Special Issue: Comparative Approaches to Studying Privacy: Opening Up New Perspectives

SM+S
social media + society

Social Media + Society
April-June 2025: 1–13

DOI: 10.1177/20563051251337206
journals.sagepub.com/home/sms
Sage

(Lack of) Patterns in Commitment: Data Protection in the Latin America and Caribbean Personal Data Protection Laws

Elías Chavarría-Mora[1,2]

Abstract

What are the data protection policies in the Latin America and the Caribbean (LAC) region? The developments over the last two decades on massive data collection, as well as the developments in computational power and data science methods appropriate for extracting insights from digital trace databases, have led to increased importance on the protection of the data of citizens, particularly sensitive data. In this exploratory study, I adopt an inductive thematic analysis approach to create a qualitative matrix based on the current version of the primary legislation protecting personal data for each country in the LAC region. Through a thick description of similarities and differences in the laws, I identify dimensions of variation in the commitment to data protection, such as the moment of approval, the existence of data protection agencies and their resources, the existence of registries, and the type of consent needed from citizens. A mapping of commitment to data protection does not show clear subregional patterns. Still, the adoption of data protection laws grows over time, and it appears to be in part propelled by the economic need to rise to the data protection standards of the European Union.

Keywords

personal data, data protection, LAC

Introduction

In 2012, Colombian hacker Andrés Sepúlveda was arrested by the Colombian government on charges of espionage and various computer crimes. Sepúlveda claimed to have an extensive professional history as a political hacker in the region, working on electoral campaigns in several countries in Latin America. In this line of work, he engaged in activities that violated the privacy of political candidates and ordinary citizens, including stealing information, manipulating social media, and spying (Robertson et al., 2016). While a spectacular case, Sepúlveda's story is not unique and highlights one facet – related to electoral politics – of the broader issue of insufficient personal data protection in the region. Other facets of this problem also include discrimination based on credit scores, criminal activity, and the misuse of data for commercial or political purposes (Robertson et al., 2016; Udupa, 2024). At least two developments have increased the importance of data protection, particularly sensitive data. The first is the rapid expansion, over the last two decades, of massive data collection across every aspect of life, driven by platforms such as Facebook and Google. The second is advancements in computational power and data science methods, which enable the extraction of insights from these vast digital trace databases (Sadowski, 2019).

Considering the various ways political espionage, discrimination based on credit scores, and criminal activity can affect the quality of life for citizens in Latin America and the Caribbean (LAC), and the vulnerabilities these issues expose regarding control over personal data, this article asks the question: What are the data protection policies in the LAC region?

Examples of the mismanagement of such data abound. Perhaps the most famous is the Cambridge Analytica scandal in the United States, in which the political consulting firm used the unethically obtained data from millions of Facebook users to create targeted advertisements to influence the 2016

[1]University of Pittsburgh, USA
[2]Universidad de Costa Rica, Costa Rica

Corresponding Author:
Elías Chavarría-Mora, University of Pittsburgh, Pittsburgh, PA 15261, USA.
Email: elc117@pitt.edu

election (Brown, 2020). The LAC region is not exempt from such controversies. In 2020, the Carlos Alvarado Government in Costa Rica suffered a significant blow to its popularity due to a scandal involving the Presidential Taskforce of Data Analysis (*Unidad Presidencial de Análisis de Datos*, UPAD). Through an executive decree, the government illegally granted the UPAD access to citizens' confidential information, triggering alarms among the opposition, the judiciary, the media, the ombudsman office, and the general public (Le Lous, 2021).

The danger of data mismanagement is amplified by the fact that virtually any form of anonymized data can be augmented with alternate data sets to re-identify respondents. Salganik (2019) documented various methods by which this can occur, often revealing sensitive information from supposedly "anonymized" databases. Some of these examples are Netflix movie rankings (Narayanan & Shmatikov, 2008) or health records (L. Sweeney, 2002), including information such as sexual orientation or home address. The growing volume of digital trace data available—much of it generated by social media—and the increasing sophistication of methods for analyzing it pose significant challenges to protecting the right to privacy worldwide, including in the LAC region.

The potential negative consequences of data mismanagement can extend to spheres including employment denial (King & Mrkonich, 2016), health care data security issues (Chandra et al., 2017), credit record information theft (Vladeck, 2016), and organized crime (Jirovský et al., 2018). On the contrary, these new volumes of data and methods offer wide-ranging opportunities for scientific research and applications to improve policy. However, these opportunities also come with the danger of unexpected negative consequences, as exemplified by the data anonymity examples above.

This article investigates the LAC region's laws regarding personal data existing during the year 2022, extending prior work in two ways: First, by increasing the number of countries to the entire LAC region and also by adding data protection laws that have been adopted since prior studies. Second, this article adopts a flexible and inductive approach that avoids constraints from prior research and instead is data-driven in its thematic analysis, identifying the relevant dimensions of variation between countries in their data protection laws. In doing so, it identifies several points in common but also recurring differences in the region's laws, ultimately leading to no clear subregional pattern. There were outliers even if the Southern Cone seems to have comparatively stronger laws than Central America and the Caribbean.

A further contribution of this article is that the mapping is done in an underexplored regional context, expanding away from most studies, which are usually focused on WEIRD (Western, educated, industrialized, rich, and democratic) countries, which have influenced the data protection laws of the LAC region, even though there are relevant differences in values that should be put attention to. The LAC region has also led to unique innovations in what is considered personal data, as well as in legal instruments such as habeas data, further underscoring the relevance of focusing on this part of the globe.

Personal data protection frameworks in LAC

A pattern of diffusion is evident in the LAC region, where one or more dominant international frameworks have influenced national data protection laws. Many LAC countries have developed their legal frameworks by adopting these dominant models. For instance, the European Union framework, or the General Data Protection Regulation (GDPR), is very influential in the Argentinian and Uruguayan frameworks (Lehuedé, 2019, p. 33). Lehuedé also notes the relationship between the GDPR framework and the set of guidelines by the Organization for Economic Co-operation and Development (OECD), which is relevant for the LAC country members of the organization, such as Mexico, Chile, Colombia, and Costa Rica. The Asia-Pacific Economic Forum (APEC) privacy framework significantly influenced the frameworks used in Mexico, Colombia, and Peru (Lehuedé, 2019, p. 33). Regional initiatives have also been identified, including the Ibero-American Data Protection Network, spearheaded by Spain, and the eLAC initiative from the United Nations Economic Commission for Latin America and the Caribbean (ECLAC) (Lehuedé, 2019).

For their part, Carrillo and Jackson (2022) carried out an extensive study on the influence of the GDPR framework throughout countries in the LAC region since 2016 until 2021. They found that Brazil, Chile, Mexico, and Uruguay were the first movers to try to adapt their legislation to the GDPR standards. Another finding was that the countries in the region often approved omnibus legislation (that is, comprehensive) and included the provision of so-called ARCO rights. ARCO is an acronym coming from access, rectification, cancelation, and opposition, all different actions citizens could engage in with regard to how their personal data are processed (Blades & Herrera-González, 2016). Furthermore, most of the countries in their study (which encompasses South and Central America) were influenced by the European standard (Carrillo & Jackson, 2022).

