459 05.10.2021	Organic Law of Personal Data Protection	Y	N/A	N/A	In Ecuador, data protection is a fundamental constitutional right. In May 2021 Ecuador's National Assembly enacted its first DP law which specifically recognizes the GDPR's impact. It contains several of the Regulation's key elements.

Table B: (continued)

Country	DP law identification & date of approval	Title of the DP law	DPA	Draft law or decree proposed after May 2016 (Y/N)	Approved changes to DP legal regime after May 2016 (Y/N)	Comments on GDPR influence
						For example, it enshrines the rights to data portability, mandates DPIAs and the designation of DPOs, as well as the duty to report data breaches. It also regulates processors' liability for data breaches with enhanced penalties for serious offenses. The original draft included the right to be forgotten but it was eliminated in the approved bill.
El Salvador	N/A	N/A	N	Y Link[c]	N	Although El Salvador's Legislative Assembly approved a Data Protection Law in April of 2021, it was immediately vetoed by President Nayib Bukele. A 'National Digital authority' was also enacted by legislative decree to oversee implementation of the new law, and vetoed as well. Thus, El Salvador remains without a comprehensive data protection Law.
Guatemala	N/A	N/A	N	N	N	Guatemala recognizes a right to privacy for personal communications in its Constitution, which has been developed through rulings of the Constitutional Court. To date, however, there is no data privacy legal regime in place. Although several legislative projects for data protection have been presented to the Parliament, none of them have been approved.

Table B: (continued)

Country	DP law identification & date of approval	Title of the DP law	DPA	Draft law or decree proposed after May 2016 (Y/N)	Approved changes to DP legal regime after May 2016 (Y/N)	Comments on GDPR influence
Guyana	N/A	N/A	N	N/A	N	Guyana has no privacy or data protection law, although it has legislation specific to the financial sector. However, Prime Minister Mark Philips announced an impending data protection law and a request for draft proposals was published in November 2020.
Honduras	N/A	N/A	N	N	N	Honduras protects the right to intimacy and confidentiality of communications in its Constitution. Despite the absence of a specific law on data protection, the country does have a National Commissioner for Human Rights with authority to protect personal data. Furthermore, Honduras in 2015 added the writ of *habeas data* to its constitutional protections. That same year, a bill on personal data protection was introduced in the Honduran Senate that focused on the protection of ARCO Rights and a sanctions regime. Since 2018, Honduras has been debating legal reforms to enact a data privacy law in line with European standards.
Mexico	LFPDPPP 07.5.2010 LGPDPPSO 01.26.2017	Federal Law for Protection of Personal Data in Possession of Individuals	Y	Y	Y Link	In 2017, Mexico enacted the General Law on the Protection of Personal Data in the Possession of Obligated Subjects, which imposed data privacy duties on public authorities and entities that were not covered by the private actor-focused Federal

Table B: (continued)

Country	DP law identification & date of approval	Title of the DP law	DPA	Draft law or decree proposed after May 2016 (Y/N)	Approved changes to DP legal regime after May 2016 (Y/N)	Comments on GDPR influence
						Data Protection Law of 2010. The new law incorporates a number of GDPR key elements, including data portability, DPOs and DPIAs. In 2021, the Senate approved a controversial legal reform to create a central government database for mobile telephone users (PANAUT) of sensitive personal data. The Mexican Supreme Court is hearing numerous challenges to this initiative, not least for violating the Data Protection Law. The Court has suspended the collection of data under the new law due to the legal challenges filed against the initiative.
Nicaragua	Act No 787 03.21.2012	Protection of Personal Data Law	Y	N	N	Nicaragua protects the right to personal data and the *habeas data* action in its Constitution and Law on Protection of Personal Data (Act No 787) of 2012. No legislative proposals for updating the Law have been found. On January 2021, the telecommunication regulatory body (TELECOR) issued an administrative decree on cybercrime which may run counter to its Data Protection Law by granting police or the Public Ministry, subject to judicial approval, the authority to prompt disclosures of personal data within information systems.

