Empirical Research of the Data Protection Culture and the National Authorities' Role in Latin America

Alexandre Veronese
University of Brasília
veronese@ccom.unb.br

Alessandra Silveira
University of Minho
asilveira@direito.uminho.pt

Amanda Braga Ferreira
University of Brasilia
amandaaabrf@gmail.com

Amanda N. L. E. Lemos
University of Brasília and University of Minho
amandaespineira@ccom.unb.br

Eduarda Costa Almeida
University of Brasília
itseduardacosta@gmail.com

Luiza Mendonça **da S. B. Santos**
University of Brasília
luiza.mendonca.s@hotmail.com

Luiza Peixoto Veiga
University of Brasília
luiza.pveiga@hotmail.com

Marcio Iorio Aranha
University of Brasília
iorio@ccom.unb.br

Rebecca Lemos Igreja
University of Brasília
rebecca.igreja@gmail.com

Thiago Guimarães Moraes
University of Brasília and Vrije Universiteit Brussel
moraes.t@gmail.com

Mariana Moutinho Fonseca
University of Brasília
mariana-moutinho@hotmail.com

Vitória Bragança Sernégio
University of Brasília
vitoriabsernegio@gmail.com

BIOGRAPHIES

Alexandre Veronese - Professor at the University of Brasília (UnB). Alessandra Silveira - Professor at the University of Minho. Amanda Braga - GETEL/UnB. Amanda Espiñeira. Lemos is a Ph.D. candidate at the UnB and the University of Minho. Eduarda Costa Almeida - GETEL/UnB. Luiza Mendonça Santos - GETEL/UnB. Luiza Peixoto Veiga is a master's candidate for the UnB. Mariana Moutinho Fonseca - GETEL/UnB. Marcio Iorio Aranha - Professor at the UnB. Rebecca Lemos Igreja - Professor of UnB. Thiago Guimarães Moraes is a Ph.D. candidate at the UnB and the Vrije Universiteit Brussel. Vitória Bragança Sernégio - GETEL/UnB.

STRUCTURED ABSTRACT

[Purpose] The paper compares Latin American cultural concepts of privacy and personal data protection. It draws data from fieldwork research that targets nine countries in the region: Argentina, Brazil, Chile, Colombia, Costa Rica, Mexico, Panama, Peru, and Uruguay. The FAPESP (São Paulo Research Foundation) funded the original project: "Documentary and Field Research Project on Data Protection Authorities in Latin America: The Social and Institutional Concept of Privacy and Personal Data Protection."

[Methodology/approach/design] The research uses a qualitative approach. Firstly, the team classified and compared all the countries' national statutes. The team then read and analyzed all literature and documents concerning the targeted countries regarding personal data protection, privacy, and related subjects. In a secondary moment, the team classified and compared all the countries' national statutes; the team classified and compared all the countries' national statutes, and the team made fieldwork trips to all the countries to produce primary data from interviews with local authorities and academic and civil society representatives.

[Findings] The interviews led the team to conclude that privacy and personal data protection are global concepts. Notwithstanding, the nationals' descriptions show how they relate to international, national, regional, and local cultural discourses. Also, the local institutions have been essential in defining how a country will create and enforce those rights. The data classification lets us perceive the various mutual influences in a comprehensive analysis. The local players' role reflects those issues and underlines existing influences from some countries in others and world influences as well.

[Practical implications] The coexistence of global, national, and local narratives is clarifying. The expansion of digitalization and new information and communication technologies are changing the social understanding of privacy and personal data protection. Seeing how Latin American countries introduce global concepts into national statutes and enforce them allows the possibility of comparing. It makes it feasible to understand how local and international cultural trends relate to themselves.

[Originality/value] This research is entirely new. Never has a team gone to do fieldwork and deep interviews with so many stakeholders on a regional level. This paper summarizes data from dozens of reading materials and interviews. Thus, it enriches Latin America's privacy and personal data protection debate. It brings new information about the Latin American reality within a theoretical framework through an innovative perspective.

KEYWORDS

Personal data protection cultures. Latin America. Enforcement. Comparative analysis. Fieldwork research.

INTRODUCTION

This article addresses conclusions derived from field research, including interviews with authorities, academics, and representatives from civil society, as well as from bibliographic, documentary, and comparative legislative analyses of the Documentary and Field Research Project on Data Protection Authorities in Latin America: The Social and Institutional Concept of Privacy and Personal Data Protection, a project funded by the São Paulo Research Foundation (FAPESP/MCTIC 2018). The research focuses on how the national legal cultures of Latin American countries shape the notion of privacy and personal data protection. Since the beginning of the study, it is possible to verify that a strong influence of European Union (UE) law has been present, as Latin American legal tradition has a solid cultural interaction with European countries, especially Spain.

This work provides a broad review of the theoretical tools that enabled the analysis. Thus, it indicates that the concept of legal culture for privacy and personal data protection can only be understood by combining two perspectives.

The first pertains to facts and actions — taken from documents, interviews, reports, and other outputs — that underpin the sociocultural construction around the theme, eventually translating into a legal subculture. The foundational factors vary by country and may come from economic demands for integration into the global market or the struggle for legal modernization in some countries advocated by organized civil society. However, it is never the case that any of these factors operate in isolation. What unites all countries is the need to reach a minimum social consensus to enable legal changes and the creation of legal institutions. The EU and the OECD are considered two central international dissemination hubs. Eventually, it will also include the IberoAmerican Data Protection Network (RIPD), Mercosur, and the Council of Europe.

Besides this structural perspective, there is a second one that contemplates more specific social processes in a binary manner into mediations and relationships. Mediations constitute a process of local translation by different social groups of external and internal institutions, whether from the State, academia, or civil society. Relationships do not have this trend of translation. They are collaborative interactions without further conceptual transfers.

Unfortunately, it has not been possible to directly encompass in the research certain social groups that would undoubtedly have much to explain about the topic, such as digitally excluded or vulnerable populations.

The first section of this article focuses on identifying discursive elements that demonstrate the universality of the debate, particularly in their introduction and adaptation to national legal systems, whether from other countries or international bodies. Identifying such convergent elements indicates an interest of Latin American institutions in aligning with universal standards of legal and social modernity, mobilizing discourses on human and constitutional rights. In this section, there will be provided an explanation of how certain judicial cases have been fundamental in constructing these narratives and in internalizing some processual solutions like *habeas data*. It is also possible to include the integration of legal frameworks and social practices in line with other countries in the region and with international influences. Additionally, the goal is to identify narratives about beliefs, actions, and facts that highlight the need for special treatment concerning specific social groups. The right to personal data protection and privacy of teenagers and children is a recurrent one. Similarly, in some countries, other issues, such as women, indigenous people, and African descendants' rights, are also highlighted.

The second section compares discourses and narratives collected through the research about the influence of some countries' models and practices on others, specifically in the Latin American context. Naturally, the EU is constantly mentioned at some point there is also a focus on the Asia-Pacific Economic Cooperation (APEC). The third section deals with the difficulties in understanding the rights of interested parties in the surveyed countries. Some factors emerge as obstacles to developing the right to privacy and personal data protection, such as the digital divide and social unawareness. The fourth section focuses on the interactions and exchanges between different countries. It addresses the mutual influence of Latin American countries as an embryo of regional legal culture on personal data protection and the role of the RIPD in this process. Finally, the fifth section of this article is dedicated to two topics usually overseen by academic literature in this realm: the role of the RIPDand Mercosur.

CONTRAST OF SURVEYED COUNTRIES BY RELEVANT BELIEFS, FACTS, AND PROCEDURES FOR THE CONSTRUCTION OF THE CULTURE OF PERSONAL DATA PROTECTION AND PRIVACY

Law is a complex social construction involving a degree of social discourse. An isonomic understanding of the construction of rights involves, in part, awareness of a broad set of discourses emanating from a diverse range of actors (state officials, control authority employees, teachers, researchers, activists, and others). In this sense, a crosssectional analysis of these discourses shows how the rights to personal data protection and privacy in various sociocultural contexts simultaneously develop something potentially universal in discourses and practices. In different countries, the narratives concerning the legitimacy of these rights involve their recognition as human, constitutional, or fundamental rights.

Appreciating cultural phenomena — between the universal and the local — and their relationships among the various social actors is a vast, comprehensive challenge. One should consider the hypothesis that there is no national uniformity in this matter since discourses on rights always have various interpretations and understandings. It is essential to understand whether there is any dichotomy between importing legal models from the EU or its member states or observing neighboring countries' cultural practices and facts. These two ways of using external influences will become apparent and happen in most coutries. The construction of rights is dynamic and nourished by these evident paradoxes, as Table 1 summarizes. Quotes from the interviewees' discourses reveal that the construction of rights to personal data protection and privacy is not linear. It is a complex social formation involving various actors with diverse actions and beliefs.

Table 1. Possibilities of perceptions and expressions about personal data protection and privacy rights.

Scope	Positive application	Negative application
Universal	"These rights are universal."	"These rights stem from EU Law."
	"They are in international legal documents."	"We need to 'create' these rights to engage in international relations."

Local and national	"In my country, these rights are under protection in a specific manner."	"We are protecting these rights, as are other countries."
	"We differ from other countries regarding privacy and personal data management."	"We have deep relationships that lead to the national internalization of international legal rulings and norms."
	"In my country, some groups require special attention due to their social situation."	
Regional	"The exchange of information and experiences show that the law of my country is in harmony with others in our region."	"Our local peculiarities differ from those of other countries in the region."

(Source: authors' elaboration).

Some discourses about cultural universality, privacy, and personal data protection.

The first dilemma that arises from the analysis of various countries dealing with the agenda of personal data protection and the right to privacy is the establishment of a parallel between one or several cultural narratives of universal dimension and their local implementation. In interviews across various countries, there is a perceived narrative construction of the legitimacy of such rights because they are human, constitutional, or fundamental rights. These descriptions may present different logic, depending on the country. However, a striking feature is their pursuit of legitimacy, whether when enacting national statutes or advocating for establishing or strengthening data protection authorities.

Human, Constitutional, or Fundamental Rights as a Reflection of Universality

A distinguishing feature of Latin America is the constitutional and legal construction of *habeas data* to protect information, personal data, and privacy. A prime example is the case of Peru. In the 1993 Political Constitution, *habeas data* is in articles 200 and 202 (Peru, 2018). As explained in the interviews, it is a constitutional right of action that does not require the exhaustion of administrative remedies (Veronese, Silveira, Braga, Lemos, Almeida, Santos, Veiga, Fonseca, Aranha, Igreja, Moraes, and Sernégio. 2023a, 497). This explanation of habeas data as a remedy for fast and judicial access, as opposed to the use of administrative means, is apparent in the presentation in an interview with the data protection authority. The interviewee explained that this procedural avenue is related to the right to information and transparency while adding the right to personal data protection and informational selfdetermination (Veronese et al., 2023a, 530)

An interviewee from Peruvian civil society emphatically indicated that the origin of *habeas data* referred to access to information and transparency without defining the expansion of the instrument for personal data protection (Veronese et al. 2023a, 531). Another civil society member detailed that the habeas data action is filed in the first instance, with the possibility of appeal to a higher court and then, exceptionally, to the Constitutional Court itself. According to her, this procedural avenue was commonly used in Peru with the formation of constitutional jurisprudence on the subject, even between 2001 and 2012 (Veronese et al. 2023a, 455). In addition, an interviewee from the business sector indicated that there are two paths for the protection of personal data and privacy. The first one is habeas data, while the second path — in her terms — is the administrative route (Veronese et al. 2023a, 507).