The general logic of diffusion, particularly regarding the European standards, is linked to the idea of the "Brussels effect," which posits that commerce with Europe forces other countries to adopt similarly robust regulatory frameworks, including but not only applicable to data protection (Bradford, 2012). Despite the general logic of diffusion, the LAC region has historically lagged behind Europe in adopting such measures (Wolfson, 2016), likely due to the relative weakness of the integration process on human rights in the LAC region. In contrast, member countries must integrate regulatory measurements in the case of at least the European Union. Nonetheless, some unique innovations have come from the

region, such as the *habeas data*, an original creation of the 1988 Brazilian constitution that later spread to Paraguay, Peru, Argentina, Ecuador, and Colombia (Guadamuz, 2001).

Habeas data is an extension of the *habeas corpus* writ. *Habeas corpus* refers to a writ that commands that a person being held in custody be brought before the court to decide whether the detention is lawful; by extension, *habeas data* refers to the right to access one's information, that is, the data that third parties have collected about the individual (Carrillo & Jackson, 2022; Guadamuz, 2001). More specifically, the habeas data writ "provides citizens the right to access personal information collected by the government or a private entity and to challenge or correct the data" (Lode, 2019, p. 43).

In the context of social media and personal data protection, *habeas data* could be invoked to discover if a private entity has stored personal data obtained through web scraping social media and demand the destruction of correction of the data. Besides the *habeas data*, diffusion had also been found in other facets of access to data in the region, for example, in the domestic isomorphic constraints over Freedom of Information oversight agencies in Chile, Peru, and Uruguay, cases in which the prior domestic institutional design of the country and coalitions of political actors limited the strength imbued in the FOI institutions (Piñeiro Rodríguez et al., 2022).

The importance of data protection frameworks is evident in their impact on data-driven policies and their effectiveness. For example, a 2021 issue of *International Data Privacy Law* explored the role of such policies in mitigating the COVID-19 pandemic in Latin America. The studies highlighted the critical role data protection played in designing policies to address the pandemic by balancing data access for researchers and the government with protecting the well-being and privacy of citizens. Among these policies are the adoption of contact tracing (Alanoca et al., 2021), public access to pandemic data (Moraes et al., 2021), and restrictions on civil liberties (Calderon et al., 2021).

As shown in this section, data protection in the LAC region is influenced by different international frameworks, partly through a diffusion process directed by commercial interests that want to comply with European Union standards. Despite this, the region has also shown innovation in personal data protection. The next section presents the primary data and methods used to analyze patterns in data protection laws across the region. This analysis employs a comparative design that creates a qualitative matrix focused on relevant dimensions of comparison by repeatedly reading the data protection laws of the countries of the region, ultimately using it to assign scores in commitment to data protection for each country.

Data and methods

A baseline for the governmental protection of personal data is the existence of a law determining in which ways the government will allow the creation of databases with information about their citizens, which organizations will oversee these databases, and which types of collection will be allowed, as well as which penalties exist in the case that an actor behaves in bad faith. In that sense, I followed the logic of Carrillo and Jackson (2022), focusing on the *de jure* nature of personal data protection as a preliminary step before any form of *de facto* protection. In their study, Carrillo and Jackson followed this de jure approach as it allowed them to keep precise information about the similarities and influence of the European legal influence on data protection in the LAC region's legislatures.

For this study, I adopted an exploratory approach by first creating a qualitative matrix based on the current version of the primary legislation regarding the protection of personal data for each country in the LAC region until 2022. The logic of the project follows that of thematic analysis (Braun & Clarke, 2006; Maguire & Delahunt, 2017), by which a first review of the data leads to the creation of relevant categories, followed by the identification of themes. Then, through iterative processes, the data and themes are re-assessed until a saturation point is reached.

Thematic analysis offers a series of advantages, particularly the iterative process described in the next paragraph, which allows for flexibility in identifying categories (including emerging ones through exploration) and, most importantly, helps lead to a thick, in-depth description of the analyzed legal documents. Furthermore, thematic analysis is a research technic not bound to any specific epistemological or theoretical tradition (Braun & Clarke, 2006). This allows the researcher to adopt an inductive approach that is driven by the data, using the data to develop themes and categories (Maguire & Delahunt, 2017). While the data-driven, inductive approach to thematic analysis offers freedom and theoretical flexibility to the researcher, a downside is that the high volume of data and the iterative process produce less structured findings than research with a clear, pre-set theory. Thematic analysis is also ultimately an interpretative technique, which means that, like any other interpretative technique, the researcher's subjectivity will play a role in interpreting the findings.

I read and then re-read the laws in an iterative process, identifying points of commonality and differences between them and coding them as such in a qualitative matrix. The variables were identified under two complementary logics: A particular category, or highly similar language, which was repeated over and over in all of the different laws or making it clear that it was a relevant element for all the various legislation, perhaps with a variation of two types (for example, explicit vs. implicit consent). The other logic for selection corresponded to the appearance of notable divergences. For example, when some laws established a government organization to oversee data protection enforcement, other laws did not. These two logics were used throughout the first read and then a second one until saturation was achieved, and I settled on the categories used for the rest of the study.

While the project sought to approach the data collection process with no a priori theories and concepts, it was crucial to consider one concept, which was unavoidable by its sheer

necessity in defining the research question: personal data. Personal data are the primary type of data codified and protected by data protection laws in the LAC region, in part due to its relevance to the GDPR, and it is defined in most of the legislation as more or less "any information relating to an identified or identifiable natural person" (Lehuedé, 2019, p. 12). This definition is broad and vague, but was necessary as it explicitly precedes the data collection process.

I collected and read the full text of the legislation from online government sources in each country in the LAC region. Table 1 includes the 25 countries of the LAC region considered for the study; Puerto Rico and French Guiana were excluded due to their nature as dependents of countries outside the region. Of the 25 countries, only 17 had personal data protection laws: Argentina, Belize, Brazil, Chile, Colombia, Costa Rica, Cuba, Dominican Republic, Ecuador, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, Trinidad and Tobago and Uruguay.

Based on these documents, I created categories of relevance for the matrix on an iterative process based on my reading of the laws. This method aimed to identify similarities and differences between the texts of the laws, mainly around which concepts were defined and how much detail and forethought was given to the different categories of the matrix. In this regard, I expanded for all of the LAC region upon the work of Lehuedé (2019), who only included six countries (Argentina, Brazil, Chile, Colombia, Mexico, Peru, and Uruguay) in his description of the data protection frameworks, as well as Carrillo and Jackson (2022), who included 20 countries, both with and without personal data protection laws. Furthermore, more countries had approved personal data protection laws since the publication of these studies, such as Belize, and this article extended the analysis to several Caribbean countries, such as Cuba, Dominican Republic, Haiti, and Trinidad & Tobago. This work then expands upon prior literature, first by including the information for all of the countries in the LAC region and then by adopting an exploratory and data-driven strategy to identify the main points of divergence in data protection laws without the constraints of prior theoretical work.

Following this process, I created a new matrix to identify the commitment of data protection laws in the LAC region. I used relevant differences between the laws in the region to categorize each law by the level of commitment for that variable. I then added the numbers to obtain a score of each law's commitment to data protection. Finally, I created a map showing the variation over the region in data protection laws.