Table B: (continued)

Country	DP law identification & date of approval	Title of the DP law	DPA	Draft law or decree proposed after May 2016 (Y/N)	Approved changes to DP legal regime after May 2016 (Y/N)	Comments on GDPR influence
Panama	Act No 81 03.26.2019	Protection of Personal Data Law	Y	Y	Y Link	Panama adopted its first data protection law in March 2019 soon after the GDPR came into force. The law came into effect in March 2021. However, it acknowledges few of the GDPR's innovations (the right to data portability being one) while omitting most of them. Instead, the new Panamanian data protection regime follows a more sectorial approach like the one prevalent in the United States.
Paraguay	Act No (1682) 12.28.2000	Law on Information of a Private Nature	N	Y Link	N	In May 2021, a comprehensive bill was proposed in the Paraguayan Congress to update the country's Data Protection Law across the board and bring it more into line international standards. It seeks to build on the progress made by a similar 2019 legal reform of personal data protections that was restricted to the specific context of financial and credit information. The recent proposed legislation is also modelled on the GDPR and seeks to create a single independent DPA, as well as create a right to data portability.
Peru	Act No 29.733 07.3.2011	Protection of Personal Data Law	Y	N	N	The Regulatory Decree that implements Peru's 2011 Protection of Personal Data Law was modified in 2017 to strengthen the regime by giving more independence to the DPA and increasing the severity of sanctions. In December 2020, the DPA

Table B: (continued)

Country	DP law identification & date of approval	Title of the DP law	DPA	Draft law or decree proposed after May 2016 (Y/N)	Approved changes to DP legal regime after May 2016 (Y/N)	Comments on GDPR influence
						approved an additional resolution adopting a method of calculating sanctions for violations of the Data Protection Law.
Suriname	N/A	N/A	N	Y Link	N	The right of privacy has constitutional status in Suriname despite the lack of a comprehensive data protection law. In May 2018, legislators proposed the Privacy and Data Protection Law, which would fit the bill. The proposed legislation does not refer explicitly to the GDPR, but it does recognize the need to harmonize with international standards and includes several of the Regulation's key elements, such as extraterritorial application, the right of erasure, data portability, and the duty to notify breaches, among others. It is uncertain whether the bill will be enacted.
Uruguay[a]	Act No 18.331 09.11.2008 Act No 19.670 10.15.2018	Law on the Protection of Personal Data and the Right to Habeas Data	Y	Y	Y Link	In 2018, Uruguay approved changes to its 2008 Law to introduce GDPR key elements. Among these are the notification of data breaches, the duty to carry out impact assessments, and the designation of data protection officers under certain circumstances. The legislature opted not to include other key elements such as the right to be forgotten, the right to data portability or a

Table B: (continued)

Country	DP law identification & date of approval	Title of the DP law	DPA	Draft law or decree proposed after May 2016 (Y/N)	Approved changes to DP legal regime after May 2016 (Y/N)	Comments on GDPR influence
						tougher sanctions regime. In February 2020, however, the Executive enacted Decree 64/020 regulating certain aspects of the law relating to data protection officers and impact assessments; it further reinforced the liability of entities that treat personal data.
Venezuela	N/A	N/A	N	N	N	The Venezuelan Constitution contains various provisions protecting privacy, which can be enforced directly through the courts. However, Venezuela lacks a data protection law and a data protection authority, with early efforts to create a data protection law ceasing after 2005.

[a]Recognized by the European Commission to have 'adequate protection' with regard to automated processing of personal data under EU Directive 95/46. [b]On file with Authors. [c]The approved law (later vetoed) was never published, the only draft available is the 2019 Draft Law.

Table C: GDPR key elements as indicators of influence in Latin America 2021.