An analysis of the t Constitutional Court of Peru precedents demonstrates a direct link between international legal documents and the resolution of habeas data application issues. In the Genaro Villegas Namuche case

(Extraordinary Appeal No. 2488-2002-HC-TC), the Court invoked the International Covenant on Civil and Political Rights of the
United Nations as well as the American Convention on Human Rights (Pact of San José, Costa Rica) of the Organization of American States in its paragraph 5 (Peru, 2002) to justify the need for adequate judicial protection of the right to information and, consequently, habeas corpus and habeas data. However, this interpretation could follow another path since, according to an interviewee from the Peruvian civil society, article 2.6 of the Political Constitution of 1993 establishes as a fundamental right the protection of personal information in computer systems (Veronese et al. 2023a, 454).

Regarding the interviewee's statement, it is evident that the mentioned period from 1993 to 2012 includes the *Vacatio*
Legis period of Statute No. 29,733/2011. This Statute explicitly mentions the regulation of article 2.6 of the Political Constitution (Peru, 2011). This point of view also comes from the opinion of an interviewee from civil society who assertively emphasizes constitutionalizing the right to personal data protection in Peru, even though it is not directly in the Political Constitution. However, this reasoning is logical since it verifies that Statute n. 29.733/2011 itself directly references the constitutional text, as explained by an interviewee from civil society (Veronese et al., 2023a, 454). It is worth remembering that the case resolved by the Constitutional Court of Peru, mentioned earlier, was from the year 2002, which would make the legal construction more complex (Peru, 2018).

It is a social and interpretative construction of the Law, as occurred in several other countries in the region, including Brazil, before Constitutional Amendment No. 115/2022. These narratives and facts demonstrate the attempts to construct social and legal discourses in favor of the universality of the rights to information, transparency, and, more recently, personal data protection in Peru. As much as the paths are different, it is possible to see the same meaning in discourses, actions, and facts in other countries in the region. The same cultural mediation dynamic is visible in Costa Rica. The Political Constitution of the Republic of Costa Rica of November 7, 1949, deals with the right to privacy in Article 24 and Article 28, as explained by a civil society respondent. Thus, although there is no express provision for personal data protection, the attempt to anchor this right at the constitutional level is clear (Veronese, Silveira, Braga, Lemos, Almeida, Santos, Veiga, Fonseca, Aranha, Igreja, Moraes, and Sernégio, 2023b, 858).

Moreover, once again, it is clear the path of postulating—at the national level—some constitutional anchor and its relationship with international law, in this case, the American Convention on Human Rights (Pact of San José, Costa Rica). This narrative and interpretative path also includes constructing procedural means of defense. Neither the Political Constitution of 1949 nor any subsequent amendment or statute created habeas data as a specific procedural means. According to a respondent from the data protection authority, although there is no regulation of habeas data, this expression is used by several people to refer to the Amparo resource, which is the correct procedural means to postulate the protection of personal data, based on Article 24 of the Constitution (Veronese *et al*. 2023b, 926). Despite the technical and specialized view that judicial action is not habeas data, it is evident that part of the social imagination uses this expression to refer to a right of action for the protection of personal data as explained by a respondent from the business sector (Veronese et al. 2023b, 875). Interestingly, she criticizes using the right to privacy as the basis for specific constitutional actions that would leave this strict scope towards individual control of personal data.

Colombia is another example of this practice. The constitutional text of Colombia dates from 1991. However, the respondents resort to articles 15 and 20 in their original wording to justify the right to personal data protection. Like the Political Constitution of Peru, Colombia's constitutional text has provided computer resources. It is noteworthy that the text directly alludes to the collection, processing, and circulation of data as explained by Nelson Remolina Angarita due to the work of the Preparatory Commission 0404 that anticipated the need to include the contemporary technological means at that time (Remolina Angarita 2015, 121). Moreover, in the commissions, the debate on habeas data was also constructed, as well as discussions about the foundations of the rights that should be recognized (Remolina Angarita, 2015, 125).

The Colombian constitutional text neither directly refers to habeas data as a specific procedural means. That was a legislative construction later regulated through Statute 1266 of 2008, explicitly referring to Articles 15 and 20 of the Constitution in its Article 1 (Cervantes Díaz, 2009; Colombia, 2008). This construction had evident practical effects since it allowed the action of protection as already described. Through this action, a channel was opened to review the sentences of the lower courts directly by the Constitutional Court, even in cases of habeas data, as explained by an academic respondent (Veronese et al., 2023b, 1040). Moreover, this construction has become more solid due to the separation between the right to privacy and personal data protection through a judicial

decision of the Constitutional Court, as explained by the respondent from the data protection authority (Veronese et al., 2023b, 991).

In turn, the Constitution of the Republic of Chile, dated 1980, expressly included the right to personal data protection in Article 19, paragraph 4, through a constitutional amendment in 2018. There are references to the topic in some academic texts, such as the studies by Carlos Reusser Monsálvez. The author notes that the Chilean Judiciary, as in other countries in the region, uses constitutional provisions to protect private life to address cases of personal data protection (2021, 145). He also emphasizes the lack of an explicit provision on the right to be forgotten (Contreras Vásquez, Bordachar Benoit, and Ortiz Mesías, 2022, 77).

Chile is a case with an express constitutional provision concerning the right to protect personal data without an administrative entity specifically dedicated to ensuring its effectiveness. This absence still allows the defense of this right in the Judiciary. However, one of the interviewees from civil society is skeptical about the interpretation that the Judiciary might give to this right to personal data protection since there would be no experience in the topic (Veronese et al., 2023b, 1213). This context of transformations has impacted the debates on creating a new constitution. It also allowed Chile to discuss the need to update Statute No. 19,628 of August 28, 1999, based on a bill from 2017 (Chile, 2022). It is important to note three essential points of the new statute under debate (Aparicio, 2022). The first is establishing an administrative authority to protect personal data and its institutional design. The second consists of internalizing the legal norms regulating international data transfers. Lastly, the third point is constructing a system of effectiveness, even regarding administrative and judicial actions.

The case of Brazil is like Panama. Both countries have recently developed specific legal frameworks for the protection of personal data (2018 in the case of Brazil and 2019 in the case of Panama). However, like in other countries in the region, the use of habeas data to address the topic is evident. Brazil was the first country in South America and the Caribbean to foresee this remedy in its 1988 Federal Constitution (Doneda 2006, 326). Also, as occurred in other investigated countries, more than this is necessary to guarantee personal data protection through judicial interpretation; the enactment of Statute No. 13,709/2018 and its quick modification was essential to create the National Data Protection Authority (ANPD). It is observed in Brazil that the right to personal data protection derives from the fundamental rights of personality and privacy protection. The most outstanding example is the joint trial of several Constitutional Lawsuits (6387, 6388, 6389, 6390, and 6393). This preliminary injunction, endorsed by the Plenary of the Supreme Federal Court, recognized the existence of the fundamental right to personal data protection before the promulgation of Constitutional Amendment No. 115/2022, which inserted it in Article 5 of the Federal Constitution in the following terms: "as a result of personality rights, respect for privacy and informational self-determination as states the article 2 (I) and (II) of the Federal Statute No. 13,709/2018 (General Statute for the Protection of Personal Data) as specific foundations of the discipline of personal data protection" (Brazil 2020). As the debate addressed the measure related to the approach to the global health crisis of COVID-19, the court also mentioned documents from the World Health Organization (WHO) to support its decision to declare Provisional Measure No. 954/2020 unconstitutional. Later, in 2022, the National Congress approved the mentioned Constitutional Amendment, and thus, the right to personal data protection acquired explicit character in the Brazilian constitutional text (Brazil, 2019).

The social process continues in the Argentine Republic. That country's Constitution is ancient, dating back to 1853. However, the constitutional text has been widely modified, especially in 1994. One of its modifications was the introduction in Article 43 § 3 that provided for habeas data under the general heading of the amparo action (Argentina, 1994). As Pablo Palazzi explains, this path toward habeas data was not straightforward since the Presidency vetoed Statute No. 24.475/1996, which had been approved by the National Congress (1998). Despite this, according to an interviewee from the academic field, this did not prevent its use by the Judiciary in favor of access to information (Veronese et al., 2023b, 1345). It is important to note that the autonomy of habeas data concerning the amparo trial was an essential process to expand the scope of this recourse in favor of protecting personal data, as Pablo Palazzi (1998) also explains. According to an interviewee from the Argentine government, the amparo trial would be like the *Mandado de Segurança* in Brazilian legislation (Veronese et al., 2023b, 1300). As observed in the third paragraph of article 43, habeas data in Argentina also reaches private databases.

Resorting to the Judiciary to protect personal data was a recurring practice in Argentina between 1994 and 2000 (Veronese et al., 2023b, 1275). Statute No. 25.326/2000, which deals with personal data protection, introduced a specific chapter on habeas data, resolving the initial dilemma. The process of constitutional interpretation obtained its first significant ruling during that period by the Supreme Court in the "Facundo Urteaga" case (Argentina, 1998). In this case, habeas data extends the right to privacy (Ruiz Martínez, 2015, 61). According to one of the interviewees, this case generated great social commotion (Veronese et al. 2023b, 1283). The Supreme

Court ended up allowing access to the personal data of a missing person, as requested by his brother. According to Marcela Basterra, this judicial case is also directly related to the debate on the right to the truth (Basterra, 2008a, 68). As can be observed from this author's opinion, the right to the protection of personal data is understood as a right of access to other fundamental rights, as explained by a respondent from civil society (Veronese et al., 2023b, 1407). A similar understanding comes from a government interviewee who considers that the right to protect personal data is an "intermediate right," that is, as a means to protect other fundamental rights (Veronese et al. 2023b, 1310). A curious fact is that Argentina was one of the countries in Latin America that took the longest to incorporate the right of access to public information. Its Access to Information Statute dated from 2016 (Statute No. 27,275). However, the matter was not in a legal vacuum since not only did the Constitution already contemplate rights related to the subject, but also because there was already an entity derived from Statute No. 25.326/2000 (NDPDP – National Directorate for Personal Data Protection) and Decree No. 1172/2003 (Veronese et al., 2023b, 1345). The advent of this new statute was important for combining administratively the system. Thus, this statute creates the Agency for Access to Public Information (AAIP) as an autonomous entity incorporating the NDPDP (Simão, Oms, and Torres, 2019, 12). Thus, the case of Argentina also demonstrates a construction interpretative and the influence of international elements for the construction of a concept—and local instruments—for the protection of personal data. One of the problems in the region is the balance between personal data protection and the constitutional duty of transparency, something mentioned in several countries, such as Chile, Panama, and Mexico, the latter analyzed next.