Common threads in personal data protection in the region

Definitions of personal data and other types of data

As previously stated, not all countries in the LAC region had a law; this section will only refer to the countries that did have a law; the list is once again: Argentina, Belize, Brazil, Chile, Colombia, Costa Rica, Cuba, Dominican Republic, Ecuador, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, Trinidad and Tobago, and Uruguay.

First, the countries generally included an almost identical definition of personal data, understood as information or data that, by itself or combined with other data sources, either identified or could be used to identify a natural person. Legal entities were included in some cases, particularly in the Argentinian, Nicaraguan, Paraguayan, and Uruguayan cases. The laws mainly apply to data from citizens of the specific country or if the database handler is located geographically in the country.

A secondary, more restricted category, usually called sensitive personal data, was generally defined as data related to the most intimate sphere of the person and could lead to discrimination, particularly racial or ethnic origin, religious, philosophical, or political beliefs, union membership, health information, sexual orientation, and biometric data. Some countries presented somewhat unique innovations or extensions of this, such as Cuba with disability data, voice, and migratory condition, or the Dominican Republic with photographic data.

Regarding these interesting innovations, the Dominican Republic law defined personal data as "any numerical, alphabetical, graphical, photographic, acoustic, or any other type of information concerning identified or identifiable individuals.[1]" (*Ley Que Tiene Por Objeto La Protección Integral de Los Datos Personales Asentados En Archivos, Registros Públicos, Bancos de Datos u Otros Medios Técnicos de Tratamiento de Datos Destinados a Dar Informes, Sean Estos Públicos o Privados*, 2013, art. 6.9). The Cuban legislation included a longer list of protected personal data, which included but was not limited to

> gender, age, image, voice, identity, gender identity, sexual orientation, skin color, ethnic, national and territorial origin, migration status and classification, disability status, religious beliefs, political affiliation, marital status, address, medical or health data, economic-financial information, academic and educational records, professional and employment details, judicial and administrative information. (*Ley de Protección de Datos Personales*, 2022, art. 4)

This example from Cuba illustrates the omnibus-like nature of personal data in many of these laws. However, the Dominican Republic and Cuban examples also show foresight in defining personal data. This is becoming increasingly relevant given the development of generative artificial intelligence models potentially capable of using data such as voice or photographic data to generate so-called deep fakes, fake images or videos that appear realistic and portray a person doing something they never did (Appel & Prietzel, 2022; Vaccari & Chadwick, 2020).

In some instances, credit score data were given a particular relevance. Particularly for the Paraguayan law, it was the focal point of the law, which replaced a prior law that focused on personal data protection. Credit score data were also

Table 1. Commitment of personal data protection laws in the LAC region.

Country	Law	Year the law was approved	The focus is personal data protection	Government organization in charge of data	Resources given to the organization	Database registry	Consent
Argentina	*Ley de Proteccion de los Datos Personales, 25326*	2000	Yes	Yes, independent	Yes	Yes	Explicit
Belize	*Data Protection Act, 45*	2021	Yes	Yes, independent	Yes	No	Explicit
Brazil	*Provides for the Protection of Personal Data and Changes Law n. 12,965/2014 (Brazilian Civil Rights Framework for the Internet). 13709*	2018	Yes	Yes, independent	Yes	No	Explicit
Chile	*Ley Sobre Protección de la Vida Privada, 19628*	1999	Yes	No	No	No	Explicit
Colombia	*Ley Estatutaria, 1581*	2012	Yes	Yes, dependent	Yes	Yes	Explicit
Costa Rica	*Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, 8968*	2011	Yes	Yes, independent	Yes	Yes	Explicit
Cuba	Ley De Protección de Datos Personales, 149	2022	Yes	No	No	Yes	Explicit
Dominican Republic	*Ley Que Tiene Por Objeto La Protección Integral de Los Datos Personales, 172*	2013	No	No	No	Yes	Explicit
Ecuador	*Ley Orgánica de Protección de Datos Personales*	2021	Yes	Yes, independent	Yes	Yes	Implicit
Jamaica	*The Data Protection Act, 2020, 7*	2020	Yes	Yes, dependent	No	Yes	Explicit
Mexico	*Ley Federal de Protección de Datos Personales en Posesión de los Particulares*	2010	Yes	Yes, independent	Yes	No	Implicit
Nicaragua	*Ley de Protección de Datos Personales, 787*	2012	Yes	Yes, independent	Yes	Yes	Implicit
Panama	*Ley Sobre Protección de Datos Personales, 81*	2019	Yes	Yes, independent	Yes	No	Explicit
Paraguay	*Ley de Protección de Datos Personales Crediticios, 6534*	2020	No	No	No	No	Explicit
Peru	*Ley de Protección de Datos Personales, 29733*	2011	Yes	Yes, dependent	Yes	Yes	Explicit
Trinidad and Tobago	*Data Protection Act*	2011	Yes	Yes, independent	Yes	No	Explicit
Uruguay	*Ley de Protección de Datos Personales, 18331*	2008	Yes	Yes, independent	Yes	Yes	Explicit

significant for several other countries such as Nicaragua (*Ley de Protección de Datos Personales*, 2012, art. 3.g), and also Costa Rica, where the law defined credit data as one of four types of personal data. Here it states:

> The data related to credit behavior will be governed by the regulations that oversee the National Financial System, allowing for the assurance of an acceptable level of risk for financial entities, without hindering the full exercise of the right to informational self-determination, nor exceeding the limits set by this law. (*Ley de Protección de La Persona Frente Al Tratamiento de Sus Datos Personales*, 2011, art. 9.4)

The same holds for Ecuador, where several articles of its law are dedicated to these types of data (*Ley Orgánica de Protección de Datos Personales*, 2021, arts. 4, 28–29). In the Dominican Republic, more than 50% of the law focused entirely on credit score data and *Sociedades de Información Crediticia*, credit scoring agencies.

There were also cases in which specific sub-sets of personal data were given more of a focus. For example, for the case of disabled people data, the laws from Ecuador (*Ley Orgánica de Protección de Datos Personales*, 2021, art. 25.d) and Cuba (*Ley de Protección de Datos Personales*, 2022, art. 4, 14–15); Ecuador again with deceased people data (*Ley Orgánica de Protección de Datos Personales*, 2021, art. 27); or on-line data collection, as it was the case with Peru (*Ley de Protección de Datos Personales*, 2011, art. 18).

Protected rights in personal data protection laws

Discussing all the cases in the study more broadly, a series of rights considered in the reviewed data protection laws

included informed consent. Although there was variation regarding whether consent must be written and explicit for personal data, these two conditions are generally required if the data being collected is sensitive. However, consent could be revoked at any moment without retroactive effect in most cases.

Other provisions included the right to ask during or after the data collection for information about the data, including the goals, the type of treatment, and what particular data have been collected on an individual. This information must be given in plain language or in an easy-to-read format if digitalized. There were clear deadlines for the information to be given and mechanisms for demanding it if it is not provided.