	General provisions		Rights of the data subject		Controller & processor				Governance & accountability	
	Does country's data privacy (DP) law or proposed law apply extraterritorially?	Does or would it apply to processors as well as controllers?	Is the right to forgotten protected in the DP law or proposed law?	Is the right to data portability protected in the DP law or proposed law?	Is a rule that withdrawal of consent must be as easy as giving it, recognized in the DP law or proposed law?	Does DP law or proposed law require controllers to report data breaches?	Does the current or proposed law require DPIAs to be conducted for high-risk data processing?	Does the current or proposed law require that controllers and processors appoint a DPO?	Are processors liable under the relevant norms for breaches of the DP law?	Does the DP law or proposed law impose enhanced penalties for serious breaches?
Brazil Act No 13. 709/19	Yes, Art 3.	Yes, arts 5 (VI & VII) & 37.	Unlikely, arts 16 & 18 (VI).	Yes, Art 18 (V & IX Section 7).	No	Partially, Art 48 (only in cases of risk or harm to users).	No, arts 4 (IV Section 3) & 32 (national authority may request DPIAs)	Partially, Art 41 (controllers only).	Yes, arts 52.	Partially, Art 52 (one category of breach; fines based on domestic revenues).
Chile Proyecto de Ley PTDP	No	Yes, Section (2)(b).	Unlikely, Section 4; President's Introductory Message.	Yes, Section 4.	Substantially yes, Section 5.	Yes, Section 5.	No	No (Section 10 makes DPOs optional for controllers and processors).	Yes, Section 10.	Yes, Section 10 (three categories of breach, fines increased).

Table C: (continued)

	General provisions		Rights of the data subject		Controller & processor				Governance & accountability	
	Does country's data privacy (DP) law or proposed law apply extraterritorially?	Does or would it apply to processors as well as controllers?	Is the right to forgotten protected in the DP law or proposed law?	Is the right to data portability protected in the DP law or proposed law?	Is a rule that withdrawal of consent must be as easy as giving it, recognized in the DP law or proposed law?	Does DP law or proposed law require controllers to report data breaches?	Does the current or proposed law require DPIAs to be conducted for high-risk data processing?	Does the current or proposed law require that controllers and processors appoint a DPO?	Are processors liable under the relevant norms for breaches of the DP law?	Does the DP law or proposed law impose enhanced penalties for serious breaches?
Mexico LGPDPPSO	N/A	Yes, Art 3 (XV & XXVIII); title IV.	Unlikely, Art 46.	Yes, Art 57.	No	Yes, Art 40.	Yes, arts 74 to 79.	Partially, arts 83–85 (public controllers only).	Yes, Art 60.	Yes, arts 163–165 (two tiers, fines introduced).
Uruguay Act No 18. 331	Yes, Art 37 of Act No 19.670.	Yes, arts 4 & 12.	Unlikely, although DPA affirms it falls within right to deletion.	No	Unlikely, art 13 E.	Yes, Art 38 of Act No 19.670.	Yes, Art 12.	Yes, Art 40 of Act No 19.670.	Yes, Art 12.	No enhanced penalties.

Bionotes

Arturo J Carrillo
The George Washington University Law School, Washington, DC, USA
acarrillo@law.gwu.edu
https://orcid.org/0000-0002-7509-0077

Arturo J Carrillo, Clinical Professor of Law; Director, Civil and Human Rights Law Clinic; Co-director, Global Internet Freedom Project, George Washington University Law School.

Matías Jackson
Facultad de Derecho, Universidad de la Republica Uruguay, Montevideo, Uruguay

Matías Jackson, LLM in Intellectual Property Law, George Washington University Law School; Fulbright Postgraduate Student. We are grateful to Daniel Solove, Eduardo Bertoni, Lia Hernández, Miguel Morachimo and Abdias Zambrano for their comments. This article would not have been possible without the inspired research assistance of GW Law students Elisa Cardano Pérez, Matías Joel Joseph, and Yirong Mao.