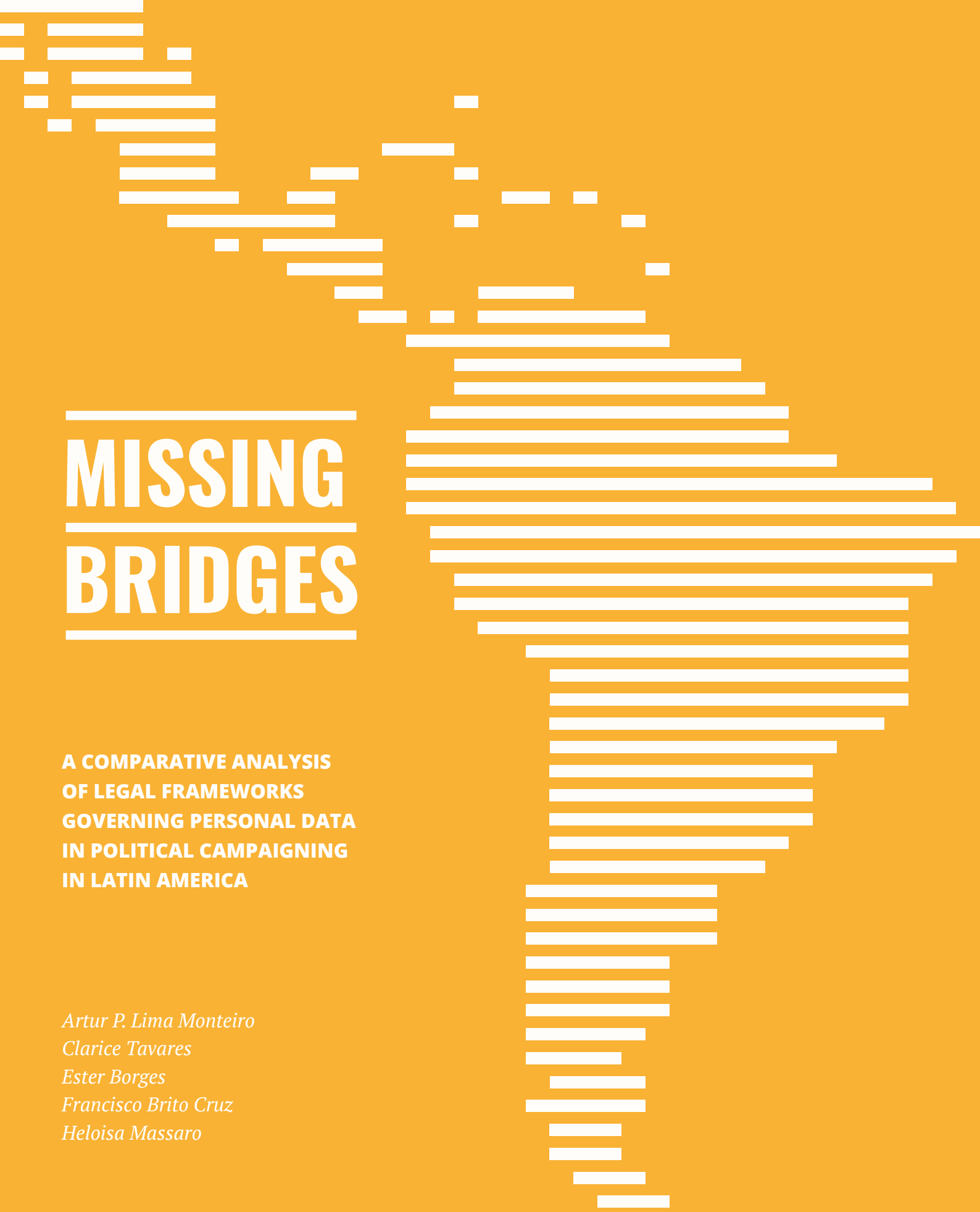

MISSING BRIDGES

A COMPARATIVE ANALYSIS OF LEGAL FRAMEWORKS GOVERNING PERSONAL DATA IN POLITICAL CAMPAIGNING IN LATIN AMERICA

Artur P. Lima Monteiro
Clarice Tavares
Ester Borges
Francisco Brito Cruz
Heloisa Massaro

INTERNETLAB

CYRILLA

MISSING BRIDGES

A COMPARATIVE ANALYSIS OF LEGAL FRAMEWORKS GOVERNING PERSONAL DATA IN POLITICAL CAMPAIGNING IN LATIN AMERICA

This work is licensed under a Creative Commons Attribution 4.0 International License.

This license allows reusers to distribute, remix, adapt, and build upon the material in any medium or format, so long as attribution is given to the creator. The license allows for commercial use.

LICENSE

https://creativecommons.org/licenses/by/4.0/legalcode

SUGGESTED CITATION

Monteiro, A. P. L., Tavares, C, Borges, E., Brito Cruz, F., & Massaro, H. (2021). Missing bridges: a comparative analysis of legal frameworks governing personal data in political campaigning in Latin America. São Paulo, InternetLab.

INTERNETLAB

ABOUT US

InternetLab is a Brazilian internet policy think tank that works towards building the intellectual and evidential foundation for public awareness, action, and policy-making, by delivering sophisticated evidence-based and impact-oriented social and legal research, as well as analysis to identify and clarify critical issues.

PROJECT TEAM

Researchers
Clarice Tavares and Ester Borges

Head of Research, Freedom of Expression
Artur Péricles Lima Monteiro

Head of Research, Information and Politics
Heloisa Massaro

Director
Francisco Brito Cruz

Communications Coordinator
Karina Oliveira

Design by
Sergio Berkenbrock dos Santos

Supported by

CYRILLA

INDEX

EXECUTIVE SUMMARY

Recent elections have been plagued by allegations of voter manipulation and abuse of personal data, particularly with reports of the involvement of the infamous Cambridge Analytica going much beyond the 2016 US presidential elections. Regardless of the actual results of that and other digital strategies adopted by campaigns, they present questions related to the legitimacy of the outcomes of elections and the appropriate regulation of electoral advertising in networked societies. This report adds to those discussions by mapping the legal landscape governing the use of personal data in electoral campaigning of six Latin American countries: Argentina, Brazil, Colombia, Chile, Mexico and Paraguay.

Informed by the analyses of legal documents and by interviews with civil society experts in each country, our comparative approach seeks to understand the context of personal data use by electoral campaigns in those countries and looks to the framework around both elections law and data protection legislation. We examine how elections are regulated, who is the electoral management body, and whether there are specific provisions around data processing by campaigns. We also inspect data protection provisions and how they have been articulated for the electoral context regarding rulemaking and guidance. We further explore enforcement action in connection to the use of personal data in elections.

What we find is a diverse field. Higher rates of internet access are generally linked with how relevant digital strategies are considered. Uses and abuses of personal data in digital campaigning have been more prominently discussed in Argentina, Brazil and Colombia, where there has been some response in terms of either legislation, regulation or official guidelines. However, even where there has been some action, the extent and impact of these campaign practices remain obscure — in fact, there is little transparency about what those practices have been beyond reporting by newspapers.

While the presence of data protection legislation is a starting point, its proper enforcement during electoral periods depends on a yet to produce comprehensive regulation that addresses the features of the digital campaign strategies adopted in the region. This is as true of Brazil, with its General Data Protection Law (*Lei Geral de Proteção de Dados*, *LGPD*) entering into effect in 2020, as it is of Chile, the data protection pioneer in the region — and it is certainly also true of Paraguay, which still lacks a data protection law. With episodic exceptions, data protection authorities and elections management bodies have been at most timid

and at worst silent about personal data use by electoral campaigns. In Argentina, Chile and Mexico, not only are electoral authorities not leveraging data protection law to ensure elections are fair, but the reverse has happened: transparency requirements around voter rolls (*padrones electorales*) are seen as exposing excessive personal data from voters and creating opportunities for abuse, both by campaigns and other actors, including those unconnected to elections, for commercial use.

Our study finds authorities generally face three challenges:

- a lack of coordination by electoral and data protection authorities, leading to neither regarding itself as responsible;

- concerns over the independence of authorities that lack autonomy from the executive or partisan politics, leading to distrust of their capacity to apply data protection law without compromising competition between candidates and parties and, finally,

- a serious lack of information about campaign use of personal data and the role of data in digital campaigning — transparency requirements, where present, are limited to expenditures and official account registration.

With campaigns increasingly adopting digital strategies, data protection is key to ensuring that the electoral process is fair. New tools available to candidates and parties enable them to make their message more relevant to the electorate, and also have the potential to empower candidates, particularly those with limited resources to be more efficient in campaign spending. At the same time, the employment of these tools may pose risks both in terms of voter manipulation and privacy violations, besides threatening the integrity of electoral process.

Data protection experts and officials and their electoral counterparts must engage with each other to respond to those questions. Regulation should not adopt necessarily the most restrictive available option for data processing, nor should it allow a personal data free-for-all. The former might hinder the communication between candidates and voters, besides precluding opportunities for making electoral contests more amenable to entrants standing for interests that have been downplayed in the political arena, as well as underrepresented segments of the population. The latter is harmful in and of itself, and it is also capable of undermining the legitimacy of the electoral process. Even when digital campaigns are not seen as decisive in determining winners and losers, uncertainty about whether practices are legal can hurt trust in elections and compromise the level playing field. The regulation of campaign data as such must be thought of as building bridges, an issue pertaining both to privacy and to making sure elections are open and fair.

INTRODUCTION

In October 2018, ahead of the second round of national elections in Brazil, a major newspaper published an investigation on bulk messaging services hired by Jair Bolsonaro's supporters to send political messages on WhatsApp.[1] Along with debates on the spread of disinformation on social media during the electoral period, the revelations regarding the Brazilian elections joined a growing number of elections around the world plagued with allegations of voter manipulation and concerns about the lawfulness and the transparency of the digital marketing techniques employed by electoral campaigns. Seven months earlier, in March 2018, it had been revealed how Cambridge Analytica, a data analytics firm hired by US President Donald Trump's campaign, used personal data collected from Facebook to profile voters, customize political messages, and micro-target campaign advertisements.[2] Documents revealed later show that the Cambridge Analytica case was not restricted to the United States and the United Kingdom. There were reports of the company's services in Latin American countries, including Mexico, Colombia and Brazil.[3]

Those cases have raised concerns about the manipulation of electoral processes, and they are also examples of how political campaigns changed over time. The emergence of new information and communication technologies and the growing use of the internet and social media around the world transformed how we communicate. Consequently, the dynamics of political communication changed, leading to the development of new configurations of political campaigns.