There were also provisions regarding the obligatory correction, destruction, or blocking (that is, not using) data that could be erroneous, and the illegality of using such data or even non-erroneous data on forecasting that could lead to decisions that might discriminate against the person. Furthermore, in the case of personal data that was not anonymized, it was required to eliminate the variables that allowed the identification of individuals.

Excluded data from the data protection laws

Several exclusions were presented to the cases to which the law applied, particularly regarding private, personal databases, databases maintained for journalism, as it was in the case of the Jamaican law (*Data Protection Act*, 2020, art. 36. a), or for statistical, historical or scientific research for Nicaragua, Ecuador and Jamaica (In order, *Ley de Protección de Datos Personales*, 2012, art. 27; *Ley Orgánica de Protección de Datos Personales*, 2021, art. 26. f; *Data Protection Act*, 2020, art. 37). Exceptions were also usually given to the military as were the case for Nicaragua and the Dominican Republic (*Ley de Protección de Datos Personales*, 2012, art. 24; *Ley Que Tiene Por Objeto La Protección Integral de Los Datos Personales Asentados En Archivos, Registros Públicos, Bancos de Datos u Otros Medios Técnicos de Tratamiento de Datos Destinados a Dar Informes, Sean Estos Públicos o Privados*, 2013, art. 40), or for the databases of judicial and law and order agencies. Some examples of this last type, but not the only ones, included the cases of Costa Rica, Panama, Colombia, and Peru (in order, *Ley de Protección de La Persona Frente Al Tratamiento de Sus Datos Personales*, 2011, art. 1.c; *Ley Sobre Protección de Datos Personales*, 2019, art. 11; *Ley Estatutaria de Protección de Datos Personales*, 2012, art. 6.d; *Ley de Protección de Datos Personales*, 2011, art. 27). The logic also applied to administrative data collection for the correct functioning of the bureaucracy, for example, in the cases of Panama and Brazil (*Ley Sobre Protección de Datos Personales*, 2019, arts. 8.2, 23, 33.7; *Provides for the Protection of Personal Data and Changes Law n. 12,965/2014 (Brazilian Civil Rights Framework for the internet*), 2018, art. 11. b,d).

In some cases, organizations such as unions or churches were allowed to collect some sensitive data of their members for internal processes, as with Nicaragua and Colombia (*Ley de Protección de Datos Personales*, 2012; *Ley Estatutaria de Protección de Datos Personales*, 2012, art. 5.c). The same applied to particular cases regarding health care, business contracts, or incarceration data (Consider the cases of Nicaragua, Uruguay, and Argentina. *Ley de Protección de Datos Personales*, 2008, arts. 18, 19; *Ley de Protección de Datos Personales, 2012*, arts. 8.a-b, d; *Ley Protección de Los Datos Personales*, 2000, arts. 7.4, 8), but always only inside the scope of data related to that domain.

For examples of that domain restriction, consider the wording of article 8 of the Argentinian law regarding health care data:

> Public or private healthcare establishments and professionals associated with health sciences may collect and process personal data related to the physical or mental health of patients who visit them or who are or have been under their treatment, respecting the principles of professional secrecy.

Likewise, article 7.4 states "data relating to criminal or contravention records may only be processed by competent public authorities within the framework of the respective laws and regulations," again limiting the use of the data to relevant bureaus.

Clarification is needed in several observed similarities, such as the definition of personal data, sensitive personal data, or which types of data are included in these categories. The definitions varied slightly in all of these cases. Because different countries and lawmakers created different laws, it would be implausible that all the laws would have the exact definition up to punctuation marks for any of these concepts. The relevant issue, however, is that most personal data definitions are functionally equivalent, for example that they are close enough to see a general, shared understanding of these concepts between the different countries. As such, the slight variations would do little to affect the commitment to data protection, but they are valuable for the thick description of the legislation, which is a goal of this article.

Continuing with the idea of thick description, it is helpful to highlight the cases of innovations or interesting deviations that could indicate trailblazing or first movers in data protection legislation. Ultimately, the outlier cases in both directions did not amount to clear subregional patterns inside of the LAC region, such as similarities between Central American countries or Southern Cone countries. This could only be discovered by thoroughly comparing the slight variations in the commonalities. Added to this, the process helped identify relevant differences between the laws of each country, for example, the fact that some statutes did not focus on personal data protection, but rather only on credit scores. The same applies to the fact that personal data protection was singled out in some cases and that the informed consent

concept presented variations, which informs one of the categories in the following section.

Variation in the commitment to personal data protection in data protection laws

For this section, I focus on the differences between the data protection laws in the LAC region, particularly in those conditions that would play a role in strengthening or weakening the legal and operational framework for offering protection to personal data. The categories are chosen as they emerged in the thematic analysis's iterative and interpretative process as the notable differences between the different laws. The first condition was the existence of a law focused on personal data protection. Other conditions are how long the law has existed, whether the focus was personal data protection, the creation of an independent or a dependent government organization in charge of personal data protection, whether such an organization had monetary and legal resources to fulfill its duties, and whether there was a registry of databases. The last column referred to whether consent was explicit or implicit when collecting personal data. Explicit consent means that the person actively and explicitly affirms that they desire to share their data freely. In contrast, implicit consent implies that giving the data means citizens consent to sharing it. All of these categories, as stated before, come from the repeated reading of the laws and the identification that, instead of being virtually equivalent in these features, the laws varied considerably in these categories. Table 1[2] includes the relevant information.

The different government organizations in charge of personal data protection could have many names, including being a unit, a bureau, an institute, a directorate, or an agency, but the main difference was whether this was an autonomous organization inside the government that could act by itself and had access to its own resources, or whether it was just a part of a ministry or other part of the government that controls it and limits its independence. When I used "resources given to the organization," I meant both material resources, but specifically, whether the organization had the legal capability to engage in a series of actions to promote personal data protection in the country, as well as if the organization had the legal ability to impose penalties on those who break the law.

Some of the activities that data protection agencies could engage in included educating the public on personal data protection, proactively making sure that the dispositions of the law were being followed and sanctions when they were not, dealing with claims of particulars when their personal data rights were being broken, creating reports for the government as well as research regarding personal data protection. An essential duty, which I included as a separate variable, was whether there was a registry of databases in the country, which is handled by the data protection authority. In some cases, there were registries, but they were not managed by a specific institution (such as Cuba), or there was no particular institution, but some sanctions and duties specified otherwise, as was the case with the Dominican Republic. Finally, the last column focuses on consent for personal data collection, which can be either explicit or implicit.

In Table 2, I reproduced Table 1, but assigned different scores based on each variable's commitment to data protection for each law. Even if the final goal of the coding is additive, the values themselves were merely ordinal. By this, I mean this is not an "objective" measure of commitment, but somewhat relative; what matters is that a higher number is always above a lower number in the pointing system; that is, 2 is bigger than 1 and therefore stronger, and 1 is bigger than 0 and thus stronger. However, the numbers do not display the property of consistent intervals between consecutive numbers; a 2 is not twice as strong as a 1. Furthermore, the numbers should not be interpreted as a particular category having more relevance than another in assigning the level of commitment. Ultimately, this assignment of ordinal values was enough to describe a relationship between the level of commitment between the two countries' legislation and is the same logic used to assign utility to actors in formal theory.