The interview with a Mexican authority points out this difficulty since, in 2000, there was a broad institutional reform on the issue of access to information, which, consequently, was intertwined with the issue of personal data protection and privacy. The managers had wondered: "What would be the status of citizens' information?" This answer would be the need to build a regulatory and institutional framework for protecting personal data and privacy, influenced by international sources, and define that the competence for the matter would be federal (Veronese et al. 2023a, 788). This initial framework gained a new dimension with the reform to the Political Constitution of the United Mexican States of 2009, which recognized the autonomy of the right to personal data protection concerning the right to access information (Parra Noriega 2011, 155). The regional influence, that is, from the Latin American debate, is evident when observing that the constitutional text foresees the so-called "ARCO rights" (access, rectification, cancellation, and opposition) (Veronese et al., 2023a, 630).

The international influence in the constitutional incorporation of the rights to personal data protection in Mexico is evident, and it is in line with an ongoing social process in the various countries of Latin America. Uruguay's path was somewhat different since these rights are not explicitly in the constitutional text of the Oriental Republic. The constitutional anchoring of these rights in that country is carried out by Article 72, which links them to the rights of personality (Uruguay, 1967).

According to the interviewees in this country, the essentiality of the right to personal data protection must also derive from international conventions incorporated into the national legal system. Like in other countries, it is usual to identify in the interview's references to the Universal Declaration of Human Rights of the United Nations as well as to the American Convention on Human Rights (Pact of San José, Costa Rica) as legal elements that would inform the essentiality of the rights to personal data protection as part of a broader legal set. The same occurs in the Republic of Panama, as didactically explained by the interpretative functioning to relate international law with local law (Veronese et al., 2023b, 1473).

Panamanian doctrine and the Judiciary derive the constitutional right to personal data protection from the right to privacy. Thus, it is possible to identify in the investigated countries the existence of a social and legal dynamic of the production of fundamental or constitutional rights, considering the national panoramas and their relationship with international law. This process is enjoyable as it demonstrates in evidence the actions and discourses of the interviewed actors in favor of universalizing the rights to personal data protection and privacy, either as human rights or as constitutional or fundamental rights of application. Nevertheless, the vision described in this subsection highlights a cultural production of internalization in local texts and narratives of various external elements. The following subsection will address a related topic. However, it will be more attentive to practices, mainly when referring to the need to modernize the legal structures of the countries.

Rights and National Practices as a Reflection of Global Western Legal Modernity

In the interviews, the narratives conveyed a sense of the need to insert the investigated countries into a paradigm of legal modernity. Thus, this subsection will focus on judicial or administrative cases and discourses, always

from the perspective of the countries' international and transnational insertion (participation in the conventions of the Council of Europe and the OECD, for example).

Peru provides a first example: an administrative decision from 2015 on the "right to be forgotten." The first question is whether it is related to the case resolved by the Court of Justice of the EU known as "Mario Costeja." As in several countries in the region, the "right to be forgotten" has aroused the population's curiosity and the legal world in general about personal data protection and privacy. However, the grounds of judicial and administrative decisions in Latin America that refer to this expression may differ significantly from those constructed in the EU. In the Peruvian case, Statute No. 29733/2011 does not expressly contemplate the right to be forgotten (de-indexation in the sense of the EU). However, it was not an obstacle for the National Directorate for Personal Data Protection of Peru to decide administratively on the topic, determining the de-indexation of links by Google (Borgioli, 2016). This fact is mentioned by a respondent from civil society ascrucial for giving visibility to the country's data protection authority in 2015 (Veronese et al. 2023a, 471). The respondent explicitly relates the case of Peru with the case of the EU. This case was critical because it demonstrated that the local authority could sanction a global company, just as it occurred in the EU.

The two Costa Rican cases are local, and have no international or regional influence. However, they also show the same sense that the application of sanctions serves, on the one hand, to make the problem visible, as well as to demonstrate that local authorities are in tune with the practices of other countries. The first case is known as UPAD (Presidential Data Analysis Unit), an agency directly attached to the Presidency of the Republic of Costa Rica. As explained by one of the respondents from civil society, the decree creating this administrative body was considered a game-changer in the Costa Rican debate (Veronese et al., 2023b, 838). As another respondent from civil society explains, in theory, this unit had been created to perform massive analyses of citizens' data to produce more efficient public policies (Veronese et al. 2023b, 820). However, it has generated much concern among the citizens. The Presidency of the Republic itself revoked the decree creating the UPAD. Still, various political groups, state authorities, and civil society entities have mobilized in this regard (Gómez, 2021a), even though a lawsuit on the case is still pending (Gómez, 2022).

The second one is the FARO case, in which the government collected personal data through a questionnaire delivered to children in periodic exams conducted in the country (Gómez, 2021b). A Costa Rican civil society respondent explained that they applied these tests to eleven-year-old students. However, some questions had no academic relevance and were questions of a socioeconomic nature. According to the respondents from civil society, these questions would have generated trauma in the children, which led to a feeling of indignation among the parents of the students (Veronese et al., 2023b, 841). The case of the FARO tests is another example of a problem that has affected Costa Rica, and that has to do with the protection of personal data and privacy. Curiously, both cases refer to State action, unlike the case against Google in Peru.

Legal modernization to support the protection of personal data has also advanced significantly through judicial and administrative decisions in Colombia. According to one of the interviewees from the entity, the day-to-day approach of the work of the data protection authority in that country concerns financial issues, such as evaluating loans (Veronese et al., 2023b, 982). Professor Rodrigo Ruiz states that the Colombian court, in the T-414/92 judgment, would have adopted a potent form of interpretation of financial data so that the right to privacy would protect them. Their availability would only be possible with the consent of the interested party. They must delete the negative record when the customer pays the debt (Ruiz 2011, 83). An academic interviewee talks about this understanding. He explains the consolidation — in the financial sector and commerce — of risk centers. The country uses them widely, and therefore, their judgments on citizens could generate direct harm to them (Veronese et al., 2023b, 1024).

The Constitutional Court of Colombia has established standards for the exposure or protection of individuals' data (Restrepo 2009, 53). Between 2008 and 2013, it produced a series of decisions in which it consolidated several understandings, among them the definition of a "right of free determination of digital information" in Judgment No. T-094/95 (Colombia 1995). In Judgment T-729 of 2002, the Constitutional Court reiterates this concept (Restrepo 2009, 47). In this sense, Betsy Yahanna Ruiz Ardila, in her monograph, considers that personal data protection combines several sources, among them the Constitutional Court and the Superintendence of Industry and Commerce (SIC) (2016: 33). The production of renewed legal concepts in a legal dialogue between the judiciary and the administrative authorities demonstrates Colombia's emphasis on the need to participate in a local process of legal modernization with a view beyond its borders.

The case of Chile is the most peculiar. The country has the oldest legislation in the region. s previously explained, Chile has no authority dedicated exclusively to protecting personal data. In practical terms, the Council for

Transparency has been the primary responsibility for the protection of data as well as access to public information. As noted in the last subsection, Chile is discussing the reformulation of its specific legislation, focusing on these topics. This discussion began in 2014, and the legislative project was presented in 2017 (where? to whom?) (Veronese et al., 2023b, 1187). According to the interviews, other international factors would justify the Chilean administrative and legal system update. The first is participation in APEC (Veronese et al., 2023b, 1165, 1246). As a respondent from civil society emphasizes, APEC would be less rigorous than the OECD or the EU itself (Veronese et al. 2023b, 1165).

Moreover, Chile is part of the DEPA – Digital Economy Partnership Agreement – which involves flexible personal data flows among its members (New Zealand, Chile, and Singapore) (Veronese et al., 2023b, 1193). This approach towards the Pacific distinguishes Chile from other Latin American countries. The interviewees mentioned little influence of comparative law in Chilean courts, either through reading foreign decisions or by "inter-American standards."

The jurisprudence is not uniform but tends not to recognize the right to be forgotten based on different arguments. Only in one of the evaluated cases did the Supreme Court understand that it would be applicable as a right to data cancellation for specific issues. In the Chilean Judiciary, some protection for the right to privacy may lead to the eventual protection of personal data. A respondent from civil society mentions that his entity began to undertake strategic litigation to seek the consolidation of judicial understandings on the topic. He explains that there have been some victories, including the payment of moral damages due to an information security breach. He also appears skeptical and considers that barriers to access to justice hinder the jurisprudential construction in Chile of the right to privacy and the protection of personal data (Veronese et al., 2023b, 1247-1248).

A highly problematic issue in Chile is the treatment of personal data for criminal purposes, which was addressed in detail by two respondents from civil society in the country. In this context, they mentioned the Chilean police's desire for cooperation. However, they are concerned about the risks of abuse that may exist (Veronese et al., 2023b, 1197-1198). Another respondent from civil society, in turn, pointed out that during the debate to amend the Chilean Computer Crimes Statute, the police presented requests to increase their competence with a reduction of previous and subsequent limits, but it was declined. One of the main arguments is the need to restrict this type of power (Veronese et al., 2023b, 1199). Chile is an excellent example of a country debating the need to modify its legal system to increase the protection of personal data and privacy and even integrate further into the global scenario; however, it is facing internal challenges that hinder this construction.

The case of Brazil is very different from that of Chile. Despite the late introduction of personal data protection and privacy on the political and social agenda, it is noticeable that it is gaining more and more ground. The most outstanding example was the promulgation of Constitutional Amendment No. 115/2022 so that the right to personal data protection is autonomous concerning personality rights. The topic of personal data protection in Brazil starts with academic studies, such as the pioneering thesis by Danilo Doneda (2006). This scenario was like what would happen, for example, in Argentina and Colombia. Especially in Argentina, academic production has been visible since the approval of Directive 95/46/EC in the then-European Community in the mid-1990s. The topic of national regulation with a focus on the Internet increased around the 2010s due to various factors, from the increasing use of communication applications such as social networks in political processes to the approval of the Marco Civil da Internet of Brazil (Statute No. 12.695/2014) in which the topic of personal data protection was debated and introduced for a future political agenda. This agenda ended up resulting in Brazilian legislation in 2018. The approval of the bills in the National Congress was a necessary response to Brazil's social and economic integration into the global paradigm. Although the LGPD – General Statute for the Protection of Personal Data (Statute No. 13,709/2018) has a *Vacatio Legis* of two years, this served as part of the legal basis for the joint ruling of the Constitutional Lawsuits 6387, 6388, 6389, 6390, and 6393 in 2020. This situation only reinforced itself with the creation of the National Data Protection Authority (ANPD), as diagnosed by the emerging scientific production on the topic in the country (Oliveira, 2020, 390; Keller, 2019, 246; Gutiérrez, 2019, 403).