It has already been argued that the internet favored the emergence of campaigns structured as networks of propaganda composed of both supporters and professional efforts.[4] At the same time, political campaigns incorporated new technologies and took advantage of a wide range of

1 MELLO, Patricia Campos. *Empresários bancam campanha contra o PT pelo WhatsApp*. Folha de S. Paulo, São Paulo, ano 98, nº 32.705, 18 out. 2018. Available at: folha.uol.com.br/poder/...

2 THE GUARDIAN. The Cambridge Analytica Files. Available in: theguardian.com/news...

3 GNIPPER, Patrícia. *Polêmica envolvendo o Facebook também afeta a América Latina*. Canal Tech. April 18, 2018. Available at: canaltech.com.br/...;
CADWALLADR, Carole. Fresh Cambridge Analytica leak 'shows global manipulation is out of control'. The Guardian. Jan. 4, 2020. Available at: theguardian.com/...

4 BRITO CRUZ, Francisco; VALENTE, Mariana Giorgetti. *É hora de se debruçar sobre a propaganda em rede de Bolsonaro*. El País, 22 out. 2018. Available at: brasil.elpais.com/... ; BRITO CRUZ, F. C. *Definindo as regras do jogo: a regulação de campanhas políticas e a internet*. 2019. 380 pp. Thesis (Doctorate in Jurisprudence and Legal Theory) – Faculty of Law, University of São Paulo, São Paulo, 2019

new political marketing tools and techniques. Among those, the increasing capacity to collect, process, and store personal data has been one of the most prominent technological capabilities adopted by campaigns to pursue an even more personalized communication with voters.

Regardless of the impact those strategies had, both Cambridge Analytica's microtargeting strategies and the bulk messaging tools used during Brazilian elections relied on voters' personal data. Be it employed in a simple practice of sending messages to a list of email addresses or cell phone numbers, or in the most sophisticated profiling and microtargeting techniques, personal data has been a valuable asset to political campaigns. In Latin America, a series of country case studies conducted by local organizations examined the use of personal data and digital strategies by political campaigns in electoral processes between 2015 and 2018.[5] Those studies revealed a wide range of tactics and techniques adopted by political campaigns across the region. To a greater or lesser extent, microtargeting and voter profiling practices were recorded in many Latin American countries. Most cases involving digital campaigns reached the public only through media reports.

Those new techniques can add to the political debate by allowing candidates with limited resources to get their message across to smaller and more specific audiences and by making campaign communication more diverse and relevant to voters. At the same time, however, those techniques also pose risks to fundamental rights and democratic values, such as the risk of voter manipulation and violations of voters' privacy and data protection rights. This transformation, therefore, brings a regulatory question on how to deal with these new ways of campaigning. The challenge is to develop regulatory approaches that preserve citizens' rights and foster an authentic political debate.

A recent study by InternetLab emphasized the importance of a regulatory approach that establishes data protection guarantees and defines rules for the processing of personal data by political campaigns.[6] Bridging the gap between the legal framework governing electoral campaigns and data protection regimes is critical. In the Brazilian case, campaign strategies first seen in the 2018 elections collided with an electoral law designed for television campaigns, relying mainly on the removal of illegal content and the accountability of those responsible for it. At that time, the country did not have a data protection law in place, and the few rules in the electoral law addressing such issues were rather timid. Even with the General Data Protection Law, which was approved in 2018 and came into effect in 2020, the impact of a data protection framework for electoral practices remained unclear.[7]

5 The case studies conducted in Argentina, Brazil, Chile, Colombia and Mexico were part of a larger research organized by Tactical Tech. TACTICAL TECH. Personal Data: Political Persuasion Inside the Influence Industry. How it works. Tactical Tech, 2019. Available in: cdn.ttc.io/....

6 BRITO CRUZ, Francisco (coord.); MASSARO, Heloisa; OLIVA, Thiago; BORGES, Ester. *Internet e eleições no Brasil: diagnósticos e recomendações*. InternetLab, São Paulo, 2019. Available at: www.internetlab.org.br/...

7 In September 2020, with the presidential sanction of Provisional Measure 959/2020, the Brazilian General Data Protection Law came into force; therefore in effect during the 2020 municipal elections, which took place in November.

This research aims to better understand how these transformations and the risks they pose to digital rights have been addressed across Latin American countries. The purpose is to advance the debates on how to govern these news forms of political campaigning.

Through the collection and analysis of data regarding legislation and case laws, this research seeks to develop a comparative analysis of the legal frameworks governing the use of personal data by political campaigns in countries across Latin America. The questions that this research seeks to address are the following: how are digital political marketing techniques that involve the use of personal data - such as direct marketing and microtargeting - regulated in Latin American countries? How do the data protection regimes and electoral regulations in place address the concerns posed by the use of personal data by political campaigns?

METHODS AND GOALS

In researching the legal frameworks governing the use of personal data by political campaigns across Latin American countries, we adopt comparative legal research methods. More specifically, we deploy functional and law-in-context comparative legal research methods, combined with the CYRILLA methodology for mapping legal landscapes.[8]

Since we are interested in examining the use of personal data by political campaigns and in mapping the legal framework response in each country, the comparative method entailed is functional. Also, as we focus on understanding how actors perceive, invoke and apply regulations, the functional method is combined with a law-in-context method. While the functional method analyzes the problem in question and how different jurisdictions have responded to it, the law-in-context method takes into account the historical, cultural, economic, religious, and political context of the analyzed laws.[9]

The research was conducted through the collection, organization, and analyses of laws, bills, and judicial decisions regarding the use of personal data by political campaigns in electoral contexts. The data collection and organization followed the CYRILLA methodology for mapping legal landscapes, adapting it to the problem we are seeking to study. Instead of looking for laws affecting digital rights, we looked for laws that address or are applied to issues regarding the use of personal data and digital strategies by political campaigns. We looked mainly to areas regarding electoral regulation, data protection rules, and marketing and consumer guarantees. We conducted interviews with local organizations to better understand where to look to find legislation and how these rules are being mobilized, challenged, and applied in a given context.

The research encompassed six countries in Latin America: Argentina, Brazil, Chile, Colombia, Mexico, and Paraguay. Those are the four largest in population in the region (Brazil, Mexico, Colombia and Argentina), Chile, the first country in the region to enact a data protection law, and Paraguay, where internet penetration is significantly lower than the rest of the countries.

8 DHEERE, J. A methodology for mapping the emerging legal landscapes for human rights in the digitally networked sphere. In: ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS. Unshackling Expression: a study on laws criminalising expression online in Asia. 2017.

9 VAN HOECKE, M. Methodology of Comparative Legal Research. Law and Method, p. 279–301, 2016.

To better understand the discussion regarding data protection in the electoral context, we interviewed researchers from digital rights organizations in Argentina, Chile, Colombia, Mexico and Paraguay, whose names are withheld. The section on Brazil was based on a report on data protection and elections published in September 2020 to which InternetLab contributed.[10]

Based on the interviews carried out and the research done on official government websites, in the media and with the support of other academic productions regarding the use of personal data by political campaigns, we have produced categories of analysis to systematize the legal framework of each of the countries:

- Local background: the social and political context regarding the use of personal data by political campaigns, the main campaign practices adopted, and the emblematic cases involving personal data in elections.

- Electoral legal framework: how national law regulates internet ads and whether there are specific rules governing personal data usage.

- General legal framework on data protection

- Other relevant legislation: other legislations, besides electoral and data protection laws, relevant to the issue, including legislation regarding spam or direct marketing.

- Oversight and enforcement: data protection authorities and electoral management bodies (EMB),[11] their legal competence, the extent of their autonomy, and their articulation during elections.

Based on the analyses conducted through these categories, we produced an account of each country's legal framework and identified common trends across the region. We should stress that our aim was not to provide a detailed account of the intricacies of the legal framework in each country, but rather to map legal landscapes regarding specific issues within electoral legislation and data protection law, as relevant to our discussion. Also, as the research were conducted through the second semester of 2020, no further developments of each country's legal framework were considered for the analyses.

10 Massaro, Heloisa; Santos, Bruna; Bioni, Bruno; Brito Cruz, Francisco; Rielli, Mariana; Vieira, Rafael. *Proteção de Dados nas Eleições: democracia e privacidade*. Grupo de Estudos em Proteção de Dados e Eleições, 2020. Available at: www.internetlab.org.br/... . This study was conducted in partnership with Associação Data Privacy de Pesquisa and Instituto Liberdade Digital.

11 International Institute for Democracy and Electoral Assistance. (2007), Electoral Management Design: The International IDEA Handbook. Suíça, IDEA.; LÓPEZ-PINTOR, Rafael. (2000), Electoral Management Bodies as Institutions of Governance. New York, United Nations Development Programme; Marchetti, Vitor. (2008). Governança eleitoral: o modelo brasileiro de justiça eleitoral. Dados, 51(4), 865-893. doi.org/...

ARGENTINA

USE OF DATA BY CAMPAIGNS

Voter profiling and microtargeting, since the 2015 elections, with the increased use of social media

DATA PROTECTION FRAMEWORK

Constitutional right of a data subject to learn, update and rectify the information that has been collected about them in databases (National Constitution, art. 43, No. 3) **Data protection law** (Law No. 25.326/2000)

SENSITIVE DATA

Personal data that reveal racial and ethnic origin, **political opinions**, religious, philosophical or moral convictions, union affiliation and information about health or sexual life

EXCEPTIONS

Personal data from publicly-accessible sources. Under Resolution No. 86/2019, issued by the Access to Public Information Agency, some data is also not subject to consent (name, national identity document, tax or social security identification, occupation, date of birth and address)

DATA PROTECTION AUTHORITY

Access to Public Information Agency (*Agencia de Acceso a la Información Pública*), a functionally and legally **independent** agency of the executive branch

ELECTIONS MANAGEMENT BODY

National Electoral Commission (*Cámara Nacional Electoral*), part of the judiciary

ACCESS TO VOTER ROLL DATA?

No. Since 2013, voter roll data have been integrated into the Integrated Biometric Identification System - Sibios (*Sistema Integrado de Identificación Biométrica*), but hese data are reserved for the public authorities

ELECTORAL PROVISIONS ON PERSONAL DATA PROCESSING?