For the existence of a law, I assigned 0 if no law existed, and I assigned a 1 if there was a data protection law. As stated before in this document, I followed the logic that the existence of *de jure* protection was a minimum for the other instances of commitment in data protection laws. There was no commitment to personal data protection if no personal data protection law existed.

For years, I assign 0 if there was no law, 1 if it was created in or after 2015, and 2 if it was made before that year, following the logic that the country had shown more interest and for a more extended period on devising legislation that would protect the personal data of its citizens. The intended concept to be captured here was: How long had the country been interested in personal data protection? This shows an interest in the issue from the legislature and proactivity in being early adapters of robust personal data protection frameworks, including countries identified by Carrillo and Jackson (2022) that adopted GDPR-influenced legislation or countries that passed data protection legislation before.

For focus of the law and whether resources are given to a data protection agency, I assigned 1 if yes and 0 otherwise. More explicitly, if the law focused throughout in its articles on the protection of the general category of "personal data," I assigned a 1. Instead, if the law did not focus on any article on the general category of "personal data," and instead focuses throughout on a concrete category, such as "credit scores," I assigned a 0. Likewise, for the data protection agency condition, I assigned a 1 if the law had at least one explicit article creating a data protection agency, and 0 if there were none. A law that did not focus on personal data protection, for example, the ones centered around credit data, would ignore or not cover other aspects of personal data, such as health care data, union membership, image, and so on. Resources were also crucial for the data protection

Table 2. Assignment of scores for commitment of personal data protection laws in the LAC region.

Country	Law	Year the law was approved	The focus is personal data protection	Government organization in charge of data	Resources given to the organization	Database registry	Consent	Commitment of personal data protection law
Argentina	1	2	1	2	1	1	1	9
Belize	1	1	1	2	1	0	1	7
Bolivia	0	0	0	0	0	0	0	0
Brazil	1	1	1	2	1	0	1	7
Chile	1	2	1	0	0	0	1	5
Colombia	1	2	1	1	1	1	1	8
Costa Rica	1	2	1	2	1	1	1	9
Cuba	1	1	1	0	0	1	1	5
Dominican Republic	1	2	0	0	0	1	1	5
Ecuador	1	1	1	2	1	1	0	7
El Salvador	0	0	0	0	0	0	0	0
Guatemala	0	0	0	0	0	0	0	0
Guyana	0	0	0	0	0	0	0	0
Haiti	0	0	0	0	0	0	0	0
Honduras	0	0	0	0	0	0	0	0
Jamaica	1	1	1	1	0	1	1	6
Mexico	1	2	1	2	1	0	0	7
Nicaragua	1	2	1	2	1	1	0	8
Panama	1	1	1	2	1	0	1	7
Paraguay	1	1	0	0	0	0	1	3
Peru	1	2	1	1	1	1	1	8
Suriname	0	0	0	0	0	0	0	0
Trinidad and Tobago	1	2	1	2	1	0	1	8
Uruguay	1	2	1	2	1	1	1	9
Venezuela	0	0	0	0	0	0	0	0

agency, as it could not fulfill its function without them. Even if resources were not allotted in practice when the law states that they should, this was unlike the situation in which the law does not even state that they should be allotted.

For the existence of a database registry and whether consent was explicit, I also assigned 1 for a yes and 0 otherwise. In a similar logic to the previously explained conditions, if there is at least a single article in the law ordering the creation of a database registry, the coding is 1, while if there is no such article, the coding is 0. For explicit consent, if the text of the law stated in the corresponding article that the consent had to be explicit, I coded as 1; if the text of the law did not include any article mentioning explicit consent, I coded as 0. Database registries were considered something that led to stronger laws because it meant that the government would at least hold some level of oversight over private and commercial databases. Finally, explicit consent requires an act of the individual to opt in to share their data, which means that they would have more control over the decision than if they did not have to engage in an explicit act of acceptance.

For the personal data protection organization, I assigned 0 if there was no organization, 1 if there was one dependent on another government organization, and 2 if it was independent. Like all the other categories, this coding depends on what is explicitly stated in the articles of the respective data protection law: if the law has a single article creating a new government organization that has independence from any already existing ones I coded it as 2, instead if there is at least a single article creating an organization that is dependent to an already existing government organization I coded as 1. If no article in the law creates an oversight organization, the coding was 0. The idea here was that independent organizations would better resist any form of pressure from any government branches that might potentially weaken personal data protection. This was important, as the laws should protect both from the abuse of private, commercial databases (as with the registry) and from government agencies.

To visualize better the variation, I used geographical polygons from the Global Administrative Areas Database (n.d.) and the programming language for statistical analysis R to create Figure 1, a map of the LAC region showing the commitment to data protection laws.

As can be seen, excluding the countries with no data protection laws at all, most countries arrived at least at a minimum level of 5 in their data protection. The countries that appeared entirely purple, such as Bolivia, El Salvador, Guatemala, Guyana, Haiti, Honduras, Suriname, and Venezuela, were those with no personal data protection laws.

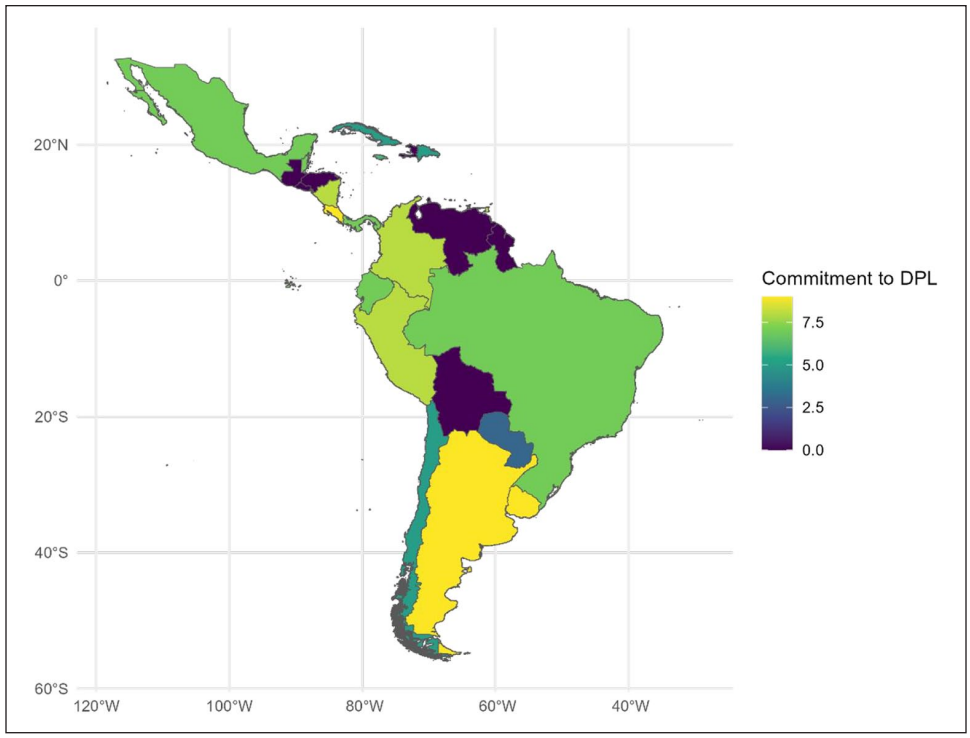

Figure 1. Map of the LAC region showing the commitment to data protection laws.