Thus, the Brazilian paradigm of international insertion from the constitutional, legal, and institutional point of view is centered on legal modernity, although belatedly compared to several countries in the region, as already widely noted in this research. Two points of future development will help this image become more explicit. The first step will be the implementation and effectiveness of the ANPD in its regulatory performance, either alone or in cooperation with other bodies and entities of the Federal Public Administration. The second point is the judicial evolution of the issue. According to one of the academic interviewees from Brazil, there is hope that the judiciary will take over the topic. The same judicial takeover is the history of consumer law. An interviewee said: "Now the topic has become fashionable; let's all adapt as much as possible because this is fundamental." So, there would be

many judicial decisions on protecting personal data and privacy, especially with the attribution of civil liability (Veronese et al., 2023a, 200). According to a respondent from civil society, in line with the above, the legal issue of civil liability is vital for the Judiciary to assume a more prominent role in personal data protection. However, she is pessimistic about her diagnosis because she does not believe that, in the short term, there will be a sufficient volume of judicial decisions on the topic (Veronese et al., 2023a, 200-202). It is striking that the concern about the difficulties in addressing the subject in Brazil falls, like in other countries such as Chile and Panama, concerning the preparation — and even the generational issue — of the magistrates. This situation of concern about the legal training of those who exercise judicial activity is something relevant to highlight. In the judicial panorama, Argentina presents a dissonant example compared to the countries mentioned.

Argentinian Judiciary was critical in giving concreteness to the claims for access to information through habeas data, despite the initial difficulty in approving a specific law regulating Article 43 of the Constitution after its extensive reform in 1994. According to an interviewee from the government, judicial action during the period was essential (Veronese et al., 2023b, 1311). It is possible to infer that from an internal perspective, the Statute for the Protection of Personal Data of Argentina (Statute No. 25.326/2000) seems necessary to correct the deficiencies and insufficiencies of habeas data and the Amparo Trial as a procedural means for the protection of rights related to information and data. This need was so evident that despite the veto of the bill of 1996, its structure turned out to be helpful and was taken advantage of (Puccinelli, 2004, 45).

Moreover, due to Argentine federalism, the issue became part of the legislative agenda of the provinces, which had repercussions on federal law (Basterra, 2008b, 26). As previously indicated, factors related to international insertion were decisive for Argentina to approve its legislation, particularly the economic and social relationship that the country maintains with Spain (Veronese et al., 2023b, 1411, 1281). The Argentine casuistry was a motivating factor for including the topic on the public agenda. In addition to the famous "Facundo Urteaga" case in 1998 (Argentina, 1998), in 2010, the trial of the case "Belén Rodríguez vs. Google and Yahoo" took place, which referred to the issue of civil liability of search providers about indexed content and was resolved by the Supreme Court of the Nation. The providers won the case and were able to rule out objective liability. "Belén Rodríguez" is often called a case about the right to be forgotten. However, its focus has centered on the providers' responsibility (or, in this case, the detachment from their objective nature) and freedom of expression (Palazzi, 2021, 130). The closest case to international influence focusing on the right to be forgotten is the "Natalia Denegri" case, judged in 2022. Once again, the Supreme Court of Justice of the Nation valued freedom of expression (Veronese et al., 2023b, 1381). These cases came from celebrities who requested the de-indexation of search engines about facts of their past that, for some reason, are a source of embarrassment. It is worth noting that none of these cases delved into the issue of the use of images, which are usually treated incidentally in the prominent lawsuit. Therefore, there is no consolidated jurisprudence on the limits to the right to the image on social networks and the responsibility of the providers in damages and losses to the holders of personal data. Another critical case was "Halabi" in 2009, which was about the unconstitutionality of Statute No. 25,873 and its regulatory decree 1563/2004, which provided the capacity of public power to intervene in private communications to collect telecommunications metadata. This interference was due to requests for records that had to be stored indefinitely. The first collective lawsuit to reach the Supreme Court was "Halabi." Based on this case, the Supreme Court qualified the inviolability of communications as a fundamental right (Argentina, 2009). Finally, it is essential to note that Argentina is in the process of reforming its Personal Data Protection Statute, reinforcing the existing momentum to maintain its leading role in the region (Argentina, 2022).

Contrary to Argentine rulings, there are only a few relevant judicial cases regarding personal data protection in Mexico. According to an interviewee from the business sector, the Mexican Judiciary has historically been off the topic (Veronese et al., 2023a, 660). However, in 2021, the INAI presented a constitutional lawsuit that sparked a great national debate around the National Registry of Mobile Telephony Users – PANAUT. This system, among other measures, is intended for telecommunications companies to be required to collect biometric data to combat illicit acts committed through telephone lines, according to the responses to the survey questionnaire kindly answered by the INAI (Veronese et al., 2023a, 641). It had the participation of various civil society organizations. The INAI and civil society entities maintain a good relationship. This scenario is optimistic for expanding the personal data protection agenda in the country.

Uruguay is another country where the topic has had little judicial repercussion (Veronese et al., 2023a, 299), like Mexico, despite having a robust administrative system. Like Argentina, Uruguay was directly influenced by the European Community's decision to approve Directive 95/46/EC in 1995. This movement continues to advance in the political and administrative space of Uruguay. In the same way as Argentina, Uruguay sought an adequacy decision from the European Commission. An interview with an academic reinforces the topic (Veronese et al.,

2023a, 343). Furthermore, according to another interviewee from the academic field, the arrival of the General Data Protection Regulation will bring the need to promote new discussions postponed by the priorities of the newly elected Government and the pandemic (Veronese et al. 2023a, 362). Another sign of insertion has been the excellent relationship with the Council of Europe, as reported by two interviewees from the URCDP (Veronese et al., 2023a, 374-377).

Finally, in Panama's case, the scenario is still too incipient to describe the international influence concerning international organizations and jurisprudence. It is true that the approval of the legislation and its regulation, as already described in the national panorama, are closely related to the fact that the country is evolving in its scenario as a service provider at an international level.

It is evident when comparing the scenario of the surveyed countries that there is an international influence in forming legal standards and social beliefs and actions related to personal data protection and privacy. There is an attempt to anchor local legal meanings to international documents, such as treaties, and to observe what happens abroad to internalize legal meanings. The path to defining personal data protection as constitutional or fundamental rights is different. There are some similarities between some countries, such as a more significant influence of the judicial debate with constitutional antecedents (Argentina and Costa Rica). In others, the topic occupies more space on the administrative agenda (Colombia). What unites all the analyzed countries is the apparent attempt to organize their legal systems according to a paradigm that they consider part of modernity, directly related to the social and economic future. The following section will be dedicated to comparison, focusing on the specificities of the investigated countries in the region.

DISCOURSES IN FAVOR OF INSTITUTIONAL AND CULTURAL SPECIFICITIES, NATIONAL AND LOCAL, OF THE PROTECTION OF PRIVACY AND PERSONAL DATA

National and local contexts determine the practical construction of the Law. Various social, economic, and political factors will differ in legal meanings and social practices. For example, what makes protecting and managing personal data and privacy socially managed differently in Mexico and Argentina? The same concern applies to the other surveyed countries. The interviews and the literature analysis provided good clues about these possible answers. All field research shows a certain degree of attention in South America and the Caribbean regarding what happens in neighboring countries.

Broad National Singularities

A cursory review of the landscape in South America and the Caribbean might lead us to believe that there are mere attempts to emulate foreign models, particularly those of the EU or the United States (US), conveyed mainly through exchanges between state agencies, academic entities, and civil society. Research indicates that although these models are considered fundamental, their influence is not necessarily direct, as they are adapted and transformed according to national and local contexts.

It is possible to synthesize some peculiarities. One can start with Chile. Of all the surveyed countries, it is the most curious. It has the oldest statute and has yet to consolidate better means of protection due to the lack of a supervisory authority. The government is under legal influences from many origins - the EU, the US, Asia, and the Pacific traditions. This dilemma about directions and models becomes evident when reading an interviewee's criticism that the US needs a clear legal framework (Veronese et al., 2023b, 1235). This discourse demonstrates how Chile is amid an exciting moment, with several possibilities to complement its data protection and privacy model. President Joe Biden published an opinion article in the Washington Post, urging the US Congress to discuss and approve a federal statute for privacy protection on the Internet (Biden, 2023).

Mexico is another country with peculiarities. The first is its federated structure regarding the system of personal data protection, in which the INAI acts as a body for reviewing state decisions. Its duality of statutes is also peculiar. Since 2010, the Federal Statute for the Protection of Personal Data Held by Private Parties – LFPDPPP applies to the private sector. For the public area, there were several state laws. This country only harmonized the framework by creating a federal statute in 2017, the General Statute for the Protection of Personal Data Held by Obligated Subjects – LGPDPPSO. This process also has consequences for reorganizing the data protection authority - INAI. It experiences the expansion of its competence throughout the country in administrative cooperation with state authorities. According to a respondent from the business sector, the duality of the statutes came from the fear of the private sector that a single legislation could be too heavy a burden for the industry and

companies; however, he also expresses dissatisfaction with the solution since as he explains, it is not clear to citizens and businesses in certain situations which state law is applicable since there are 32 state and district statutes in addition to the federal statute (Veronese et al., 2023a, 653). There is a convergence in the interviews that perhaps the ideal would be to promote the separation between protecting personal data and privacy from access to public information. According to an interviewee from the business sector, the issue of access to public information would culturally have more prestige in Mexico than the protection of personal data, for example (Veronese et al., 2023a, 669). A similar conclusion is given by a representative of civil society. She underscores that the solid and recognized performance of the INAI ends up overshadowing its performance in the field of personal data protection; this fact would even have repercussions on state authorities and in the federal capital (Veronese et al., 2023a, 680-682). Finally, for another interviewee from the business area, this would also be reflected in allocating resources for personal data protection, which would be disadvantaged compared to the defense of access to public information (Veronese et al., 2023a, 698).

Another peculiar legal and formal feature of Mexico is that the topic evolved from the right to access information (Parra Noriega 2011, 155). Although this has been a constitutional right since 1977, the country's Constitution did not contemplate habeas data as a procedural means (Arroyo Kalis, 2017, 65). This scenario means that the procedure before the judiciary was the amparo trial (Veronese et al., 2023a, 661). It is interesting to see the case of the Argentine Republic, where the formalization of habeas data accompanied the creation of the Personal Data Protection Statute.

Regarding social participation, we analyze the case of Argentina, Brazil, and Mexico. Argentina has mechanisms for social participation within the Agency for Access to Public Information (AAIP). Thus, it is possible to contrast the Argentine case with the Brazilian one. In the latter, there is an excellent capacity for the articulation of civil society organizations around these issues, which is expressed by the Coalition Rights on the Network, in contrast to other countries with large territorial extensions, such as Argentina (Veronese et al., 2023b, 1421) and Mexico (Veronese et al., 2023a, 768). In Argentina, the Executive Power and the Senate appoint the directors of the data protection authority (Veronese et al., 2023b, 1345-1346). Civil society has pressured the government not to dictate in a particular direction, demonstrating social pressure despite lacking a formal coalition (Veronese et al., 2023b, 1413). In the case of Mexico, civil society organizations carry out their articulation at an adequate international level, forming coalitions such as the Global Encryption Coalition (2022) and AlSur (2022). However, they have yet to create an alliance at the national level (Veronese et al., 2023a, 688). The participation of Brazilian civil society has even influenced the approval of legislation that foresees an organ of the ANPD with its members: the National Council for Data Protection.