Resolution No. 86/2019 establishes data revealing political opinions or the affiliation to a political organization are considered sensitive data, which can be processed lawfully with the data subject's consent

ENFORCEMENT

There are no records of investigations regarding the use of personal data by political campaigns. In 2013, the Sibios was expanded to include electoral registration and incorporated photos of voters without asking for individuals' permission. The case was challenged in court after a leak of images from this database. In 2015, the photos were removed from the register

1 CONTEXT OF THE USE OF PERSONAL DATA IN POLITICAL CAMPAIGNS

Argentina has a population of 44 million. According to a 2019 report from the National Institute of Statistics and Censuses (Indec), 79.9% of citizens and 82% of houses have internet access.[12] In other words, Argentina ranks high in connectivity, differences between provinces notwithstanding. When it comes to social media, Facebook has 29 million users, and Instagram has 17 million users in the country. WhatsApp is the most popular instant messaging app, with 92% of internet users between 16 and 64 years-old using its services.[13]

Not surprisingly, given this high connectivity, electoral advertising is present online. Since 2015, Facebook and Twitter have been treated as additional campaign platforms. That year, the three most popular Argentine politicians were also those with the largest presence on social media: Mauricio Macri, with 5 million followers on Twitter and 4 million on Facebook; Daniel Scioli, with 1.5 million followers on Facebook and 1.2 million on Twitter; and Sergio Massa with 1 million followers on Twitter and 900 thousand on Facebook.[14]

Electoral advertising spending with social media in Argentina has remained stable since 2015: it varies between 23% and 30% of total campaign expenditures. According to the Argentine Electoral Management Board, this represents a third of the total campaign expenditure registered in a common "digital" item. However, there are not yet adequate tools to deepen its transparency.[15] As a result, campaigns' digital strategies are unknown, which is itself a factor limiting the enforcement of data protection law in electoral contexts.

12 Available at: indec.gob.ar/...

13 *Situación digital, Internet y redes sociales Argentina* 2020. Available at: yiminshum.com/...

14 Ariza, Andrea (July, 2016). *Las estrategias comunicativas, en Twitter y Facebook, en la campaña electoral presidencial 2015. V Congreso Internacional en Comunicación Política y Estrategias de Campaña. Asociación Latinoamericana de Investigadores en Campañas Electorales, Buenos Aires*. Available at: aacademica.org/...

15 *Publicidad electoral en redes sociales - PubliElectoral: una herramienta en búsqueda de transparencia*. Available at: publielectoral.lat/Informe-PubliElectoral.pdf

2 LEGAL FRAMEWORK

A THE ARGENTINE ELECTORAL SYSTEM AND THE POLITICAL ADVERTISEMENT

In Argentina, elections are governed by the 1983 Electoral Code,[16] which has been amended several times since then. The Argentine electoral management body is the National Electoral Commission (*Cámara Nacional Electoral*), which is part of the judicial branch. The Electoral Code does not address advertising in detail; its provisions cover the definitions of electoral campaign,[17] the length of the period in which advertisements are allowed and instructions for the mandatory presidential election debate.

Specific provisions on campaign advertisement on social media and digital platforms are found in the Law on the Finance of Political Parties (LFPP).[18] LFPP mandates, at each election, a register of all social media accounts, websites and other digital communication channels for candidates, political groups and high party authorities. Legal representatives of recognized political parties, confederations and party alliances also must register the identification data of the respective profiles in this register. The law also provides for the provision of campaign expenditures on digital platforms. As such, the audiovisual material used by campaigns on the internet, social media, messaging, and any other digital platform must be disclosed for auditing by the National Electoral Commission (*Cámara Nacional Electoral*), the elections management body in Argentina.

The law also defines specific destinations for government investments in digital electoral advertising. Of the total public resources in digital advertising, at least thirty-five percent (35%) must be for digital news sites that generate national content and production. Another twenty-five percent (25%) must go for digital journalism on websites that generate content and production at the provincial level, following a criterion similar to that of federal co-participation.

16 *Codigo Electoral Nacional*. Available at: servicios.infoleg.gob.ar/...

17 "set of activities developed by political groups, their candidates or third parties, through acts of mobilization, dissemination, publicity, opinion and communication consultation, presentation of plans and projects, debates in order to capture the political will of the electorate, which they must develop in a climate of democratic tolerance. Academic activities, conferences and the holding of symposia will not be considered as integral parts of the electoral campaign." Article 64, Electoral Code.

18 Ley 26215/2007. Available at: ervicios.infoleg.gob.ar/...

B THE ARGENTINE DATA PROTECTION REGIME

In 1994, the Argentine National Constitution (CN) was amended, with the addition of a chapter entitled "New Rights and Guarantees". Under this heading, different rights and guarantees were included in the Constitution, including the right to privacy. Under the new provisions, it is worth emphasizing article 43, which provides for "*habeas data*" in paragraph three.[19] The provision established an institution that lacked antecedents in federal law, although it was already found in the provincial constitutions. This reform marked the first steps in data protection legislation in Argentina.

Six years after the reform, in October 2000, Congress passed Law No. 25.326, the Data Protection Law.[20] It defined several data protection-related terms and included general principles regarding data collection and storage, outlining data subjects' rights and setting out guidelines for personal data processing. It is an omnibus law largely based on the EU Data Protection Directive (Directive 95/46/EC),[21] in force at that time, and on the subsequent national legislation transposing the directive in member states.

Argentina's Personal Data Protection Regime does not contain specific information about the use of data during elections. Nonetheless, in 2019, the Access to Public Information Agency (*Agencia de Acceso a la Información Pública*), the national data protection authority, issued guidelines for the processing of personal data for electoral purposes through Resolution No. 86/2019.[22] It set basic guidelines to ensure the integrity and protection of personal data during election processes. The resolution did not imply a change in existing regulations but restated the general principles established in them, adapting the regulations to the context of electoral campaigns. The guidelines for the processing of personal data for electoral purposes note that data that reveal political opinions or affiliation to a political organization are considered sensitive data, which can be processed lawfully with the data subject's consent. They also underline data protection principles such as purpose limitation, proportionality, accuracy, fairness, accessibility and minimization.

While the guidelines were welcomed by civil society, some questions have been raised. One of them is the fact that non-sensitive data, according to the guidelines, can be collected without consent when limited to name, national identity document, tax or social security identification, occupation, date of birth and address.

19 "Any person may file an amparo action to learn what and for which data about them contained in public registries or data banks, as well as in private ones whose purpose is to provide information, and, in case of inaccuracy or discrimination, to demand the suppression, rectification, confidentiality, or updating of the same. The secrecy of journalistic information sources shall not be affected."

20 Available at: argentina.gob.ar/...

21 Available at: eur-lex.europa.eu/...

22 Available at: servicios.infoleg.gob.ar/...

The guidelines came three years after a case around the use of welfare benefits data by the Secretariat for Public Communication. Under Resolution 166/2016,[23] issued by Chief of the Cabinet of Ministers, the National Administration for Social Security (ANSES) would share its database (containing data such as name, identity card number, home address, phone number, email address, date of birth, and marital status) with the Secretariat of Public Communication, which is functionally reliant on the Chief of the Cabinet of Ministers, in order to improve the government's communication strategy. The decision was contested by experts on data protection law and members of opposition parties,[24] who alleged that the data transfer does not align with the purpose principle, because the data were collected for a efficient operation of the social security system, not for communication or public relations activities. While not directly related to elections, this signaled concerns over the use of citizens' data, especially for purposes other than those justifying collection initially.

The ANSES case was preceded by a controversy around an incident involving voter roll and national ID biometric data. In 2011, the Argentinian government established the Integrated System of Biometric Identification - Sibios (*Sistema Integrado de Identificación Biométrica*). Sibios integrated the existing ID card database, Argentine National Registry of Persons (RENAPER)[25] and included digital image and fingerprint, civil status, and place of residence. Aimed at facilitating the identification of citizens and enabling cross-reference of data to support crime investigation and as a tool for preventive security functions, this system is accessible by the National Directorate of Immigration, the Airport Security Police, and the National Gendarmerie. It is even available to provincial enforcement entities. Later, for the 2013 presidential election, the biometrics system was expanded to include electoral registration (*padrón electoral*), incorporating photographs from the RENAPER without asking for individuals' permission or informing them.

The case was only challenged in court in 2014 when there was a leak of images from this database. Segu-Info,[26] a blog that publishes information on free and open information safety, discovered the weakness in the online electoral registration roll during the first round of presidential elections on 11 August 2013. They reported a system vulnerability which allowed the download of photos to the Computer Emergency Response Team of the Argentine Public Administration (ArCERT).[27] ArCERT had passed on the report to the National Electoral Commission (*Cámara Nacional Electoral*), but nothing was done about it.

Once this information was public, the Asociación por los Derechos Civiles (ADC) brought a case before the Contentious Administrative Proceedings Tribunal requesting the removal of photos from

23 Available at : boletinoficial.gob.ar/...

24 *Politico Argentina, Sectores de la oposición cuestionan la utilización de bases de datos de la Anses*, 26 July 2016. Available at: politicargentina.com/...

25 Resolution 3020/14 Available at: servicios.infoleg.gob.ar/...

26 *Descargar todas las fotos del Padrón Electoral Argentino*. 28 octubre 2013. Available at: blog.segu-info.com.ar/...

27 Available at: arcert.gov.ar/...

the database on the basis that: the photographs' publication was unconstitutional and in violation of the right to privacy as it was not necessary for the electoral process to function; and publication online increased the risk that they would be downloaded by third parties, after two years of the incident, in 2015, the photos were removed from the register.[28]

C OTHER LEGISLATION

In 2014, Law No. 26.951 (the Do Not-Call Law)[29] created the do-not-call registry and expanded the data subject rights in Argentina. This regulation allows the data owner to block contact from companies advertising, selling or giving away products and services. Companies offering products and services by telephonic means must register with the Agency and consult the list of blocked numbers on a monthly basis before engaging in marketing calls. However, this law is only intended to block calls from companies offering services, while election campaigns are presented in Article 8 as an exception.

3 OVERSIGHT AND ENFORCEMENT

According to article 19 of the Right of Access to Public Information Law (Law No. 27275),[30] the data protection authority in Argentina is the Access to Public Information Agency–since 2017, an independent body with legal and functional independence. The Agency aims to "supervise the protection of personal data stored in files, records, databases, or other technical means of data processing, whether public or private, intended to provide information, to guarantee the right to honor and privacy of individuals, and to ensure the right to access information that is registered about them."

According to Decree No. 899/2017,[31] on Access to Public Information, the Agency has the prerogative to audit the activities of controllers of databases and the data they manage; assessing compliance with the Regulations; and making recommendations in order to improve their performance within the legal framework. At its sole discretion, this body is entitled to audit compliance with the Protection Data Regulations. Article 4 of the Decree expressly authorizes the Agency to apply the appropriate sanctions if legal principles are not fulfilled. In addition, if data

28 UNO. *Quitan las fotos de ciudadanos del padrrón electoral nacional*. unoentrerios.com.ar...

29 Available at: argentina.gob.ar/

30 Avaible at: servicios.infoleg.gob.ar/...

31 Available at: oaip.mpd.gov.ar/...

subjects request it or if the Agency, at its sole discretion, finds it relevant, it is entitled to check: the lawfulness of data collection; the legality of exchanges of data and their transmission to third parties, as well as the interrelation between them; the lawfulness of the transfer of data; and the legality of both the internal and external control mechanisms for files and databases.