Following them was Paraguay scoring barely 3, followed by countries with only 5 points on the scale, such as Cuba, which delegated all data protection to a ministry instead of an independent body.

Jamaica was barely better at 6 points; however, most countries were clustered around 7 on the scale after that point. Then the countries started to get the highest scores; Colombia, Nicaragua, Peru, and Trinidad and Tobago had an 8, while Argentina, Costa Rica, and Uruguay scored the highest commitment to personal data protection in their data protection laws, a 9.

Discussion

With the increase in size and broadness of databases with individuals' data and the increase in the capacity to extract new information and analyze such big data sets, protecting personal data has become an essential political problem throughout the world. The insights coming from personal data analysis can be used for political manipulation, appropriate policy choices based on facts, decisions that affect people's life prospects, such as with loan denials due to credit scores, or revelations about sensitive data such as sexual orientation or health records (Narayanan & Shmatikov, 2008; Robertson et al., 2016; L. Sweeney, 2002).

Latin American and Caribbean countries are not immune to these developments. The diffusion of modern technology and its use for trade and other economic actions have made it so that regional governments must contend with these realities. Throughout the region, international frameworks have influenced the adoption of different personal data protection laws (Carrillo & Jackson, 2022; Lehuedé, 2019).

In this project, I adopted an inductive thematic analysis approach (Braun & Clarke, 2006; Maguire & Delahunt, 2017). For 25 countries in the LAC region, I collected each country's respective personal data protection law in which one had been approved. I read every law in an iterative process, creating a qualitative matrix contrasting the laws regarding similarities and differences. That matrix informed two sections, the first described the common threads through the region, and then a second section identified variations in the commitment to data protection in the data protection laws. This second section included a second matrix that I created of those variables that are relevant for the commitment of the laws, which were then used to generate a score of commitment for each law per country, which was then used to create a map that showed the commitment to data protection in the personal data protection laws in the LAC region.

As can be seen from the section comparing the commitment of the different personal data protection laws in the region, there were many points in common and similarities between the laws, particularly when it comes to similarities in the definition of personal data, sensitive data and other special categories, as well as the common presence of ARCO rights in the bills. There are clear, interesting innovations in extending protection to "new" data types, such as biometric ones. At the same time, there was no clear subregional pattern regarding their commitment, which derives from

differences in how long a country has had a data protection law, the existence of a government agency in charge of it and how powerful it is, and the other variables in Tables 1 and 2. The Southern Cone might be considered to have stronger laws; however, Paraguay was one of the countries with no law specifically focused on the broad area of personal data protection, and while Central America and the Caribbean could be thought of as being comparatively weaker, there were still cases of robust frameworks, such as with Costa Rica and Nicaragua.

Considering how recent some of the laws are, it was evident that there was a pattern toward adopting some measurement of personal data protection, in part due to the commercial pressures of the European Union, that is, the previously mentioned "Brussels effect" (Bradford, 2012). In the long term, this presents an opportunity to adhere more strictly to the European framework alongside learning and adapting the most developed laws in the region. This would be advantageous considering the strong stance on the protection of the European framework; although a danger would be to ignore the specificities and particular needs of the LAC context, such as with different values regarding informal economies and piracy (Goldgel-Carballo & Poblete, 2020) or regarding more communal rather than individually oriented views on rights of Indigenous populations—again considering property rights (Nwauche, 2015). These examples are tangential but related to personal data, and more importantly, these cross-cultural differences in values should be considered to avoid erroneously turning the European standard into a gold one.

At the same time, looking at the similarities and differences, it is clear that there is quite a thorough extension of the data that should be protected, and the variation has more to do with the capabilities given by the legislation to protect it. In other words, the creativity and thoroughness of the legislators play an important part role regarding what innovations will appear in extending protection to new types of data; it could be the case that in the future, the references and mutual influences between the legislation of different countries in the LAC region would lead to innovations spreading through imitation, as was the case with *habeas data*.

One of the reasons this topic appears relevant is that citizens are constantly generating an enormous amount of digital trace data, of which a considerable percentage is being produced using social media networks. Political and commercial actors know that these spaces are ripe for data collection and, later, analysis for different goals (Brown, 2020; Udupa, 2024). Even though people opt-in to use these networks and publicly share their data there, this does not mean they opt-in to have that data analyzed in such a fashion. It is even more so the case when the analysis can be used to target the citizens in ways that are damaging to them. An example previously mentioned in the text is the use of micro-targeting by political campaigns that support public policy positions that individuals might not usually support (Brown, 2020; Udupa, 2024). A further example was the use of machine learning models to predict undisclosed characteristics (Narayanan & Shmatikov, 2008; L. Sweeney, 2002), which could then lead to discrimination against the individuals (King & Mrkonich, 2016).

A robust framework of personal data protection laws can be a tool for individuals to maintain, or regain, control over their data and stop it from being used for goals such as the ones just presented, but also for other cases that might be less technologically complex, such as avoiding being included in a campaign propaganda database. Having a data protection agency to which citizens can go to to demand that an actor that has their data tells them which data they have is vital for being able to exercise this control. It is also crucial that the organization has funding and that there are adequate legal processes for making sure that private and public databases comply with sharing the data with the subject, as well as comply with other rights such as rectifying wrong information or deleting data that the subject does not want to share.

Aside from explicitly nefarious uses, the personal data protection framework is also relevant for the use of digital trace data generated through social media concerning scientific research that can depend on this type of data and the potential benefits that such research can bring (Bruns, 2019, 2020; de Vreese & Tromble, 2023; Ohme et al., 2024). Some examples were already mentioned earlier in this article, regarding the COVID-19 pandemic, but public health policy is only one area that can benefit from insights obtained through digital trace data. Some of the legislation, such as the Nicaraguan, Ecuadorian, or Jamaican ones, protected and gave guidelines for the use of personal data for research purposes. For example, the collected data and the analysis must be appropriate for the goal of the research, the data must be previously anonymized, and the data must not be used to target specific individuals, nor damage them in any substantial way. Clear guidance with regards to what data can and cannot be used in research is essential both to protect citizens from unexpected negative consequences but also to reap the benefits of such research.

Discussion regarding both the benefits and potential dangers of data mining and how data protection laws can potentiate the former and mitigate the latter cannot be blind to the power imbalances inherent to the fact that private corporations develop most social media platforms in the global north. This discussion has two angles: One focuses on WEIRD (Western, educated, industrialized, rich, and democratic) versus non-WEIRD countries (Masur et al., 2024), and the other focuses on private versus public censorship (Messina, 2023), or, to be more precise, private versus public control over access to personal data as it can be mined from social media.