Uruguay and Argentina have the peculiarity of dedicating legal provisions in their specific laws to processing personal data in advertising matters. Neither GDPR nor Ibero-American Data Protection Network (RIPD) standards present this feature. A skeptical interviewee explains this by saying the Uruguayan statute would be a copy of the Argentine one (Veronese et al., 2023a, 314). Another example of the similarity between Uruguay and Argentina is that these countries look to the EU as an essential model, which explains the similarity of the statutes according to other interviewees from the academic sphere (Veronese et al., 2023a, 321, 400). This feature is also visible in that Uruguay was the second country in the region to receive an adequacy decision from the European Commission after Argentina, as explained by an interviewee from the URCPD data protection authority (Veronese et al., 2023a, 374).

This indirect influence of the EU also occurs in Panama and Brazil, although with different institutional results. Panama follows the Mexican model of adding personal data protection to public information access and anticorruption efforts, while Brazil created an autonomous data protection authority. The issue of public information access and the fight against corruption falls into the General Comptroller's Office (CGU), a ministry in Brazil.

The uniqueness of Costa Rica is that the Constitutional Chamber has had a historic role since before 2000 in importing the concept of "informational self-determination" and dealing with new information and communication technologies. It has given rise to exciting case law that regulated personal data protection even before the 2011 Statute. To this day, the Judiciary plays a noticeable role in the country and arouses criticism. An example is the ruling of the Constitutional Chamber that excluded the condition of being vaccinated from the category of sensitive personal data (Veronese et al., 2023b, 858). In the case of Peru, it is interesting to note the cooperative regulation between the data protection authority and the National Institute for the Defense of Competition and Intellectual Property Protection (INDECOPI). This administrative entity has the competence to act in the field of consumer law, which attracts the need to join efforts in personal data protection (Veronese et al., 2023a, 535).

Colombia presents a data protection authority that is peculiar since it does not combine with public information access (something that happens in Argentina, Mexico, and Panama, for example) but is within a significantly strengthened body in the national context linked to the Ministry of Economy, which is the SIC – Superintendence of Industry and Commerce. This authority has broad competencies in the field of competition and consumer protection. An appointed official manages it, and the protection of personal data is the responsibility of a Subcommission. This latter has a recent history of much activity, even with significant media impact, including other countries. A notable feature of Colombia is the substantial increase in complaints and orders issued (Veronese et al., 2023b, 1017). This efficacy is also due to the creation of electronic means for conflict resolution that involve the mediation of the authority. This electronic system has streamlined processes, reducing costs and difficulties for citizens in resolving their complaints.

Another Brazilian peculiarity, besides the participation of organized civil society, is found in the rapid approval of Statute No. 13.709/2018 and the legal community's commitment to the issue. The approval process was so fast that it generated the need for quick changes to ensure the construction of the ANPD (Veronese *et al*., 2023a, 174). While modifying the Statute, other changes were made, such as the imposition of a veto to the provision (paragraph 3 of Article 20 of the LGPD) that provided for human review of exclusively automated decisions. According to an interviewee linked to businesses, there was pressure from the industry that such a forecast would delay Brazilian technological development (Veronese et al., 2023a, 122). Another aspect of the issue is the opinion of an interviewee from the data protection authority, who indicates that this imposition would determine an increase in costs for credit entities, which would need to create many teams to carry out this task despite emphasizing that he and the ANPD are aware of the risks involved with automated systems (Veronese et al., 2023a, 48). An academic interviewee mentions that despite the veto, the issue is still not fully defined due to the applicability of other fundamental rights and principles — such as transparency, contradiction, and due legal process, for example — to automated decisions that restrict rights (Veronese et al., 2023a, 206).

Creating a unique classification among the different countries studied is difficult. What stands out is that there are several national paths to incorporate the issue of personal data protection and privacy, whether in legal systems, institutional structures, or defense means (judicial or administrative). This comparison clarifies that simplistic views of Latin America may lead to incorrect interpretations. Personal data protection and privacy are under building in several regional countries, even when they present interesting institutional differences related to specific cultural contexts. Even if Latin American countries try to import the legal concept of personal data protection from the UE as a fundamental right, the means for its implementation will be diverse. In the following subsection, we will see how the issue of the treatment of the various social groups existing within the different countries appeared in interviews and research documents.

National Singularities of Specific Social Groups

It is not surprising that the issue of the protection of legal minors arises in several interviews and is on the agenda of various countries. This is a global issue, but the means to achieve protection for children and adolescents vary in different countries. In the case of Costa Rica, the "FARO case" was addressed, which referred to the exams that the government tried to apply to children and has led to significant political and legal agitation. In Peru, it is interesting to note that in an interview, the data protection authority commented on the issue, relating it to the RIPD and its established standards — an active organization that is not an international body — as a basis for the entire region (Veronese et al., 2023a, 538). Concern for children and adolescents was also referred to in Uruguay as a relevant problem by two interviewees from the academic area and by a member of the data protection authority (Veronese et al., 2023a, 306, 355, 386).

In the case of Colombia, there was controversy regarding digital control systems, health data, and, therefore, citizens' sensitive data. The national application created for such control, which generated a QR code to allow access to specific spaces (Veronese et al., 2023b, 1033), has faced several controversies, according to a statement from a member of the data protection authority (Veronese et al., 2023b, 1016). As also explained by an interviewee from civil society, there needed to be more work in ensuring the application's proper use of personal data (Veronese et al., 2023b, 1109). For them, this scenario is worse since the possibility of the SIC sanctioning any deviation would be almost nil, as it would need more competence and autonomy to investigate and punish public agents (Veronese et al., 2023b, 1056).

The issue of gender and violence against women is a shared concern for Costa Rica and Panama. In Costa Rica, the respondent indicates a collaborative approach to ensure the effective functioning of a research center, with the

collaboration of the Spanish Data Protection Agency, Facebook, and other digital platforms. According to an interviewee from the business area, the goal is to create an accessible way to handle these cases in specialized channels in cooperation with agencies and government entities. The same interviewee also mentioned the Eurosocial project and the Organization of American States as elements supporting the effort (Veronese et al., 2023b, 901). In Panama, there is a need for women's empowerment, citing the cooperation of the data protection authority, ANTAI, with the National Institute of Women to create channels of protection against gender violence through applications, among other issues. These actions culminated in the creation of a Guide for Data Processing for Women Victims of Violence and collaboration with UNESCO. The problem was also expressly mentioned by ANTAI interviewees when they mentioned the need to attend to vulnerable groups such as immigrants, indigenous peoples, women, children, adolescents, and people living with HIV (Veronese et al., 2023b, 1524).

In the case of Mexico, it is worth highlighting that INAI conducted a national survey of social perception on data protection (Mexico, 2018). In the latest edition of the study, conducted in 2018, something that the literature calls the "privacy paradox" emerged. Some substantial people know their data needs to be under adequate processing. Yet, they need to find out measures to mitigate it. In this survey, 50% of the population said they were unaware of the existence of INAI, and 93% admitted that they had never filed any complaints about the improper use of their data. This phenomenon and the research data are a severe problem in the opinion of an academic interviewee, as it would further affect children and adolescents (Veronese et al., 2023a, 688). The privacy paradox also appeared in interviews with two academic women from Argentina (Veronese et al., 2023b: 1284, 1300). A third academic interviewee linked the problem to the vulnerability of children and adolescents.

Finally, when analyzing Brazil's case, the interviews brought the racial theme into the debate. One of the interviewees expressed his concern about facial recognition and racial issues. He also criticized the absence of black people in the National Data Protection Council and the leadership of the ANPD (Veronese et al., 2023a, 194).

The issue of specific social groups extended further to exposed or vulnerable groups. There needed to be a way to assess to what extent the judicial or administrative apparatuses for protecting personal data and privacy are effective in dealing with these specific social groups or if they perceive personal data differently than the general population. However, there are some clues about the possible social cultures and specific legal demands on the issue according to the broad set of interviewees (academics, government members, data protection authorities, and civil society representatives).

LOCAL DIFFICULTIES IN ACCESSING AND UNDERSTANDING THE RIGHTS OF PERSONAL DATA HOLDERS AND PRIVACY IN DIFFERENT COUNTRIES

Three significant issues undoubtedly affect the populations of Latin American countries: the digital divide, barriers to access to justice, the administrative protection system, and difficulties in raising awareness.

These three factors are concerning. The effectiveness of the right to personal data protection and privacy depends on social participation and an agreement between the state, civil society, and businesses. Therefore, collecting interviews and analyzing documents from various sources has been relevant to identifying these dilemmas in the surveyed countries.

It is possible to begin this description and analysis with the case of Peru, from which emerges the discourse of a civil society interviewee who considers that the country's population does not show a high degree of concern for protecting their data and privacy. Her discourse expresses a sentiment that can be identified in several other countries in the region and perhaps in the world. When reporting on issues such as video surveillance and facial recognition, she says that a good part of the population reacts like this: "They can monitor me and collect my data; I don't care; I have nothing to hide" (Veronese et al., 2023a, 449).

When recounting the regulatory history of the issue, an interviewee from the Peruvian business sector mentions that the local statute dates from 2011, and its regulation entered into effect in 2015. Therefore, she considers, quite optimistically, that it will take ten years for the issue to become widespread. Her perception is that the problem has gained ground in recent years and that although it is impossible to consider that there is a culture of personal data protection in the country, this reality is on its way (Veronese et al., 2023a, 508).

The need for social, individual, and collective actions also appears in Costa Rica. In this sense, according to an interviewee from civil society, the proactivity of the citizenry is very important to her, and it is fundamental to know this "popular culture among the citizenry," something that one can understand as the need for greater

routinization of the issue. There would be more excellent protection led by the citizen's actions based on their awareness and good responses from the state and businesses (Veronese et al., 2023b, 836). PRODHAB is the data protection authority in Costa Rica. The interviewee, an employee of the Institution, also emphasizes the need for "database education" for the general population (Veronese et al., 2023b, 952).

The Chile's case is also interesting. An academic interviewee explains that the Council for Transparency annually conducts a national survey on social concerns for personal data. According to her, most citizens would have shown in their responses that they were concerned. However, she considers that social practice would be diverse in general terms. Access to the citizen identification number in Chile — RUT (*Rol Único Tributario*) — would be facilitated by everyone to obtain discounts at pharmacies, for example. And that fact would not bother them at all. This Chilean case would be an example of the "privacy paradox" mentioned earlier. During the pandemic, there was a noteworthy event as a group of citizens started, on their own, protesting — offensively even — against the request for their data by the authorities when withdrawing money from pension funds as financial aid. This fact was reported (El Desconcierto, 2020), and the video is available on YouTube (T13, 2020). According to an interviewee, the case would be curious since there would be a legal basis for this practice, and there would never have been any public manifestation in favor of data protection in Chile (Veronese et al., 2023b, 1228-1229). Chilean civil society has effective organizations such as *Derechos Digitales* and *Fundación Datos Protegidas*, among others, but such aggressive action on the street was unprecedented. A Chilean government interviewee explains that the annual survey demonstrates growing concern and points out the rise in public awareness about the issue of personal data protection. For example, he noted that there would be more significant concern for advertisements. He also confirmed that there was resistance to handing over the RUT. However, he indicated that when they asked questions about health data in the survey conducted during the pandemic, there was a greater willingness to provide them (Veronese et al., 2023b, 1166).