As to the electoral regulatory framework, the electoral management board in Argentina is the National Electoral Commission (*Cámara Nacional Electoral*),[32] which is the highest authority for applying political-electoral legislation. The Comission is a court of unique sort that is given an essential role in national electoral justice in everything that concerns the organization of electoral processes. For this, it has regulatory, operational and controlling powers over the National Registry of Voters, among other powers related to electoral management. It also enjoys the jurisdictional functions like any court. Opinions in judicial cases are binding on all first-instance courts as well as on national electoral boards. In addition to the National Electoral Commission, each Argentine province has a first-instance court, overseeing elections at the local level.[33]

Data protection in the electoral context falls under the purview of both authorities. Yet they have not undertaken joint action in personal data protection in electoral peridos, nor have they imposed sanctions. As already mentioned, the Agency for Access to Public Information contributed to this debate by issuing guidelines for the processing of personal data for electoral purposes. While the National Electoral Commission has been working on the transparency of accountability for online campaigns. In 2018, through the *acordada extraordinária n. 66*,[34] the Commission mandated registration of official accounts in social media and websites belonging to candidates, political groups and high-ranking party authorities. It also required that political parties include in their campaign reports the audiovisual material used on the internet and social media. It specifically called for CNE auditors to include that material in their audit of the digital campaigns developed by advertising agencies and consultants. Beyond those transparency mechanisms, neither the CNE nor the Access to Public Information Agency were seen as monitoring campaign use of personal data or enforcing data protection law in electoral contexts.

32 Decree No. 1285. Available at: servicios.infoleg.gob.ar

33 argentina.gob.ar/...

34 Available at: cij.gov.ar/...

4 OUTLOOK: ADVANCED IN DATA PROTECTION, NOT SO MUCH IN DIGITAL CAMPAIGNING

Argentina is currently one of the countries in the region with the most advanced legislation on the use of the internet and social media by campaigns, as is evidenced by the fact that among the countries analyzed, it is the only one with a guideline provided by a government agency on the use of data in election campaigns. It was also the first country in the region, in 2003, with an adequacy decision under the European Union's data protection framework,[35] which has inspired efforts in Latin America and elsewhere.

Still, the regulation of personal data processing by campaigns is in its early days. Electoral law (mainly the LFPP) is limited to regulating the use of profiles on platforms such as Facebook, Instagram and Twitter. It requires transparency around expenditures, but not around data processing. The guidelines issued by the data protection authority, which could fill in that gap, are too general and high-level to control campaign strategy effectively. As a result, despite having strong institutions and advanced legislation, Argentina is not in a significantly different situation when compared with other countries discussed here.

35 2003/490/EC: Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina. Available at: eur-lex.europa.eu/...

BRAZIL

USE OF DATA BY CAMPAIGNS

Voter profiling and microtargeting have been adopted. The most conspicuous digital strategy involved bulk messaging via WhatsApp during the 2018 elections.

DATA PROTECTION FRAMEWORK

Constitutional right to privacy (art. 5, X, XI & XII). **Data protection law** (General Data Protection Law — LGPD; Law No. 13.709/2018).

SENSITIVE DATA

Data on racial or ethnic origin, religious belief, **political opinion**, union membership or organization of a religious, philosophical or **political nature**, data relating to health or sexual life, genetic or biometric data.

EXCEPTIONS

Data may be processed without prior consent when it has been manifestly made public by the data subject, provided processing is keeping with data subject rights and data protection principles set forth in the General Data Protection Law. Under electoral regulation, electoral advertising through electronic messages requires consent.

DATA PROTECTION AUTHORITY

National Data Protection Authority (*Autoridade Nacional de Proteção de Dados - ANPD*), a department of the federal government, within the Office of the President of the Republic. Members cannot be dismissed without a cause.

ELECTIONS MANAGEMENT BODY

Superior Electoral Court (*Tribunal Superior Eleitoral - TSE*) is part of the **judiciary**.

ACCESS TO VOTER ROLL DATA?

No, voter roll data are not public in Brazil.

ELECTORAL PROVISIONS ON PERSONAL DATA PROCESSING?

In 2019, the Superior Electoral Court adopted Resolution No. 23610/19, which banned bulk messaging tools and encompassed some references to the newly enacted legislation on personal data protection when interpreting the electoral law.

ENFORCEMENT

In 2020, the Superior Electoral Court banned more than 1,000 WhatsApp accounts on suspicion of bulk messaging. However, the decisions mentioned disinformation, not privacy violations.

1 CONTEXT

Brazil has a population of 212 million.[36] Since 2018, the country has 120 million internet users.[37] According to the Reuters Institute Digital News Report, the most popular social media is WhatsApp, used by 83% of internet users, followed by Facebook, with 76%, and Instagram, with 61%.[38]

Since at least 2005, political campaigns have been using the internet to communicate with voters to some degree.[39] However, it was only in 2018 that digital communications emerged as key to campaign strategies. Until then, TV and radio were the central focus of political campaigning. In 2017 the Superior Electoral Court (*Tribunal Superior Eleitoral – TSE*), the Brazilian electoral management body, enacted a regulation on these strategies, allowing for boosting electoral advertising on social media. In the following year, R$ 77 million was spent on this type of advertising, representing 2% of the total campaign expenditures declared to TSE. Of this amount, 80% went to Facebook and 8% to Google.[40] After this regulation, in the 2018 general elections, President Jair Bolsonaro was elected with a campaign carried out almost exclusively online. The then-candidate appeared less frequently and for shorter durations on TV than other presidential candidates, before the runoff.[41]

36 *Instituto Brasileiro de Analise e Planejamento* (IBGE) ibge.gov.br/...

37 CETIC.BR. TIC Domicílios 2018. Available at: cetic.br/...

38 Reuters Institute Digital News Report. Available at: reutersinstitute.politics.ox.ac.uk/...

39 SORJ, Bernardo. *Internet, espaço público e marketing político: entre a promoção da comunicação e o solipsismo moralista*. Novos Estudos, São Paulo, n. 76, p. 123-136, nov. 2006. Available at: scielo.br/...

40 InternetLab. *O custo da propaganda eleitoral paga na internet em 2018*. Available at: internetlab.org.br/...

41 For more information on Bolsonaro' electoral campaign: CRUZ, Francisco Brito; VALENTE, Mariana Giorgetti. 'It's time to address Bolsonaro's propaganda network'. Available at: internetlab.org.br/...

2 LEGAL FRAMEWORK

A THE BRAZILIAN ELECTORAL SYSTEM AND POLITICAL ADVERTISING

In Brazil, elections are governed by the 1965 Electoral Code[42] and the Electoral Law (Law No. 9504/1997).[43] The Superior Electoral Court (TSE) is charged with calling, organizing and supervising elections, besides elaborating the electoral legislation requirements through regulations. Under the Electoral Code, the TSE shall also provide political parties, on equal terms,with the facilities allowed for their respective adversitement.[44]

The Brazilian legislation has a specific and intricate concept of electoral advertising (*propaganda eleitoral*), which broadly refers to advertisements disseminating candidates' bids and platforms to persuade voters that they are the aptest to assume the elective positions in dispute.[45] The Electoral Law defines several parameters for this type of advertising: deadlines; the use of public and private goods for campainging; press advertising; electoral contributions; the free time slots granted to political parties and candidates in radio and television programming; among others.

Until 2002, all political advertising regulations focused on in-person campaigning and TV and radio advertising. After the significant increase in the use of the internet as a means of political communication, the TSE initiated a policy conversation that led to Law No. 12034 in 2009[46] and the 2013 electoral reform.[47] Those rules authorized candidates and parties to use the internet for campaigning but banned any paid advertising. They also regulated several aspects of electoral advertisement on the internet, including content removal orders, accountability records, criminal offenses, among others. Under the new provisions, the electoral courts constantly addressed digital campaign strategies in a march that resonates in the adoption of these techniques by campaigns in Brazil.

In the 2017 electoral reform, the Electoral Law was amended to allow "content boosting" as the only lawful form of paid advertisement on the internet.[48] From the 2018 elections onwards, "content boosting" tools hired directly with application service providers with office or filial in

42 Electoral Code. Available at: planalto.gov.br/...

43 Available at: planalto.gov.br/...

44 Article 256 - Electoral Code

45 Available at: tse.jus.br/...

46 Available at: planalto.gov.br/...

47 Available at: planalto.gov.br/...

48 Law No 13488/2017 Available at: planalto.gov.br/...

Brazil became lawful for electoral advertising. In Resolution No. 23551/2017,[49] the TSE defined content boosting as "the mechanism or service that, hired with application service providers, potentialize the reach and dissemination of the information to reach users that, normally, would not have access to its content."

On the protection of personal data, the 2009 Law (Law No. 12034) included Art. 57-E in the Electoral Law. The new provision barred a series of organizations and entities – listed on article 24 of the law – from using, donating or giving records containing electronic registers from its clients in favor of candidates and parties. The provision also barred the selling of such records and established monetary penalties for the infringement of both rules. Until today, this provision is the main rule of the electoral legislation that guarantees a minimum level of data protection. It provides minimal protection against the activities of entities that distort the purpose for which their clients' data were collected, exploiting them, giving them away or selling them for electoral purposes without the subject's consent.

In 2019, this rule was updated by the Resolution No. 23610/19 of the Electoral Superior Court.[50] The requirements of art. 57-E now specify that not only the organizations and entities listed in article 24 but also private legal entities in general are forbidden from using, donating and giving personal data from their clients in favor of candidates and parties. The inclusion of "private legal entities" followed a decision enacted by the Brazilian Supreme Court that forbade enterprises from donating resources to political campaigns by considering "private legal entities" as included in the list of article 24. Also, the resolution replaced "electronic registers" with "personal data", strengthening the protection guaranteed by employing a terminology consolidated on personal data legislation. Finally, the requirements regarding this issue now specify that activities involving the processing of personal data conducted by legal entities or individuals, including its donation, use or assignment, must comply with the General Data Protection Law (*Lei Geral de Proteção de Dados - LGPD*).[51]

B THE BRAZILIAN DATA PROTECTION REGIME

The Brazilian Constitution includes the protection of privacy and private life as a fundamental right. It also provides for secrecy of data of all persons residing in the country the secrecy of data, establishing that any restrictions can only be made pursuant to the law through a judicial decision.[52]

49 Available at: tse.jus.br/...

50 Available at: tse.jus.br/...

51 Available at: in.gov.br/...

52 The Constitution also grants habeas data as a judicial measure that permits people to know and correct their personal data in governmental records: LXXII - habeas data shall be granted: a) to ensure the knowledge of information related to the person of the petitioner, contained in records or databanks of government agencies or of agencies of a public character; b) for the correction of data, when the petitioner does not prefer to do so through a confidential process, either judicial or administrative;

> **Article 5**. All persons are equal before the law, without any distinction whatsoever, Brazilians and foreigners residing in the country being ensured of inviolability of the right to life, to liberty, to equality, to security and to property, on the following terms:
> [...]
> X - the privacy, private life, honor and image of persons are inviolable, and the right to compensation for property or moral damages resulting from their violation is ensured;
> [...]
> XII - the secrecy of correspondence and of telegraphic, data and telephone communications is inviolable, except, in the latter case, by court order, in the cases and in the manner prescribed by law for the purposes of criminal investigation or criminal procedural finding of facts.[53]

Until the enactement of the Brazilian General Data Protection Law (*Lei Geral de Proteção de Dados* – LGPD)[54] in 2018, the few data protection provisions that existed in the country were scattered across sectorial legislation. The 2014 Brazilian Civil Rights Framework for the Internet (*Marco Civil da Internet*)[55] is not a data protection law, but a substantial portion of it deals with privacy and data protection on the internet. Besides the electoral legislation, it is one of the main statutes that may cover data-driven campaign practices. The privacy provisions can be widely classified into three main groups: (i) principles and user rights; (ii) specifications on log's retention; (iii) access to personal data. Privacy and data protection are mentioned at the outset of the statute as principles governing internet usage. Art. 7 guarantees a series of internet user rights and defines general rules for any personal data processing activity on the internet, including rules about consent, purpose, transparency, and personal data sharing.