Regarding the first angle, the WEIRD label effectively works as a synonym of the United States and Western Europe, adding perhaps some other Anglo countries such as Canada and Australia or, in short, the global north. This would exclude the LAC region, regardless of whether countries in LAC are indeed Western, industrialized, or democracies. As such, most of the platforms were developed for the use of the WEIRD public and with the interests of agents from WEIRD

countries in mind, which means that the data protection laws have a limit or disadvantage due to geopolitical power imbalances, something that is itself replicated in the research on data protection laws (Arora, 2019; Henrich et al., 2010). This, of course, does not mean that all the WEIRD countries see eye-to-eye regarding data protection laws (as, indeed, the United States and the European Union do not). Still, instead, it highlights that the platforms in which personal data can be collected are created and regulated with the WEIRD countries' views in mind, not to mention that these countries can set the pace regarding how much and which type of data protection they prefer, due to the imbalance in economic, and therefore, negotiating power.

In many cases, the agents will be private companies focused on profit-maximizing, which could potentially be obstructed by private data protection. An example can be seen in the conflicts between Elon Musk, the owner of Twitter, and the Brazilian Supreme Court (Pessoa & Ortutay, 2024). While this conflict is centered around the sharing of misinformation and not access to personal data per se, it underlines the power of a social media mogul to antagonize democratically appointed judges and the legal framework of a country, reminiscent of the time Musk tweeted that the United States could coup whichever country it wanted in reference to Bolivia (S. Sweeney, 2020).

The laws represent an important first step, but they are not the final step in data protection. This article focuses on that first step regarding personal data protection; however, this step alone would not be effective without the resources and political will to implement adequate data protection measures. The next phase of this research agenda would involve measuring other elements of data protection effectiveness, including collecting data on various resources, such as the allocated budget, bureaucratic capacity, and others. It would also involve identifying the goals and outcomes of broader data protection policies and assessing whether these goals are achieved. These goals can then be linked to the resources using regression methods to determine the weight and significance of each potential resource in effectively achieving data protection policy objectives.

Acknowledgements

The author would like to thank Katie M. Angell, the editors of the special Social Media + Society issue on "Comparative Approaches to Studying Privacy: Opening Up New Perspectives," and the anonymous reviewers for their constructive comments, which strengthened the paper.

ORCID iD

Elías Chavarría-Mora https://orcid.org/0000-0001-6424-3915

Ethical Considerations

This research did not require ethical approval statement, as it used observational data that had been previously collected.

Consent to Participate

This research did not require a patient consent statement.

Funding

The author received no financial support for the research, authorship, and/or publication of this article.

Declaration of Conflicting Interests

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Notes

1. In Spanish in the original. Translated by the author. All other citations from law originally in Spanish are also translated by the author.
2. The following countries did not have a law: Bolivia, El Salvador (A law was originally approved by Congress but vetoed by President Bukele), Guatemala, Guyana, Haiti, Honduras, Suriname, and Venezuela. The Dominican Republic is coded as not having a government organization in charge of data. However, it does have an organization specifically for credit data, the *Superintendencia de Bancos*, which receives funding. Still, I do not consider it a positive case due to the limited nature of its domain of action. Similarly, Paraguay has a dependent institution established for this goal but with a scope limited exclusively to credit score-related data

References

Alanoca, S., Guetta-Jeanrenaud, N., Ferrari, I., Weinberg, N., Çetin, R. B., & Miailhe, N. (2021). Digital contact tracing against COVID-19: A governance framework to build trust. *International Data Privacy Law*, *11*(1), 3–17. https://doi.org/10.1093/idpl/ipab001

Appel, M., & Prietzel, F. (2022). The detection of political deepfakes. *Journal of Computer-Mediated Communication*, *27*(4), zmac008. https://doi.org/10.1093/jcmc/zmac008

Arora, P. (2019). Decolonizing privacy studies. *Television & New Media*, *20*(4), 366–378. https://doi.org/10.1177/1527476418806092

Blades, N., & Herrera-González, F. (2016). An economic analysis of personal data protection obligations in the European Union. In *27th European Regional Conference of the International Telecommunications Society (ITS): "The Evolution of the North-South Telecommunications Divide: The Role for Europe."* https://hdl.handle.net/10419/148661%0AStandard-Nutzungsbedingungen

Bradford, A. (2012). The Brussels effect. *Northwestern University Law Review*, *107*(1), 1–68.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brown, A. J. (2020). "Should I stay or should I leave?": Exploring (dis)continued Facebook use after the Cambridge Analytica scandal. *Social Media + Society*, *6*(1). https://doi.org/10.1177/2056305120913884

Bruns, A. (2019). After the 'APIcalypse': Social media platforms and their fight against critical scholarly research. *Information*

Communication and Society, *22*(11), 1544–1566. https://doi.org/10.1080/1369118X.2019.1637447

Bruns, A. (2020). Big social data approaches in internet studies: The case of Twitter. In *Second international handbook of internet research* (pp. 65–81). Springer. https://doi.org/10.1007/978-94-024-1555-1_3

Calderon, A., Gonzales, S., & Ruiz, A. (2021). Privacy, personal data protection, and freedom of expression under quarantine? The Peruvian experience. *International Data Privacy Law*, *11*(1), 48–62. https://doi.org/10.1093/idpl/ipab003

Carrillo, A. J., & Jackson, M. (2022). Follow the leader? A comparative law study of the EU's General Data Protection Regulation's impact in Latin America. *ICL Journal*, *16*(2), 177–262. https://doi.org/10.1515/icl-2021-0037

Chandra, S., Ray, S., & Goswami, R. T. (2017). Big data security in healthcare: Survey on frameworks and algorithms. In *2017 IEEE 7th International Advance Computing Conference (IACC)* (pp. 89–94). https://doi.org/10.1109/IACC.2017.0033

Data Protection Act. (2011). (testimony of Parliament of Trinidad and Tobago). https://agla.gov.tt/downloads/laws/22.04.pdf

Data Protection Act. (2020). (testimony of Parliament of Jamaica). https://japarliament.gov.jm/attachments/article/339/TheDataProtectionAct,2020.pdf

Data Protection Act. (2021). (testimony of National Assembly of Belize). https://www.nationalassembly.gov.bz/wp-content/uploads/2021/12/Act-No-45-of-2021-Data-Protection-Act.pdf

de Vreese, C., & Tromble, R. (2023). The data abyss: How lack of data access leaves research and society in the dark. *Political Communication*, *40*(3), 356–360. https://doi.org/10.1080/10584609.2023.2207488

Global Administrative Areas Database. (n.d.). *GADM data version 3.6 Accesado: 23 Abril, 2021*. https://gadm.org/download_country_v3.html

Goldgel-Carballo, V., & Poblete, J. (2020). *Piracy and intellectual property in Latin America*. Routledge. https://doi.org/10.4324/9780367823955

Guadamuz, A. (2001). Habeas data vs. the European data protection directive. *Journal of Information, Law & Technology*, *3*.

Henrich, J., Heine, S. J., & Norenzayan, A. (2010). Most people are not WEIRD. *Nature*, *466*(7302), 29–29. https://doi.org/10.1038/466029a

Jirovský, V., Pastorek, A., Mühlhäuser, M., & Tundis, A. (2018). Cybercrime and organized crime. In *Proceedings of the 13th International Conference on Availability, Reliability and Security* (pp. 1–5). https://doi.org/10.1145/3230833.3233288

King, A. G., & Mrkonich, M. (2016). "Big data" and the risk of employment discrimination. *Oklahoma Law Review*, *68*(3), 555–584.