The report from the ANPD in Brazil on the awareness issue was like that of Panama. There were indications of future work, and the authority was building institutional agreements with national institutions (National Secretariat of Consumer, Ministry of Justice and Public Security, CADE, Internet Steering Committee, among others) and international institutions (such as the Spanish Data Protection Agency). The interviewee also underscored the interest of the ANPD in having the government adhere to Convention 108+ (Veronese et al., 2023a, 35). In Panama, ANTAI is carrying out its campaigns and events to spread the issue despite the criticism from civil society interviewees (Veronese et al., 2023b, 1470-1471, 1503). The academic interviewee considers the issue new and, therefore, is being managed to the extent possible (Veronese et al., 2023b, 1446).

In Uruguay, the interviews also pointed out that citizens need help understanding their rights as the most significant obstacle. An academic interviewee considers this a complex issue and, therefore, difficult for society to assimilate (Veronese et al., 2023a, 352). This interviewee explained the dilemma in very logical terms. The population would know their rights and be aware of information misuse and security problems. However, there needs to be awareness of the means of protection to raise mobilization. This diagnosis does not harm an interviewee because progress must continue (Veronese et al., 2023a, 352, 409-410). Another academic interviewee reiterated that the issue of data protection and privacy has advanced in Uruguay, a fact that would have impacted greater social awareness. Therefore, businesses would see this protection—and compliance with the legislation—as an added value in their economic activities (Veronese et al., 2023a, 403). The respondents from the data protection authority of Uruguay had the same understanding as the academic respondents. He explained that URCDP conducts national surveys annually. The results would demonstrate positive effects based on awareness and communication campaigns on personal data protection and information security (Veronese et al., 2023a, 386). Another academic interviewee was quite explicit: there is still much to do before speaking of an influential culture of personal data protection (Veronese et al., 2023a, 320).

In the Argentine Republic, an academic interviewee considered that the issue would be outside the general focus of the population as they would be more concerned about satisfying other needs, especially of an economic nature (Veronese et al., 2023b, 1373). However, there would be a geographical and social division that would explain the dilemma, according to another civil society interviewee. The issue would be more widespread in cities than rural areas (Veronese et al., 2023b, 1419). This report also occurs in Mexico's case, in which a civil society interviewee indicated the need to travel to the country's capital, that is, to the headquarters of INAI, to assert rights (Veronese et al., 2023a, 760-761).

The Colombian literature diagnoses the dilemma of the digital divide, and it is a good starting point for this question. According to a recently published book, almost 60% of the poorest population did not use the Internet daily, in contrast with about 80% of daily use by the most affluent population (Saavedra Rionda, Práxedes, Ospina

Celis, Upegui, and León Torres, 2021, 70). There are multiple consequences, among them the difficulty of accessing opportunities and enjoying public services. The data protection authority focuses a lot on the problem of the interoperability of systems and their use by other state entities. It demonstrates that the SIC can issue orders to other state entities regarding the use of citizens' data.

Nevertheless, its competence does not enable it to apply sanctions since the Colombian legal system assigns this function to the Public Ministry. This legal situation did not turn into inertia on the part of the authority. An interviewee from SIC reports that a file was issued to other organs and state entities to explain that citizens' data could be used in public policies — even for issues related to the COVID-19 crisis — if there is observation of legal principles, which included security, transparency, purpose, and confidentiality, among others. The interviewee even asked: "How would it be possible to create an effective national public policy without interoperability?" (Veronese et al., 2023b, 1011).

Indeed, it is a recurring issue in the debate on protecting personal data and privacy. Data protection laws do not aim to prohibit the use of personal data; they determine its responsible and controlled use. Another reflection of the geographical and social problem would be evident in the interview with a state government representative, in this case, Jalisco. She points out that her state would be one of the most populated and that to enforce the law against private parties (LFPDPPP), it would be imperative to go to the capital. This problem would be reflected in less compliance by businesses outside the capital, besides explaining a lesser awareness of the population (Veronese et al., 2023a, 742). Somebody will likely repeat these narratives about the dichotomy between rural and urban areas and the great distances verified in federal countries like Mexico, Argentina, and Brazil.

The following section is dedicated to a relevant subject for the research: the mutual influences between the different Latin American countries and whether this could lead to the construction of a regional legal culture on the issue.

THE INFLUENCES OF LATIN AMERICAN COUNTRIES ON THE REGION: THE EMERGENCE OF A REGIONAL LEGAL CULTURE?

An epistemological caveat is necessary. The research team would be keen to see numerous responses indicating the existence of significant cultural exchanges among countries, whether in academic, business, or state cooperation realms. This expectation did not induce bias in terms of distorting the information obtained. Such exchanges do exist, being a prime example of the existence of the Ibero-American Data Protection Network (RIPD). The response for this survey leans less towards continuous interaction and more towards a national and local reception process of parameters, practices, and beliefs that have developed in other countries, such as EU member states, APEC members, OECD standards, and even actions —and defenses— by globally reaching companies like significant platforms.

In Peru, according to a civil society respondent, there would often be copies from other countries in the region. However, this parallels the EU model. The rationale for copying regional models would be the similarity with their neighbors (Brazil, Colombia, Argentina, and Chile are directly listed). In the case of employing European models, the respondent expresses some fear, considering the reality across the Atlantic to be different (Veronese et al., 2023a, 443). The respondent's discourse strongly references models of law and norms. The academic respondent clearly stated the influence of Colombian public policies in Peru, including listing different topics such as intellectual property and Internet governance (Veronese et al., 2023a, 580). The interview with a civil society representative was very enlightening. She also refers to Colombia as an example and then Chile and Argentina in general terms.

Regarding personal data protection regulation, she points out that Colombia is an example to follow, unlike Argentina. She considers that Chile would lag on the issue and that Brazil would have passed interesting legislation since it would not be a mere copy of the GDPR. She complains that some business and state sectors would focus only on Colombia and Brazil, ignoring ongoing innovative experiences in Paraguay and Ecuador (Veronese et al., 2023a, 466).

The same dichotomy appears in the narrative of a Costa Rican civil society interviewee. Mexico and Peru are named; however, the issue of looking at the closest neighbors is also raised (Veronese et al., 2023b, 835). An interviewee from the Costa Rican business sector acknowledged the need to strengthen the RIPD and internalize its standards into the legislation of different countries. Her response contains some speculation about the Uruguayan model, thinking it might be old—and therefore better established—and coming from a country with

similarities in territory and population. It is noteworthy that Costa Rica, in the PRODHAB interview, indicates a practical framework for cooperation with Mexico and a close relationship with Panama, including marked optimism about the new Statute they have approved there. The notion of a Central American scenario is evident (Veronese et al., 2023b, 950-951). The interviews with Panamanian civil society reinforce the regional image that the countries in the region are directly linked, including details of advances and issues (Veronese et al., 2023b, 1489-1493). An example is the close relationship between Panama and Costa Rica in the realm of exchange of experience on state affairs.

The interview with ANTAI in Panama also highlighted this concern to connect its work with Costa Rica and other neighbors; it indicates the dichotomy of doing so in line with some observance of EU processes (Veronese et al., 2023b, 1528). Additionally, the academic interviewee blamed the country's economic relationship with EU member states when reporting it at a public event directed at businesses in the financial sector (Veronese et al., 2023b, 1442).

In this case, Colombia, Argentina, and Uruguay are references, according to an interviewee from the academic area, due to their experience in the subject. It is well known that both countries have adequacy decisions issued by the European Commission. This same interviewee from the academic area, from Colombia, reinforces that the subject has advanced in Peru but slowly than he would have liked (Veronese et al., 2023b, 1130). A civil society representative reiterates the dichotomy between observing the neighbors and having contact with the EU experience, pointing out the importance of the RIPD. For her, despite being a newcomer to the subject, Brazil has impacted the region by creating a specific authority with a claim to autonomy. It is interesting because this civil society interviewee explains the reason for Colombia's prominence in the area. Part of the answer would lie in the investigations opened by the SIC about possible massive violations of the Colombians' personal data protection rights by large applications such as significant apps like Facebook and Zoom, among others.

This administrative action is possible as the country's legislation is technologically neutral and well-managed in such cases. The SIC is not an agency exclusively dedicated to protecting personal data; its scope of action covers other competencies linked to industrial and commercial regulation and competition law in a model like the U.S. FTC. The interview concluded with the remark that it would be necessary to conduct parallel investigations in the future, with the cooperative combination of several authorities, and that the RIPD could play a role in facilitating this process (Veronese et al., 2023b, 1099)

Latin American countries have faced the challenge of resolving this tension between data protection and the right to access public information. As reiterated by a Chilean government interviewee, the EU's experience has been received in a specific and unique manner across various Latin American countries (Veronese et al., 2023b, 1177).

The Brazilian case addresses the issue of isolation. The ANPD is a recent entity. Upon interviewing a representative of the entity, it becomes clear that, at this initial stage, they shall give more practical consideration to the experiences of other Latin American countries. Besides, they are paying close attention to debates within the EU. There was also no reference to the RIPD or any other country in the region. (Veronese et al., 2023a, 85).

The case of Argentina is quite different. It is a country with both a data protection authority and older legislation, and it has already obtained a decision of adequacy from the European Commission. In interviews with a civil society representative and a government representative, both converge in narrating Argentina's role in shaping the RIPD as well as the country's efforts to advance the matter within the Mercosur framework (Veronese et al., 2023b, 1315, 1426). They explain that the RIPD has evolved from an academic space to a forum for exchanging experiences of public policies as new data protection authorities appear in Latin America (Veronese et al., 2023b, 1315). Moreover, the country relinquishes that central role as other national entities have begun to share this burden. The interviewees point out Mexico and Colombia as influential members of the RIPD (Veronese et al., 2023b, 1292, 1317), and an academic interviewee postulates the need for the Network to consolidate a more influential role so that Latin American countries can address international dilemmas (Veronese et al., 2023b, 1297).

As mentioned in this text, constitutionalizing *habeas data* in Brazil influenced the region. According to a government interviewee, the 1994 constitutional reform receives fundamental inspiration from the Brazilian Federal Constitution of 1988 to include habeas data (Veronese et al., 2023b, 1301). Finally, an Argentine academic interviewee reiterates information — obtained from interviewees from Uruguay — about the evident influence of that country's legislation on the latter. She also mentions the importance of significant countries entering the fray, particularly Brazil and Mexico (Veronese et al., 2023b, 1292).