The General Personal Data Protection Law, enacted four years after the Brazilian Civil Rights Framework for the Internet, finally brought a general regulation for privacy and data protection issues in Brazil, governing personal data processing in accordance with international standards. The new law, which came into force only in 2020, defined principles, hypotheses, rules and duties for personal data processing and established the data subject rights. Under the law, information on political opinion or affiliation to unions or organizations of a religious, philosophical or political nature is defined as sensitive data,subjected to more strict requirements

53 *Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;*

54 Available at: in.gov.br/...

55 Available at: planalto.gov.br/...

3 OVERSIGHT AND ENFORCEMENT

The Brazilian electoral management body, the Superior Electoral Court is part of the judiciary composed of at least seven members: three judges from the Supreme Federal Court, two judges from the Superior Court of Justice and two judges appointed by the President.[56] The court has administrative, jurisdictional, normative and consultive functions.[57] It is authorized by law to issue normative instructions[58] detailing electoral legislation through regulation necessary for its enforcement.[59]

The Brazilian data protection authority is the National Data Protection Authority (*Autoridade Nacional de Proteção de Dados* - ANPD), a body of the federal public administration within the Office of the President of the Republic.[60] The Board of Directors is composed of five directors – including a chair – appointed by the President and confirmed by the Senate. The ANPD is encharged of enforcing the LGPD and is empowered to enact regulation as well as to audit, rule on complaints, and fine and impose other sanctions on controllers or processors of personal data.

The authority was only established in late 2020 after the municipal elections took place in the country. Until then, the electoral courts, led by the TSE, were the only enforcement bodies with jurisdiction over privacy and data protection violations during elections in Brazil. Their jurisdiction, however, is bounded by the terms of the electoral legislation. If any of the electoral rules that touches on data protection issues are violated, the electoral courts may be called upon by candidates, parties, coalitions and the public prosecutors to order the illegal practice to ceases immediately. Subsequently, the candidate responsible or beneficiary of the offense may be sanctioned.[61]

In 2019, the TSE played a very active role in regulating digital electoral campaigns. In 2018, the newspaper *Folha de S. Paulo* published a report denouncing the use of bulk messaging tools by Jair Bolsonaro's supporters to convey messages through WhatsApp through undeclared expenditures.[62] When the court later enacted Resolution No. 23610,[63] it banned the use of bulk messaging tools to send electoral propaganda and encompassed

56 Art. 119, Federal Constitutional.

57 Jairo, G. (2019), Direito Eleitoral, 15ª edição, Grupo GEN, p. 99.

58 TSE's normatives instructions are called Resolutions and have a force of law.

59 Art. 1 and art. 23, IX, Electoral Code, and art. 105, Law No. 9.504/97.

60 Law No.13853/2019 Available at: planalto.gov.br/...

61 Massaro, Heloisa; Santos, Bruna; Bioni, Bruno; Brito Cruz, Francisco; Rielli, Mariana; Vieira, Rafael. *Proteção de Dados nas Eleições: democracia e privacidade.* Grupo de Estudos em Proteção de Dados e Eleições, 2020

62 Mello, Patrícia Campos. *Empresários bancam campanha contra o PT pelo WhatsApp*. Folha de S. Paulo, São Paulo, 18 out. 2018. Available at: folha.uol.com.br/poder...

63 Available at: tse.jus.br/...

some considerations about the newly enacted legislation on personal data protection when interpreting and defining the electoral law requirements. In the 2020 local elections, the court banned more than 1,000 WhatsApp accounts suspected of illegal bulk messaging. However, the bans were justified based on their engagement with disinformation, not for violating the bulk messaging rule.

While some electoral court decisions about personal data processing activities were reported, it is still too soon to understand how the LGPD impacted campaigns' digital strategies. For the next elections, in 2022, doubt hangs over the data protection authority. Some have expressed concerned over ANPD's enforcing the data protection law in electoral contexts, given its status as an agency under the Office of the President, prompting questions about its independence and distance from partisan politics.

4 OUTLOOK: A NEW DATA PROTECTION LAW; TOO SOON TO KNOW ITS IMPACT

Brazil is a country with high internet connectivity and high use of social media. Consequently, the internet affects several instances of public debate, and the electoral context is not an exception. The country has a robust and periodically updated system of electoral rules, overseen by electoral courts striving to make worth on the principles of fair elections, with equal chances between the candidates, and the technological events of digital advertising. Rules on the use of data by campaigns have been part of electoral law since 2009 (with the inclusion of Art.57-E in the Elections Law) — although not precisely to ensure data protection, but rather to preserve a level playing field. In any case, it shows how electoral law has been continually amended and expanded to keep pace with campaign strategies.

Yet, that has not stopped questions being raised about the lawfulness of campaign strategies, including, and notoriously, in the 2018 presidential election, where the use of personal data was a topic of vigorous discussion. Since then, Brazil has had advances, mainly with the enactment of a new data protection law in 2018 and its mentions in the resolution issued by the Superior Electoral Court in 2019. The law only entered into effect in September 2020, so it is too soon to understand its impacts on campaigns. Experts and authorities, both on data protection and on elections, are still making their first steps in seriously considering the issue of the use of personal data by campaigns; monitoring and enforcement structures are not yet fully in place.

COLOMBIA

USE OF DATA BY CAMPAIGNS

Voter profiling and microtargeting. There are also cases involving the use of personal data for clientelism practices. The most relevant case involves **Kontacto**, an app that was misused by city officials to collect citizen data for a mayoral campaign.

DATA PROTECTION FRAMEWORK

Constitutional right to privacy and constitutional right of a data subject to learn, update and rectify the information that has been collected about them in databases and files of public and private entities (art. 15). There is a data protection legislation (Statutory Law No. 1581/2012).

SENSITIVE DATA

Any information that can affect the subject's intimacy or cause any discrimination, related to as racial, sexual and health information; **political**, religious, philosophical **orientation**; data related to **membership of political parties**, social or human rights organizations; and biometric data.

EXCEPTIONS

Sensitive data can be processed for legitimate activities of a foundation, NGO and non-profit organization, with political, philosophical, religious or union purpose, if the data processed belongs to its members or to people who maintain regular contact due to their purpose.

DATA PROTECTION AUTHORITY

Superintendency of Industry and Commerce (SIC). Superintendent serves at the pleasure of the President, undermining provisions for its autonomy.

ELECTIONS MANAGEMENT BODY

National Electoral Council (*Consejo Nacional Electoral*). Its members are chosen by the political parties, which make local politicians have a heavy influence in CNE.

ACCESS TO VOTER ROLL DATA?

Limited. Voter rolls (called *Censo Electoral*) are available at the Registraduría Nacional del Estado Civil website. Citizens can have access only to their own data. There is no public access to the full document.

ELECTORAL PROVISIONS ON PERSONAL DATA PROCESSING?

SIC's Act 330, directing all political parties and movements to comply with the data protection law.

ENFORCEMENT

Regarding the case of the app Kontacto, the Risaralda Contentious Administrative Court rescinded the election results for violation of the fundamental right to vote freely. The data protection authority will also consider the case.

1 CONTEXT OF THE USE OF PERSONAL DATA IN POLITICAL CAMPAIGNS

Colombia has a population of approximately 50 million. According to the 2018 National Census, only 43.4% of Colombian homes have access to the internet, whether fixed or mobile.[64] In terms of population, according to the Ministry of Information and Communication Technology, 28.9 million Colombians have access to the internet, which means that 6 out of 10 Colombians have internet access.[65]

Social media, such as Facebook and WhatsApp are popular in Colombia. In 2017, Facebook had a daily access rate of 17 million users in Colombia.[66] According to local studies, WhatsApp is the most popular app in the country: 87,3% of internet users in Colombia use WhatsApp, mostly because the large majority of mobile phone plans include zero-rating access to the app.[67]

Since the 2016 Plebiscite, political content on social media has been increasing. In the 2018 elections, the collection and processing of personal data for political and electoral purposes grew.[68] Political parties use profiling techniques based on data collected from Twitter, Facebook and Instagram to target political advertising.[69]

A case that occurred during the 2019 elections raised a public debate regarding data protection and electoral advertising. Cuestión Pública — a Colombian investigative media outlet — and Qurium — a Swedish civil society organization dedicated to safe hosting and defense of digital rights — published in 2019 an investigation about an app called Kontacto, created to collect data from voters in the city of Pereira.

64 *Censo Nacional de Población y Vivienda 2018*, Colombia. Available at: dane.gov.co/...

65 *Boletín trimestral de las TIC: cifras tercer trimestre de 2019*. Published: Bogotá D.C. - Colombia, Jan. 2020. Available at: colombiatic.mintic.gov.co/...

66 Peñarredonda, José Luiz. *Elecciones y datos personales: un estudio de las elecciones legislativas 2018*. Tactical Technology Collective; Fundación Karisma. Colombia, Bogotá: 2018. p. 6. Available at: web.karisma.org.co/...

67 Linterna Verde. *La política (en WhatsApp) es dinámica: desinformación y difusión de 'cadenas' políticas en Colombia*, p. 6.. August, 2018. Available at: linternaverde.co/...

68 Ibidem, p. 24.

69 Ibidem, p. 12.

According to the journalistic reporting, Juan Pablo Gallo, mayor of Pereira,[70] compelled city officials to enter city voters' data in the app. This data was used for the campaign of Carlos Alberto Maya, who was elected in October 2019.