Lehuedé, H. J. (2019). *Corporate governance and data protection in Latin America and the Caribbean*. https://repositorio.cepal.org/handle/11362/44629%0Ahttps://repositorio.cepal.org/bitstream/handle/11362/44629/S1900395_en.pdf?se

Le Lous, F. (2021, February 10). ¿Qué es el caso UPAD? Explicado en sencillo [What is the UPAD affair? Explained simply]. *La Nación*. https://www.nacion.com/blogs/el-explicador/la-upad-y-el-allanamiento-de-casa-presidencial/LGB253COXZG3PJK2G5SNVTPXSY/story/

Ley de Protección de Datos Personales, 18331. (2008). (testimony of Asamblea General de Uruguay). https://www.impo.com.uy/bases/leyes/18331-2008

Ley de Protección de Datos Personales, 29733. (2011). (testimony of Congreso de la República del Perú). http://www.pcm.gob.pe/transparencia/Resol_ministeriales/2011/ley-29733.pdf

Ley de Protección de Datos Personales, 787. (2012). (testimony of Asamblea Nacional de Nicaragua). http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/7bf684022fc4a2b406257ab70059d10f

Ley de Protección de Datos Personales, 149. (2022). (testimony of Asamblea Nacional del Poder Popular de la República de Cuba). https://www.gacetaoficial.gob.cu/sites/default/files/goc-2022-o90_0.pdf

Ley de Protección de Datos Personales Crediticios, 6534. (2020). (testimony of Congreso Nacional de la República del Paraguay). https://baselegal.com.py/docs/df321d5a-1de3-11eb-82fb-525400c761ca

Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, 8968 (2011) (testimony of Asamblea Legislativa de Costa Rica). https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989

Ley Estatutaria de Protección de Datos Personales, 1581 (2012) (testimony of Congreso de Colombia). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Ley Federal de Protección de Datos Personales en Posesión de los Particulares. (2010). (testimony of Congreso General de los Estados Unidos Mexicanos). http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Ley Orgánica de protección de datos personales. (2021). (testimony of Asamblea Nacional del Ecuador). https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf

Ley Protección de los Datos Personales, 25326. (2000). (testimony of Congreso Argentino). http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm

Ley que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados, 172. (2013). (testimony of Congreso Nacional de República Dominicana). https://www.sb.gob.do/regulacion/leyes/ley-no-172-13-proteccion-de-los-datos/

Ley Sobre Protección de Datos Personales, 81. (2019). (testimony of Asamblea Nacional de Panama). https://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/2010/2019/2019_645_3008.pdf

Ley Sobre Protecciónde la Vida Privada, 19628. (1999). (testimony of Congreso Nacional de Chile). https://www.bcn.cl/leychile/navegar?idNorma=141599&idParte=864270

Lode, S. L. (2019). "You have the data..".The writ of habeas data and other data protection rights: Is the United States falling behind? *Indiana Law Journal*, *94*(5), 41–63.

Maguire, M., & Delahunt, B. (2017). Doing thematic analysis: A practical, step-by-step guide for learning and teaching scholars. *All Ireland Journal of Higher Education*, *9*, 3351–33514. https://doi.org/10.62707/aishej.v9i3.335

Masur, P. K., Epstein, D., Quinn, K., Wilhelm, C., Baruh, L., & Lutz, C. (2024). Comparative privacy research: Literature review, framework, and research agenda. *SocArXiv*. https://doi.org/10.31235/osf.io/fjqhs

Messina, J. P. (2023). *Private censorship*. Oxford University Press. https://doi.org/10.1093/oso/9780197581902.001.0001

Moraes, T. G., Lemos, A. N. L. E., Lopes, A. K., Moura, C., & De Pereira, J. R. L. (2021). Open data on the COVID-19 pandemic: Anonymisation as a technical solution for transparency, privacy, and data protection. *International Data Privacy Law*, *11*(1), 32–47. https://doi.org/10.1093/idpl/ipaa025

Narayanan, A., & Shmatikov, V. (2008). Robust de-anonymization of large sparse datasets. In *Proceedings—IEEE Symposium on Security and Privacy* (pp. 111–125). https://doi.org/10.1109/SP.2008.33

Nwauche, E. S. (2015). The emerging right to communal intellectual property. *Marquette Intellectual Property Law Review*, *19*, 221.

Ohme, J., Araujo, T., Boeschoten, L., Freelon, D., Ram, N., Reeves, B. B., & Robinson, T. N. (2024). Digital trace data collection for social media effects research: APIs, data donation, and (screen) tracking. *Communication Methods and Measures*, *18*(2), 124–141. https://doi.org/10.1080/19312458.2023.2181319

Pessoa, G. S., & Ortutay, B. (2024, April 11). What to know about Elon Musk's "free speech" feud with a Brazilian judge. *Associated Press News*. https://apnews.com/article/brazil-musk-x-twitter-moraes-bef06c0dbbb8ed87495b1afbb0edf211

Piñeiro Rodríguez, R., Muñoz, P., Rosenblatt, F., Rossel, C., & Scrollini, F. (2022). Domestic isomorphic pressures in the design of FOI oversight institutions in Latin America. *Governance*, *35*(3), 827–845. https://doi.org/10.1111/gove.12614

Provides for the protection of personal data and changes Law n. 12,965/2014 (Brazilian Civil Rights Framework for the Internet), 1. (2018). (testimony of Congresso Nacional do Brasil). https://www.lgpdbrasil.com.br/lgpd-english-version/

Robertson, J., Riley, M., & Willis, A. (2016, March). How to hack an election. *Bloomberg Businessweek*. https://www.bloomberg.com/features/2016-how-to-hack-an-election/

Sadowski, J. (2019). When data is capital: Datafication, accumulation, and extraction. *Big Data and Society*, *6*(1), 1–12. https://doi.org/10.1177/2053951718820549

Salganik, M. J. (2019). *Bit by bit: Social research in the digital age*. Princeton University Press.

Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *10*(05), 557–570. https://doi.org/10.1142/S0218488502001648

Sweeney, S. (2020, July 27). After Bolivia, Elon Musk says capitalists can overthrow any government they want. *People's World*. https://www.peoplesworld.org/article/after-bolivia-elon-musk-says-capitalists-can-overthrow-any-government-they-want/

Udupa, S. (2024). Shadow politics: Commercial digital influencers, "data," and disinformation in India. *Social Media + Society*, *10*(1). https://doi.org/10.1177/20563051231224719

Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. *Social Media + Society*, *6*(1), 205630512090340. https://doi.org/10.1177/2056305120903408

Vladeck, D. C. (2016). Consumer protection in an era of big data analytics. *Ohio Northern University Law Review*, *42*(2), 493–516.

Wolfson, J. (2016). The expanding scope of human rights in a technological world—Using the Inter-American Court of Human Rights to establish a minimum data protection standard across Latin America. *University of Miami Inter-American Law Review*, *48*(3), 188–232.

Author biography

Elías Chavarría-Mora, (MA, University of Pittsburgh) is a PhD candidate at the University of Pittsburgh, and a lecturer at the Universidad de Costa Rica. His research interests include the use of social media for electoral campaigning, party competition, and protest politics.