Regarding Mexico, a government interviewee explicitly indicates the use of normative practical references from Spain, Colombia, and Chile, emphasizing that there is always a search for international standards (Veronese et al., 2023a, 808). The legal literature on data protection in Mexico reiterates this information, indicating that the appropriation of influences comes from Spain, Germany, and Argentina, as the practice of data protection in these countries has enabled the development of the concept of informational self-determination (Quijano Decanini 2022, 165). Mexico's INAI has begun to play a very active role in the RIPD, assuming an evident protagonism (Veronese et al., 2023a, 632). Several interviewees point this out as a factor justifying Mexico's influence in countries like Colombia and Chile in the past, such as —recently—in Ecuador, Panama, Nicaragua, and El Salvador (Veronese et al., 2023a, 623, 642, 717, 765, and 770). Except for the latter country, Mexico's most significant influence would lie in indicating the need to build autonomous data protection authorities. Many interviewees praise the INAI's international performance (Veronese et al., 2023a, 595, 682, 699, 752).

Lastly, in interviews conducted in Uruguay, it was mentioned that there is influence among Latin American countries due to the existence of forums and conferences through which exchanges and interactions occur (Veronese et al., 2023a, 310). Another academic interviewee from Uruguay also highlighted the knowledge of legal frameworks and the direct exchange between data protection authorities (Veronese et al., 2023a, 357). The RIPD is indeed marked as one of these exchange forums, as will be mentioned in the following section. Moreover, Uruguay hosts the Mercosur institutions.

Concerning the Mercosur space, according to an Argentine academic interviewee, the attempts at practical cooperation among data protection authorities through the Network, such as conducting joint research, have not been successful despite indicating the production of manuals and joint studies by the Argentine and Uruguayan authorities, which she qualifies as academic rather than practical (Veronese et al., 2023b, 1260). The proximity between the data protection authorities of Argentina and Uruguay is evident if one considers the attempts to introduce the topic through Mercosur. In a 2005 book, Uruguayan researchers already tried to discuss data protection concerning the four countries of this economic bloc (Delpiazzo, Pascale, Peña, Meleras, and Saravia, 2005). In 1999, an Argentine researcher published a book addressing this idea's potential (Slavin, 1999).

Thus, it is evident that personal data protection has occupied the Mercosur agenda at certain times. One such instance was when an agreement with the EU was signed in 2010 to develop "Mercosur Digital" to strengthen the topic of including the information society in the bloc (Travieso, 2014, 1111). Despite the risk of sounding repetitive, it is worth noting how an interviewee from the data protection authority of Argentina believes that the topic can strongly return to the Mercosur agenda due to the approval of the LGPD in Brazil and the creation of the ANPD (Veronese et al., 2023b, 1334).

The "Mercosur Digital" project is also mentioned by the data protection authority of Uruguay to establish a common standard in the bloc and not to create an international law norm (Veronese et al., 2023a, 391). The topic remains in the economic bloc's debates within the Digital Agenda Group (Mercosur, 2023), with particular attention to the potential trade agreement with the EU. This issue was the subject of an academic debate in 2019 at the University of Buenos Aires (UBA) when Eduardo Bertoni was still at the helm of the National Directorate of Personal Data Protection of the Argentine Republic (Argentina, 2019).

This section demonstrates that a social process is underway in the region to disseminate and incorporate personal data protection and privacy as a social value in various countries. There is no single Latin American culture of personal data protection and privacy due to the social and institutional differences that mark the countries. This ongoing process finds some proposals focus on harmonizing the various legal cultures, whether external or internal. It is also important to note that it is not possible to say that any country in the region offers better or worse protection of personal data or privacy than another. Societies and their institutions have legally sheltered these values to the extent that they perceive them as a set of rights.

A MODEL OF APPRECIATION OF SOCIAL ACTIONS AND CULTURAL BELIEFS ON PERSONAL DATA PROTECTION AND PRIVACY

In this last section, there will be a set of social actions and cultural beliefs in the form of a table that explains the formation of concepts related to data protection and privacy culture in Latin America and other countries and regions. Social actions and the construction of beliefs can be individual and autonomous. These beliefs and actions may occur when individuals act alone and thus with greater protagonism, i.e., when they take specific actions to protect themselves or to build beliefs about the need for protection. Or even when individuals are

recipients of the actions and beliefs of others with less individual protagonism when they are recipients of technical, legal, and social protection means. These actions and beliefs can also be collective and autonomous, i.e., when a social group is involved. In this case, there can also be more group protagonism, such as the collective use of technical, legal, and social means to protect themselves. Alternatively, there may be less collective protagonism when other groups or institutions mobilize these means on their behalf.

Similarly, the table lists possible individual and heteronomous social actions and beliefs with greater or lesser individual protagonism to protect privacy and personal data. They are heteronomous because they use external elements concerning individuals and groups. In the case of the protagonism of other actors, the performance of office by administrative or judicial authorities (public defender, public ministry) in defense of specific individuals would be notable. Associative entities also are in this quadrant if they act on behalf of individuals. In the case of individual protagonism, actions and beliefs are often crafted by themselves as a means of self-defense.

Lastly, the table categorizes actions and beliefs that are collective and heteronomous, with varying degrees of institutional protagonism. This term refers to the role of authorities and social entities in protecting data and privacy.

In instances of greater institutional protagonism, these entities use technical, legal, and social means to benefit society or a specific group. In cases of lesser institutional protagonism, individual action is evident in pursuing collective means of protection, such as lawsuits or administrative requests. These actions can also include individual instruction from external and collectively used means, such as general guides produced by the State, companies, and civil society.

Table 2. Classification of means for seeking protection of privacy and personal data.

<table>
<tr><th>Actions and social beliefs for the protection of personal data and privacy</th><th>Emphasis on other actors, technical, legal, and social means</th><th>Emphasis on individuals in technical, legal, and social means</th></tr>
<tr><td rowspan="3">Autonomous and individual</td><td>Use of technical means for protection, such as standardized software programs that perform such protection</td><td>Individual modification of technical systems for personal use to customize their protection</td></tr>
<tr><td rowspan="2">Training or qualifications to protect oneself and others</td><td>Adoption of individual and behavioral measures for protection</td></tr>
<tr><td>Study of new techniques and protective actions</td></tr>
<tr><td>Autonomous and collective</td><td>Participation in private computer networks that use standardized technical means of protection</td><td>Definition of policies and protection actions carried out by specific groups for their benefit</td></tr>
<tr><td>Heteronomous and individual</td><td>Action taken on their initiative by administrative or fiscal authorities, social groups, or companies to protect specific individuals, such as a minor or another vulnerable person, even without their request</td><td>Request for judicial or administrative protection of a protective nature by the person. Also, seeking individual protection within associations</td></tr>
</table>

Heteronomous and collective	The existence of legal norms that provide for the protection of individuals and groups	Request for judicial or administrative protection of an individual protective nature in the State, companies, or civil society. Seeking individual protection in collective means, such as in associations
	Direct action by administrative entities that constantly supervise protection. Actions of bodies or collectives, such as the Public Ministry (or the Public Defender's Office), militant defense (cause lawyering), and associations seeking protection	
	The State, companies, or social collectives organize awarenessraising actions on rights	Active and individual search for general and external information—produced or provided by the State, companies, or civil society—to receive certification

(Source: authors' elaboration).

Table 2 allows us to introduce the concept of plasticity to understand that a company in a specific country can have an institutional culture of personal data protection that differs from that mandated by local law, as inferred from the actions and beliefs of its employees or its institutional actions. Similarly, a social group may have a distinct culture. Moreover, these two local cultures may vary regarding regional standards (such as those of the EU) and global technical standards (ISO/IEC 27701). This table does not contradict the idea of a legal subculture of personal data and privacy protection distinct from a popular culture on the same subject. An example of this difference is the various social and legal conceptions of the "right to be forgotten," which, even among legal professionals, shows noticeable variations from one country to another (Kurtz, 2022). The "privacy paradox," which refers to the desire for protection while individuals actively engage in behaviors that expose them, is another example of the complexity of this issue. It is interesting to note that none of the table's elements precludes others' social management.

FINAL CONSIDERATIONS

The conclusion of the lengthy trajectory of analyzing sixty-three interviews and extensive documentation and literature is that there is an ongoing process in the region in favor of forming a Latin American social and legal concept of personal data protection and privacy. It exists precisely to the extent that evident exchanges of experiences and models among countries happen through state actions, interactions with civil society, or companies. Amidst the claims of building global cultural narratives to protect privacy and personal data, we observe the emergence of national, local, regional, and specific social group narratives. While not unique to these rights, this coexistence of socio-cultural narratives has been significantly amplified by the expansion of digitalization and the advent of new information technologies. These technological advancements have served as a catalyst, driving the proliferation of these narratives. In this way, an interesting parallel construction is observed—at different times and with varying resource allocations—of translations of elements from outside to inside countries, which transform themselves into specific social, institutional, and legal practices according to the contexts observed. There is no single Latin American culture of personal data protection and privacy. Several national and local versions of a type of law aim to be broad, global, and perhaps universal.

REFERENCES

1. Alsur. "*Qué hacemos*," 2022, https://www.alsur.lat/que-hacemos.

2. Aparicio, Irene. "*Claves de la Ley Orgánica de Protección de Datos Personales de Chile*." Global Suite Solutions, 2022, https://www.globalsuitesolutions.com/es/claves-ley-organica-proteccion-de-datospersonales-chile/.
3. Argentina. *Senado*. "*Constitución de la Nación Argentina*," 1994, https://www.senado.gob.ar/bundles/senadoparlamentario/pdf/institucional/constitucion_nacional_argentina.pdf.
4. Argentina. *Corte Suprema de Justicia de la* Nación. "*Urteaga, Facundo Raúl c/ Estado Nacional – Estado Mayor Conjunto de las FF.AA. – s/amparo Ley 16.986*," 1998, http://www.saij.gob.ar/corte-suprema-justicianacion-federal-ciudad-autonoma-buenos-aires-urteaga-facundo-raul-estado-nacional-estado-mayor-conjuntoffaa-amparo-ley-16986-fa98001242-1998-10-15/123456789-242-1008-9ots-eupmocsollaf.
5. Argentina. *Corte Suprema de Justicia de la Nación*. "*Halabi, Ernesto c/ P.E.N. – Ley 25.873 – dto. 1563/04 s/amparo Ley 16.986*," 2009, http://www.saij.gob.ar/corte-suprema-justicia-nacion-federal-ciudad-autonomabuenos-aires-halabi-ernesto-pen-ley-25783-dto-1563-04-amparo-ley-16986-fa09000006-2009-02-24/123456789-600-0009-0ots-eupmocsollaf
6. Argentina. "*Universidad de Buenos Aires. Acuerdo UE-Mercosur: posibles escenarios en la protección de datos personales*," 2019, http://www.derecho.uba.ar/derechoaldia/notas/acuerdo-ue-mercosur-posiblesescenarios-en-la-proteccion-de-datos-personales/+7788.
7. Argentina. *Agencia de Acceso a la Información* Pública. "*Nuevo Proyecto de Ley de Protección de Datos Personales*," 2022, https://www.argentina.gob.ar/aaip/datospersonales/proyecto-ley-datos-personales.
8. Arroyo Kalis, Juan Ángel. "*Hábeas data: elementos conceptuales para su implementación en México*." In *La Constitución y sus garantías: a 100 años de la Constitución de Querétaro de 1917*, edited by Eduardo Ferrer Mac-Gregor, and Rogelio Flores Pantoja, 53-68. Querétaro: UNAM, 2017, https://archivos.juridicas.unam.mx/www/bjv/libros/10/4633/4.pdf.
9. Basterra, Marcela I. *Protección de datos personales: la garantía de hábeas data*. Buenos Aires and Mexico City: Ediar and UNAM, 2008a.
10. Basterra, Marcela I. *Protección de datos Personales: Ley 25.326 y Dto. 1558/01 Comentados - Derecho Constitucional Provincial Iberoamérica y México*. Buenos Aires: Ediar, 2008b.
11. Biden, Joe. "Republicans and Democrats, unite against Big Tech abuses: Congress can find common ground on the protection of privacy, competition, and American children." *Washington Post*, January 11, 2023, https://www.wsj.com/articles/unite-against-big-tech-abuses-social-media-privacy-competition-antitrustchildren-algorithm-11673439411.
12. Borgioli, Martin. "*Google es sancionado por primera vez en Perú por desconocer el derecho al olvido*." *Hiperderecho*, June 21, 2016, https://hiperderecho.org/2016/06/google-sancionado-datos-personales-peruderecho-olvido/.
13. Brasil. *Supremo Tribunal Federal*. "*Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.388*," 2020, https://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949382&ext=.pdf.
14. Cervantes Díaz, Fernando. "Derecho a la intimidad y hábeas data. " *Revista Derecho y Realidad*, 7, no. 13 (Universidad Pedagógica y Tecnológica de Colombia, 2009): 27-35, https://revistas.uptc.edu.co/index.php/derecho_realidad/article/view/5010,
15. Chile. *Senado*. "*Protección y tratamiento de datos personales: claves de la modernización en trámite – el proyecto actualiza nuestra legislación a los estándares internacionales y crea una Agencia de Protección de Datos Personales*," April 2, 2022, https://www.senado.cl/proteccion-y-tratamiento-de-datos-personalesclaves-de-la-modernizacion.
16. Colombia. *Senado de la República*. "*Ley Estatutaria 1266 de 2008*," December 31, 2008, http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html.
17. Colombia. *Corte constitucional*. "*Sentencia T-094 (Carlos Alberto Legarda Valencia contra la Asociación Bancaria y entidades financieras)*," 1995, https://www.corteconstitucional.gov.co/relatoria/1995/T-09495.html.