On September 1st, 2020, the Risaralda Contentious Administrative Court rescinded in part the administrative act declaring Carlos Alberto Maya López as the winner, and canceled Maya López's credential.[71] According to the court, employees influenced voters through the Kontacto app, undermining the fundamental right to vote freely.[72] The court also referred the case for investigation by the Superintendence of Industry and Commerce, the data protection authority in Colombia.

The Kontacto app case helps us understand how data protection and electoral legislation have been mobilized in election campaigns and the role of the electoral and data protection authorities in Colombia.

2 LEGAL FRAMEWORK

B THE COLOMBIAN ELECTORAL SYSTEM AND THE POLITICAL ADVERTISING

Colombia is divided into departments, districts and municipalities. At each level, Legislative and Executive powers are elected by popular vote. Candidates must be affiliated with a political party or movement.[73] The Constitution of Colombia establishes the vote as a right to the citizen,[74] but it is not mandatory. Colombia has an Electoral Code (Law No. 96/1985) that organizes the electoral procedure and establishes the functions of electoral authorities.

Law No. 130/1994, known as the Basic Statute of Political Parties and Movements, establishes the rules for political parties and political campaign financing and the rules for conveying electoral advertising. There is no electoral legislation in Colombia that specifically addresses the use of personal data in the electoral context or political advertising on the internet. Colombia's electoral legislation governs electoral advertising on television and radio and the period that political parties can place ads, but there are no rules about how this would work on the internet.

70 Cuestión Pública; Qurium. Episodio 1: Kontacto la nueva máquina electoral de hacer votos. October 24, 2019. Available at: cuestionpublica.com/...

71 Case no. 66001-33-33-000-2019-00777-00, Tribunal de lo Contencioso Administrativo de Risaralda.

72 Art. 40 and 258, Constitución Política de Colombia.

73 Peñarredonda, José Luiz. *Elecciones y datos personales: un estudio de las elecciones legislativas 2018*. Tactical Technology Collective; Fundación Karisma. Colombia, Bogotá: 2018. p. 4-5. Available at: web.karisma.org.co/...

74 Art. 238, Constitución Política de Colombia.

Law No. 1475/2011, establishing rules on political parties and the electoral process, requires voter rolls (*Censo Electoral*) by the *Registraduría Nacional del Estado Civil*, as a technical instrument to plan, organize, execute and control the elections, and as a mechanism for citizen participation. Voter rolls contain ID information, polling place, gender, and other personal data of all citizens eligible to vote. While the principle of publicity applies to voter rolls,[75] the database is not accessible by the public. Citizens can access their own data through a website,[76] but they do not have access to the full document. There have not been reports of misuse of voter rolls.

Bill 234/2020, which would replace the Electoral Code, was passed in 2020. It has a greater emphasis on internet electoral advertising and transparency for political campaigns. It also includes social media in its provisions. Yet there is little concern regarding data protection: there are no provisions on data processing. It is still not in force, with a decision from the Constitutional Court on an automatic judicial review of this type of legislation still pending.

C THE COLOMBIAN DATA PROTECTION REGIME

In terms of data protection and data privacy, the Constitution recognizes the right to privacy and the subject's right to know, update and rectify the information that has been collected about them in databases and records of both public and private entities.[77] In addition, Colombia has a Data Protection Law (Statutory Law No. 1581/2012) enacted in 2012 and regulated in 2013 by Decree no. 1377/2013. Although there are no specific provisions about elections, the data protection legislation can be — and has been — used in electoral and political contexts.

The Data Protection Law applies to personal data on any database processed by public or private entities. The data processing must be subjected to the purpose limitation principle, the legality principle, the transparency principle, the access principle and the restricted circulation and confidentiality principle, among others.[78] Stricter rules govern the processing of sensitive data, which are defined as any information capable of affecting the subject's intimacy or causing any discrimination, related to as racial, sexual and health information; political, religious, philosophical orientation; data related to membership of political parties, social or human rights organizations; and biometric data.[79] Processing of sensitive is disallowed, except under five hypotheses: (a) express authorization, (b) when necessary to safeguard the subject's vital interest; (c) for legitimate activities of a foundation, NGO and non-profit organization, with political,

75 Art. 48, Ley no. 1475 de 2011. Available at: wsr.registraduria.gov.co/...

76 It is possible to access the data here: wsp.registraduria.gov.co/...

77 Art. 15, Constitución Política de Colombia.

78 Art. 4, Statutory Law No. 1581/2012.

79 Art. 5, Statutory Law No. 1581/2012.

philosophical, religious or union purpose, provided the data processed belongs to its members or to people who maintain regular contact on account of the organization's purpose; (d) for the exercise of defense in judicial proceedings and (e) for historical, statistical or scientific purpose.[80]

Political parties collect and process data from any person who access their websites or social media through trackers that measure activity records and forms that capture personal data, based on the authorization to process data related to members or people who maintain regular contact with foundations, NGOs, and other organizations.[81] However, this interpretation adopted by political parties is controversial.

Civil society and digital rights organizations argue that this is an extensive interpretation since it allows political parties to collect and process data without the subject's consent. Also, the mere access to the websites does not imply a shared purpose since people can access political parties' websites for reasons other than an alleged agreement with the parties' political purposes.

As a rule, the processing of personal data requires prior and informed authorization from the data subject. There is, however, no need for authorization for the processing of (a) data required by a public or administrative entity by court order; (b) data of "public nature"; (c) in case of health emergency; (d) for historical, statistical or scientific purposes; and (e) data related to the Civil Registry of Persons.[82] Under the law, data of public nature is any personal data that can be found in public access sources.[83] Therefore, the law effectively establishes a very large scope of hypotheses for the processing of personal data. Furthermore, the Data Protection Law and Decree no. 1.377/2013 are not clear about how the authorization should be provided, making the law little protective to the data subject. In practice, political parties use generic privacy policies to obtain consent for personal data processing.

The Data Protection Law also establishes sanctions for those who violate the data protection legislation. According to the law, the Superintendency of Industry and Commerce (SIC), the data protection authority, is responsible for imposing sanctions against controllers and processors of personal data.[84]

This provision impacts political parties and private operators involded with electoral campaigns. Usually, the candidate hires a private company to carry out the electoral advertising, and it is often not clear who is responsible for the data processing. A case that occurred in 2018 illustrates this controversy. In 2018, through their institutional email and institutional phone

80 Art. 6, Statutory Law No. 1581/2012.

81 Peñarredonda, José Luiz. *Elecciones y datos personales: un estudio de las elecciones legislativas 2018*. Tactical Technology Collective; Fundación Karisma. Colombia, Bogotá: 2018. p. 16.

82 Art. 10 and 11, Statutory Law No. 1581/2012.

83 Art. 5, Decree no. 1.377/2013.

84 Art. 23, Statutory Law No. 1581/2012.

numbers, students from Sergio Arboleda University started to receive electoral advertising from Zaida Barrero, the wife of dean the university and a candidate for a seat in the Senate. On social media, students denounced the unauthorized use of university databases for electoral purposes. Rodrigo Noguera and Zaida Barrera claimed that they did not use the university databases and instead hired a communications agency for the campaign, which failed to ask for permission to send electoral messages.[85] Barrero and her husband argued the communications agency was the controller, thus exonerating them from liability for the misuse of student data. The case was not brought before courts.

In summary, Colombian electoral legislation is not in tune with the practices adopted by political parties in terms of data protection and online campaigns. Colombia has consistent data protection legislation, which addresses the main points regarding sensitive data, principles for data processing, authorization for data collection and rights of the data subject. However, political campaigns still do not apply the law properly.

3 OVERSIGHT AND ENFORCEMENT

The electoral management body in Colombia is the National Electoral Council (*Consejo Nacional Electoral*), known as CNE, the highest-level electoral authority, responsible for regulating and applying constitutional rules and legislation regarding the elections. As a second-level electoral authority, the Nacional Civil State Registry is responsible for the electoral results and vote tallies.[86] Also, Colombia has a data protection authority called Superintendency of Industry and Commerce (*Superintendencia de Industria y Comercio*), known as SIC, responsible for applying the data protection law and imposing sanctions, including in elections.

Under the Constitution, CNE, the electoral management body, is responsible for regulation, inspecting, monitoring and controlling all electoral activity of political parties and movements.[87] Regarding its structure, the CNE is composed of nine members elected by the Congress, with proportional representation of the parties, for a period of four years.[88] Even if the CNE is autonomous under the law, there is much mistrust regarding the Council. The local civil society argues that local politicians heavily influence CNE, since its members are chosen by the political parties. This influence might undermine the Council's ability to act.

85 Osório, Carlos Hernández. "*Los mensajes en la Sergio Arboleda que invitan a votar por la esposa del Rector*". La Silla Vacía. March 6, 2018. Available at: lasillavacia.com/...

86 Art. 120, Constitución Política de Colombia.

87 Art. 265, Constitución Política de Colombia.

88 Art. 264, Constitución Política de Colombia.

The National Civil State Registry, which is placed under the jurisdiction of CNE, has more autonomy but a reduced scope. The Nacional Civil State Registry is responsible for the register of citizens and for calling and organizing elections under CNE's supervision. The National Civil State Registry members are chosen by the presidents of the Constitutional Court, the Supreme Court of Justice and the Council of State.[89]

Regarding the data protection law, the supervisory authority is the Superintendency of Industry and Commerce (SIC). SIC is responsible for ensuring compliance with the data protection law and carrying out investigations regarding violations of the law through the Delegation of Personal Data Protection.[90] According to the law, SIC is an autonomous and decentralized institution, and it is part of the decentralized sector of commerce, industry and tourism.[91] The top position of SIC is the superintendent, who is appointed by the President of the Republic.

The superintendent serves at the pleasure of the President. The members of the Delegation of Personal Data Protection are freely chosen by the superintendent.[92] Therefore, President and superintendent have a very close relation, and, as a consequence, each newly elected President names a new superintendent.[93] Thus, as much as there are legal guarantees of independence and autonomy, SIC's ties with the executive branch undermine the Superintendency's autonomy, with the President pulling the strings. There is also a problem related to Superintendency's staff, regarded as too small and insufficient to handle all its demands.

In an electoral context, both the National Electoral Council and Superintendency of Industry and Commerce have the competence to act on issues regarding data protection. However, there are still few actions aimed at protecting personal data in elections or safeguarding online political campaigns in practice. We highlight here two actions mobilized by the data protection authority and/or electoral authority:

I. **SIC's Act 330**: In June 2019, SIC sent to all political parties the Act 330, which directed all political parties and movements to respect the data protection law.[94] The act followed to five complaints of data misuse: voters received emails and phone calls of political advertising, but they had not authorized the use of their data. In the Act, SIC directed electoral campaigns to only send messages to those who have authorized their personal data processing and instructed political parties to respect and guarantee the right to delete the personal data of those who do not wish to receive political advertising.

89 Art. 266, Constitución Política de Colombia.

90 Art. 19, Statutory Law No. 1581/2012.

91 Art. 1.2.1.2., Decree No. 1.074/2015.

92 Art. 3, 32, Decree No. 4.886/2011.

93 Simão, Bárbara; Oms, Juliana; Torres, Livia. *Autoridades de Proteção de Dados na América Latina: um estudo dos modelos institucionais da Argentina*, Colômbia e Uruguai. IDEC, 2019. p. 24.

94 SIC. Act 330. June 26, 2016. Available at: sic.gov.co/...

II. **CNE's official communication regarding the use of social media for political advertising that resulted in the CNE's Resolution no. 2.126/2020:** In July 2020, CNE, through an official communication,[95] announced that social media, such as Facebook, Twitter and Instagram, when used to promote candidacies, constitute publicity and/or political advertising must respect the days and hours established by electoral legislation. This announcement was motivated by the investigation against one of the mayoral candidates in Tarqui, in the 2019 elections. Álvaro Trujillo Hernández was a mayoral candidate who allegedly began the election campaign before the official period. He allegedly used his own personal Facebook account to promote his campaign. In Resolution no. 2.126/2020, CNE did not sanction Hernández but established that, from now on, candidates would have to conform their electoral advertising on the internet to the Electoral Code. In the Resolution, CNE also equated social media with traditional media, but this provision did not include message services, such as WhatsApp.

CNE's decision was based on a sentence C-592/12 handed down by the Colombian Constitutional Court.[96] This sentence from 2012 refers to an article of the Consumer Legislation in Colombia (Art. 30)[97] that prohibited misleading advertising and established that "the media will be jointly and severally liable only if intent or gross negligence is proved". The case discussed whether such provision would constitute censorship. According to the decision, in case of misleading advertising, social media's liability is only possible if there is evidence of fraud or serious negligence. According to the Court, the joint liability is based on two articles of the Colombian Constitution: article 20, which established the freedom of speech, and article 78, which establishes the liability of those who produce and sell services that threaten consumers. Since there is no "strict liability", article 30 from Law No. 1480/2011 would be constitutional. In the sentence C-592/12, the Constitutional Court recognized the article's constitutionality and equated social media with traditional media.

95 CNE. Comunicados Oficiales: uso de redes sociales con fines electorales sí se considera propaganda política. July 1st, 2020. Available at: cne.gov.co/...

96 Sentence C-592/12. October 12, 2012. Available at: corteconstitucional.gov.co/...

97 Law No. 1480/2011. "*ARTÍCULO 30. PROHIBICIONES Y RESPONSABILIDAD. Está prohibida la publicidad engañosa. El anunciante será responsable de los perjuicios que cause la publicidad engañosa. El medio de comunicación será responsable solidariamente solo si se comprueba dolo o culpa grave. En estos casos en que el anunciante no cumpla con las condiciones objetivas anunciadas en la publicidad, sin perjuicio de las sanciones administrativas a que haya lugar, deberá responder frente al consumidor por los daños y perjuicios causados*".

4 OUTLOOK: A ROBUST LEGISLATION WITH ENFORCEMENT CONCERNS

The concern around data protection in elections is increasing in Colombia. Investigations conducted by the media and studies conducted by digital rights organizations demonstrate that this topic has been important for public debate. However, the institutional response to the problem is still being constructed.

The 1985 Electoral Code lays down the electoral procedure and establishes the functions of electoral authorities. Political campaigns are governed by Law No. 130, from 1994. Colombia's electoral legislation rules are detailed on electoral ads on television and radio, as well as the period during which political parties can place ads. However, there are still no rules about how this would work on the internet. In terms of electoral legislation, there seems to be a normative vacuum regarding political campaigns on the internet. There is a bill under discussion that could mitigate this problem; however, it does not address all the problems already recorded in the country.

Regarding data protection, Colombia has consistent data protection legislation, whose regime is based on consent. The data protection regime applies to individuals, public companies and governmental entities that process personal data. However, political parties do not seem to comply with data protection law adequately. Also, there are structural problems in the organization of the data protection authority and the electoral authority. SIC, the Colombian data protection authority, is tied to the President, undermining its independence. Similarly, CNE, the electoral management body, is seen as caught up in the partisan fray. That prevents an effective application of data protection law in the electoral context.

CHILE

USE OF DATA BY CAMPAIGNS

Voter profiling. The most relevant case involves InstaGIS, a company known as "the Chilean Cambridge Analytica".

DATA PROTECTION FRAMEWORK

Constitutional right to data protection, constitutional right to privacy (art. 19, No. 4 and No. 5) **Data protection law** (Law About the Protection of Private Life; Law No. 19 628/1999).

SENSITIVE DATA

Personal data that refer to the physical or moral characteristics of people or to facts or circumstances of their private life or privacy. Examples provided by law: personal habits, racial origin, **political ideologies and opinions**, religious beliefs or convictions, physical or mental states of health and sexual life.

EXCEPTIONS

Personal data from publicly-accessible sources.

DATA PROTECTION AUTHORITY

There is no data protection authority. The Council for Transparency (*Consejo para la Transparencia*) is responsible to ensure compliance with data protection by government bodies. It has a limited scope of action.

ELECTIONS MANAGEMENT BODY

SERVEL (*Servicio Electoral*). Independent and autonomous body, and is part of the Executive Branch.

ACCESS TO VOTER ROLL DATA?

Public access. The voter rolls include information, such as name, polling place and ID number of all voters eligible to vote in that election. They are public and can be accessed and processed by anyone, for electoral purposes. (Law No. 18.556).

ELECTORAL PROVISIONS ON PERSONAL DATA PROCESSING?

There is no specific provision.

ENFORCEMENT

There are no reports of investigations regarding the use of personal data by political campaigns. In 2020, the Council of Transparency warned Servel that the publication of voter rolls was disproportionate, as it exposed too much of the personal data of Chilean voters.

1 CONTEXT OF THE USE OF PERSONAL DATA IN POLITICAL CAMPAIGNS

Chile has a population of 19 million.[98] According to a study developed by the Chilean Telecommunications Undersecretariat, in 2017, internet access reached 87.4% of the total population.[99] Following global trends, social media have played an increasing role in day-to-day life and in the way the population gets informed. According to a survey carried out by the CADEM, a private studies center, in 2017, broadcast television (60%) and WhatsApp (58%) are the main channels through which the Chilean population gets informed. Also, 55% of the population get information from cable TV, and 48% from Facebook.[100]

Social media has played a central role in the electoral campaigns in Chile. According to a study developed by the digital rights organization Datos Protegidos, in the last few elections, candidates have been using more targeted campaign strategies, with the help of data-driven agencies that use personal data to profile voters.[101]

As stated by *Datos Protegidos*, in 2017, there were at least 10 companies that developed political campaigns based on personal data. A case involving Instagis received special attention from the Chilean press. Popularly called by the media as "Chilean Cambridge Analytica",[102] Instagis is a "predictive mapping platform"[103] that, by cross-referencing data from different databases, is able to predict patterns and behavior, consumption, and political preferences.

98 According to Instituto Nacional de Estadísticas (INE), from the Chilean government. Data available at: ine.cl

99 IX Encuesta de Acceso y Usos de Internet – Subsecretaría de Telecomunicaciones de Chile, 2017. Available at: subtel.gob.cl/...

100 Encuste No. 199, CADEM. November 06, 2017. Available at: www.cadem.cl/...

101 Garrido, Romina. *Datos personales e influencia política en Chile*. Datos Protegidos. June, 2018. p. 12. Available at: datosprotegidos.org/...

102 Saleh, Felipe. *Instagis, la Cambrigde Analytica chilena: empresa de big data favorita del Presidente Piñera opera al límite de la ley*, El Mostrador. October 1st, 2019. Available at: elmostrador.cl/....

103 See more at: instagis.com/...

In the 2017 elections, the company was hired to build political profiles for election campaigns in at least 27 municipalities. It was also hired for the electoral campaign of Sebastián Piñera, the current president of Chile.

In 2017, the political party *Renovacion Nacional* (RN), to which President Piñera is affiliated, hired the services of Instagis. According to the agreement between RN and Instagis,[104] the company monitors public Facebook Fan Pages where political content is published as well as users' interactions "that reveal their tendencies and preferences". Then, Instagis matches "the names of the people who publicly interact in FB and the names in the voter rolls, thus getting the Fans' RUT [national ID number] to link it with other public information."[105]

The practice was not perceived to violate electoral legislation or data protection law, as we will see below, but it caused concern on the media, civil society organizations and the population. Speaking to *El Mostrador*, an online newspaper, Pablo Viollier, from *Derechos Digitales*, said that "it isn't an illegality, but is a situation that allows citizens to have a legitimate resentment of what is happening with that data".[106] While the Instagis case was not challenged in courts, nor was it scrutinized by authorities, it started a conversation on the use of personal data in election campaigns. Based on this context, we will analyze the electoral and data protection legal framework in Chile.

2 LEGAL FRAMEWORK

A THE CHILEAN ELECTORAL SYSTEM AND THE POLITICAL ADVERTISING

Between 1973 and 1990, Chile experienced a military dictatorship, and many of its laws still date from that time. The Chilean Constitution in force today dates from the authoritarian regime. On October 25, 2020, Chileans voted on by an overwhelming majority to draft a new Constitution.[107] Electoral legislation has been undergoing reforms aiming to make the electoral process more transparent and democratic. In 2015, Law No. 20840 replaced the binomial electoral system

104 The contract was signed on September 5, 2016 and it is available at: transparencia.rn.cl/...

105 In the original: "*Instagis monitorea distintas Fan Pages públicas de Facebook (FB) donde se publican contenidos políticos y donde los usuarios que las siguen realizan interacciones públicas que revelan sus tendencias y preferencias. Instagis utiliza estas interacciones para actualizar la probabilidad de adherencia. (...) Para realizar este proceso Instagis hace un match entre los nombres de las personas que públicamente interactúan en FB y los nombres del Padrón auditado, así obteniendo el RUT de los Fans para cruzarlos con otras capas de información pública.*" (Page 3 of the contract).

106 Saleh, Felipe. *Instagis, la Cambrigde Analytica chilena: empresa de big data favorita del Presidente Piñera opera al límite de la ley*, El Mostrador. October 1st, 2019. Available at: elmostrador.cl/...