18. Contreras Vásquez, Pablo; Bordachar Benoit, Ortiz Michelle; Mesías, Leonardo. *Privacidad y protección de datos personales jurisprudencia seleccionada y comentada*. Chile: DER Ediciones, 2022.
19. Delpiazzo, Carlos E., Maricarmen Pascale, Daniela Peña, Flavia Meleras, and Andrés Saravia. *Protección de datos personales en Uruguay y el Mercosur*. Montevideo: Fundación de Cultura Universitaria, 2005.
20. Doneda, Danilo. *Da privacidade à proteção de dados pessoais*. Río de Janeiro: Renovar, 2006.
21. El Desconcierto. "*¿Por qué necesita conocer el RUT?*": *Briones hace polémica solicitud de datos de quienes retiraron el primer 10%. El Desconcierto*, November 5, 2020, https://www.eldesconcierto.cl/nacional/2020/11/05/por-que-necesita-conocer-el-rut-briones-hace-polemicasolicitud-de-datos-de-quienes-retiraron-el-primer-10.html.
22. Estados Unidos Mexicanos. *Cámara de Diputados*. "*Constitución política de los Estados Unidos Mexicanos*." December 24, 2020, http://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Constitucion_Politica.pdf.
23. Global Encryption Coalition. "About Global Encryption coalition," 2022. https://www.globalencryption.org/about/.
24. Gómez, Tomáz. "*A un año de histórico allanamiento: 10 momentos clave del caso UPAD*," *El Observador*, March 1 mar, 2021a, https://observador.cr/a-un-ano-de-historico-allanamiento-10-momentos-clave-del-casoupad/.
25. Gómez, Tomáz. "*Pruebas FARO costaron 2.319 millones – 11% fue por polémicos cuestionarios de datos personales*," *El Observador*, November 16, 2021b, https://observador.cr/pruebas-faro-costaron-2319millones-11-fue-por-polemicos-cuestionarios-de-datos-personales/.
26. Gómez, Tomáz. "*Caso UPAD: estas son las penas a los delitos que la Fiscalía acusa al presidente Alvarado*," *El Observador*, February 4, 2022, https://observador.cr/caso-upad-estas-son-las-penas-a-losdelitos-que-la-fiscalia-acusa-al-presidente-alvarado/.
27. Gutiérrez, Andrei. "*Da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade*." In *Lei Geral de Proteção de Dados Comentada*, edited by Viviane Maldonado, Viviane Nóbrega, and Renato Opice Blum, 401-419. São Paulo: Revista dos Tribunais, 2019.
28. Keller, Clara Iglesias. "*Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado*." Ph.D. diss., Universidade do Estado do Rio de Janeiro, 2019, https://www.bdtd.uerj.br:8443/handle/1/9210.
29. Mercosur. "*Agenda Digital*," 2023, https://www.mercosur.int/temas/agenda-digital/.
30. México. INAI. "*Encuesta Nacional de Percepción Ciudadana*", 2018, https://home.inai.org.mx/wpcontent/documentos/EstudiosInai/inai_parametro_201_v7.pdf.
31. Parra Noriega, Luiz Gustavo. "*Desarrollo legislativo en materia de datos personales en las Entidades Federativas: la importancia de una legislación especial en el ámbito estatal*." In *Retos de la protección de datos personales en el sector público*, edited by INFODF, 145-177. Mexico City: INFODF, 2011.
32. Oliveira, Caio César de. "*A Autoridade Nacional de Proteção de Dados e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade*." In *A LGPD e o novo marco normativo no Brasil*, edited by Caitlin Mulholland, 371-383. Porto Alegre: Arquipélago Editorial, 2020.
33. Palazzi, Pablo A. "El Hábeas Data en el Derecho Argentino." REDI: Revista Electrónica de Derecho Informático 4, 1998, https://vlex.es/vid/habeas-data-derecho-argentino-106999.
34. Palazzi, Pablo A. "*Tutela de derechos personalísimos em internet: el estándar del caso Belén Rodríguez*." In *Protección de datos personales: doctrina y jurisprudencia, tomo 2*, edited by Pablo A. Palazzi, 129-138. Buenos Aires: CETYS, 2021.
35. Peru. *Tribunal constitucional*. "*Recurso Extraordinario n. 2488-2002-HC-TC*," 2002, https://www.tc.gob.pe/jurisprudencia/2004/02488-2002-HC.html/.
36. Peru. *Congreso de la República*. "*Ley n. 29733, Ley de Protección de Datos Personales*," 2011, https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/243470-29733/.
37. Peru. *Presidencia de la República del Perú*. "*Constitución Política del Perú (1993)*," 2018, https://www.gob.pe/institucion/presidencia/informes-publicaciones/196158-constitucion-politica-del-peru.

38. Puccinelli, Oscar R. *Protección de datos de carácter personal*. Buenos Aires: Astrea, 2004.
39. Quijano Decanini, Carmen. *Derecho a la privacidad en internet*. Mexico City: Tirant lo Blanch, 2022.
40. Red Iberoamericana de protección de Datos. "Estándares Iberoamericanos de Protección de Datos Personales," 2017, https://www.redipd.org/es/documentos/estandares-iberoamericanos.
41. Remolina Angarita, Nelson. *Recolección internacional de datos personales: un reto del mundo post-internet. XVIII Edición del Premio Protección de Datos Personales de Investigación 2014*. Madrid: Agencia Española de Protección de Datos, 2015.
42. Restrepo, José Miguel de la Calle. *Autodeterminación informativa y hábeas data en Colombia: análisis de la ley 1266 de 2008 - jurisprudencia y derecho comparado*. Bogotá: Editorial Temis, 2009.
43. Reusser Monsálvez, Carlos. *Derecho al olvido: la protección de datos personales como límite a las libertades informativas*. Santiago: Ediciones DER, 2021.
44. Ruiz Ardila, Betsy Yahanna. "Regulación en materia de protección de datos personales o hábeas data en Colombia a través de la Ley 1581 de 2012: examen histórico y crítica sobre su ineficacia ante las administradoras de bases de datos, portales de Internet y motores de búsquedas," Paper, 2016, Universidad Católica de Colombia, https://repository.ucatolica.edu.co/entities/publication/4f4a2ff8-25e6-40c9-b8169bb11183b9cc.
45. Ruiz Martínez, Esteban. *Protección de los datos personales en los informes crediticios: delitos contra la intimidad informática*. Buenos Aires: Hammurabi, 2015.
46. Saavedra Rionda, Víctor Práxedes, Daniel Ospina Celis, Juan Carlos Upegui, and Diana C. León Torres. *Desigualdades digitales. Aproximación sociojurídica al acceso a Internet en Colombia*. Bogotá: Editorial Dejusticia, 2021.
47. Simão, Bárbara, Juliana Oms, and Livia Torres. "Autoridades de Proteção de Dados na América Latina: um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai." São Paulo: IDEC, 2019, https://idec.org.br/publicacao/autoridade-de-protecao-de-dados-na-america-latina.
48. Slavin, Diana D. *Mercosur: la protección de datos personales*. Buenos Aires: Depalma, 1999.
49. T13. "Minister Briones is confronted in the street." *T13*, November 5, 2020, https://www.youtube.com/watch?v=7pjUxVC4mK4.
50. Travieso, Juan Antonio. *Régimen jurídico de los datos personales, tomo II*. Buenos Aires: Abeledo Perrot, 2014.
51. Uruguay. *Parlamento del Uruguay*. "Constitución de la República," 1967, https://parlamento.gub.uy/documentosyleyes/constitucion.
52. Veronese, Alexandre, Alessandra Silveira, Amanda Braga, Amanda Nunes Lopes Espiñeira Lemos, Eduarda Costa Almeida, Luiza Mendonça da Silva Belo Santos, Luiza Peixoto Veiga, Mariana Moutinho Fonseca, Marcio Iorio Aranha, Rebecca Lemos Igreja, Thiago Guimarães Moraes, and Vitória Bragança Sernégio. *Pesquisa documental e de campo sobre autoridades de proteção de dados na América Latina: o conceito social e institucional de privacidade e de dados pessoais – Anexo 2 (unidentified surveys) – Tomo 1*, Brasilia: Fapesp, 2023a.
53. Veronese, Alexandre, Alessandra Silveira, Amanda Braga, Amanda Nunes Lopes Espiñeira Lemos, Eduarda Costa Almeida, Luiza Mendonça da Silva Belo Santos, Luiza Peixoto Veiga, Mariana Moutinho Fonseca, Marcio Iorio Aranha, Rebecca Lemos Igreja, Thiago Guimarães Moraes, and Vitória Bragança Sernégio. *Pesquisa documental e de campo sobre autoridades de proteção de dados na América Latina: o conceito social e institucional de privacidade e de dados pessoais – Anexo 2 (unidentified surveys) – Tomo 2*, Brasilia: Fapesp, 2023b.