107 See more at: gob.cl/...

— that resulted from Pinochet's dictatorial period — with a proportional, representative and inclusive electoral system, which also increased the number of parliamentarians in the legislative houses. In the following year, 2016, Congress enacted Law No. 20900, regulating political campaigns and establishing transparency requirements for electoral spending.[108]

In contrast to other countries discussed in this report, there is no electoral code in Chile. The electoral process is regulated by several sparse laws. Besides the ones mentioned above, other important regulations regarding the electoral process are Law No. 20.938/2016, governing the scope and powers of *Servicio Electoral* (or SERVEL, the independent agency that is Chile's electoral management body), and Law No. 18.556, amending rules on the electoral registration system and SERVEL.

Electoral advertisement is defined by Law No. 20.900 as "any event or public demonstration and advertising, in the radio, in writing, in images, on audiovisual media, and other similar means, promoting one or more people or political parties, either incorporated in the process of incorporation, for electoral purposes".[109] The advocacy of ideas or candidates by natural persons does not constitute political advertising. The law sets standards so that political campaigns can be fair and plural, barring public and private entities[110] – other than campaigns and political parties themselves – from contributing or engaging in campaigning, as well as banning paid advertising in the media.[111]

None of the Chilean electoral laws expressly mention digital ads, but SERVEL's understanding is that electoral ads in digital media fall under "other similar means", within the meaning of electoral advertising in Law No. 20900. SERVEL defines digital media as "all those communications through media such as web pages, social media, telephony and emails when transcending the social circle of individuals and when services are hired".[112] "Essentially private" communications via social media, such as emails and WhatsApp, are interpreted to fall outside electoral advertisement requirements.[113] In 2016, a bill aiming to fill the gap in digital electoral ads, Bill 10819-07, was introduced in the Chamber of Deputies.[114] So far, there has not been any significant progress on the bill.

108 Constitutional Decree no. 2 (DFL No. 2) accelerated the approval of Laws no. 20.840 — which updates Law No. 18.700/1986 — and of Law No. 20.900, which updates Law No. 19.884/2003. The decree was signed by the then President Michelle Bachelet. The DFL No. 2 is available at: www.bcn.cl/...

109 Art. 6°, 3, Law No. 20.900.

110 Art 2°, 11, Law No. 20.900.

111 Garrido, Romina. *Datos personales e influencia política en Chile*. Datos Protegidos. June, 2018. p. 4. Available at: datosprotegidos.org/...

112 SERVEL. *Manual de consulta de campaña y propaganda electoral* 2017. Available at: servel.cl/...

113 *Ibidem*, p. 24.

114 Boletín 10816-07. Available at: senado.cl...

Electoral law in Chile does not have any provision regarding data protection. As pointed out by studies developed by Chilean digital rights organizations,[115] the electoral system has an important loophole for personal data. Under Law No. 18556 on the electoral registration system and electoral service, SERVEL is required to prepare and publish the voter rolls for each election. Voter rolls (*padrones electorales*) are a list of all voters eligible to vote in that election.[116] They include information, such as name, polling place and ID number. Voter rolls are public and can be accessed — and copied — by anyone for electoral purposes. They are published online, in PDF format, by SERVEL, as part of its transparency efforts. In 2017, the use of voter rolls for commercial purposes was made illegal.[117] Commercial use of voter rolls can lead to imprisonment and fines.

B THE CHILEAN DATA PROTECTION REGIME

In 1999, Chile was the first country in Latin America[118] to enact data protection legislation, with the Law About the Protection of Private Life (Law No. 19.628). The law is simple in its structure. It aims to limit data processing to the purposes informed during its collectionand guarantee data subjects' rights to access to correct and eliminate their data. Data protection gained constitutional status in 2018, with the approval of Law No. 21.096, which enshrined the right to the protection of personal data and to a private life as a fundamental right (art. 19 no. 4 and no. 5 of the Constitution). Law No. 19628 and Law No. 21096 are the main regulatory frameworks for data protection in the country.

Processing of sensitive data is prohibited, except when authorized by law, e.g., when consent from the subject is obtained or when processing is necessary to grant health benefits. Sensitive data are defined as "those personal data that refer to the physical or moral characteristics of people or to facts or circumstances of their private life or privacy". The law does not exhaustively list what constitutes the circumstances of private life that would configure sensitive data, but it does provide some examples of which data could be considered sensitive: personal habits, racial origin, political ideologies and opinions, religious beliefs or convictions, physical or mental states of health and sexual life.[119]

115 Garrido, Romina. Datos personales e influencia política en Chile. Datos Protegidos. June, 2018. p. 9. Available at: datosprotegidos.org/...

116 Art. 31 and 32, Law No. 18.556.

117 Art. 4, DFL No. 5. Available at: bcn.cl/...

118 Garrido, Romina. Datos personales e influencia política en Chile. Datos Protegidos. June, 2018. p. 8. Available at: datosprotegidos.org/...

119 Art. 2°, (g), Law No. 19.628/1999.

The law also permits the processing of personal data from publicly-accessible sources. Such data can be combined in private databases. In the electoral context, that provision has meant anyone can use voter rolls data. It has also made it possible to gather publicly-accessible data from social media.

The Law About the Protection of Private Life also establishes provisions about data sharing. Under the law, data sharing may occur as long as the rights of the subjects are safeguarded and the transmission is related to the purposes of the participating organizations.[120] Those requirements do not apply to publicly-accessible data.

Experts criticize exceptions for publicly-accessible data, which they see as allowing extensive collection and processing of personal data. In 2017, a bill intended to overhaul the data protection framework, Bill 11144-07,[121] was introduced. Inspired by the European General Data Protection Regulation (GDPR), it would create a data protection authority, which currently does not exist in Chile. The bill was approved in the Senate in 2018, but it is still under discussion in legislative houses.

In summary, Chile was a pioneer in data protection legislation in Latin America and enshrines the right to data protection as a fundamental right. However, its legislation on the subject is deficient and presents problems, particularly regarding publicly-accessible data, making it possible to handle the data from voter rolls and social media. This data processing regime reflects in cases such as Instagiz, in which voter rolls data were cross-referenced with social media interactions for voter profiling purposes. Having said that, it should be noted that political preferences gleaned from social media might be subject to the stricter requirements for sensitive data.

C OTHER LEGISLATION

Chile has a consumer law (Law No. 19.496/1997), which enshrines consumers and businesses' main rights and obligations. Among other provisions, the Chilean consumer's rights protection law regulates spam.[122] Article 28 B regulates emails sent with promotional or advertising communication unconnected to purchases by the consumer. However, it does not apply to the electoral context. Thus, political campaigning has not been subject to consumer law requirements.[123]

120 Art. 5, Law No. 19.628/1999.

121 Boletín 11144-07. Available at: camara.cl/...

122 Art. 28-B, Law No. 19.496/1997.

123 Datos Protegidos. *¿SPAM o Propaganda electoral? ¿Qué pasó con mis datos personales?* November 16, 2016. Available at: datosprotegidos.org/...

3 OVERSIGHT AND ENFORCEMENT

In the absence of a data protection authority, the Council for Transparency (*Consejo para la Transparencia*) is the body responsible for ensuring government bodies comply with data protection, according to the Access to Information Law (Law No. 20.285/2008).[124] The Council for Transparency is independent and has administrative autonomy but lacks powers to impose penalties.[125] There is a controversy in Chile regarding the role of the Council for Transparency in overseeing data processing. Some experts argue that the Council for Transparency would be the controller of public databases. In contrast, others argue that its role is circumscribed to provide guidance on data protection practices for government bodies and resolve complaints about transparency requests.[126] Thus, there is not much clarity regarding the capacity of the Council for Transparency to act. As for data processed by private entities, there is an enforcement vacuum since there is no authority to ensure compliance with the data protection law.

SERVEL, the electoral management body, is responsible for the administration, supervision and inspection of electoral and plebiscitary processes; and for ensuring compliance with the rules of transparency, limits and control of electoral spending and the rules on political parties. SERVEL is composed of a board and a council. The council has five councilors appointed by the President of the Republic and confimed by the Senate. The council members' term is ten years, and they cannot be appointed for a new term. Terms are staggeredso that a new vacancy opens every two years. Members can only be removed by the Supreme Federal Court, at the request of the President of the Republic or one-third of the acting members of the Chamber of Deputies, for serious violation of the Constitution or the laws, incapacity, misconduct or negligence manifested in the exercise of their functions.[127]

Law No. 21200/2019, which established the rules for drafting the new Constitution, directs SERVEL to apply electoral rules, such as laws on voting, voter rolls and political parties. SERVEL is not empowered to apply the electoral expenditures law (Law No. 19884/2017). As a result, in the 2020 Plebiscite, SERVEL enforced spending limits by political parties but did not control spending by private individuals and companies — such on as social media.[128]

124 Art. 31, "m", Law No. 20.285/2008.

125 Electronic Frontier Foundation. The State of Communication Privacy Law in Chile, 2020. Available at: necessaryandproportionate.org/...

126 ADC por los Derechos Civiles. El sistema de protección de datos personales en América Latina: Oportunidades y desafíos para los derechos humanos. Volumen I. December, 2016. p. 31. Available at: adc.org.ar/...

127 Art. 94 bis, Constitution.

128 Garay, Vladimir. "Propaganda electoral digital: perfilamiento y noticias falsas". Derechos Digitales. March 12, 2020. Available at: derechosdigitales.org/...

In the judicial sphere, there are electoral courts. The Election Certifying Court (*Tribunal Calificador de Elecciones*) is the main electoral court, overseeing and certifying the elections for President of the Republic, deputies and senators.[129] Below the Election Qualifying Court, the Regional Electoral Courts (*Tribunales Electorales Regionales*) are in charge of voting counts and certifying other contests.

Yet, it is SERVEL, as the main body overseeing the elections — with authority to impose sanctions over violations of the rules on political campaigning, electoral offenses or violations of transparency —, who can intervene in issues of personal data processing. However, it has not been acting prominently. The Council for Transparency can make recommendations for Servel, for example. But individuals who think their data has been processed unlawfully must seek redress in court.

In 2020, the Council for Transparency alerted Servel that the publication of voter rolls was disproportionate, as it exposed too much of the personal data of voters.[130] According to the Council, the need to disseminate voter rolls for social control of the electoral process does not imply the need to provide personal data such as a personal address. So far, this has not had any effect on the publication of information by Servel.

In summary, Chile does not have a data protection authority. In certain cases, the Council of Transparency acts as a data protection authority, but with a reduced capacity to act since it can act only in what concerns the State administration's organs and cannot apply sanctions. Servel, which is the main administrative authority that protects the electoral process, can act in cases regarding data protection in the electoral context. However, there is an enforcement vacuum related to private entities, which are not under scrutiny either by the Council of Transparency or Servel.

4 OUTLOOK: A DATA PROTECTION PIONEER, NOW IN NEED OF UPDATES

Chile was the first country in Latin America to have a data protection law. However, legislation has not kept pace with technological advances and the new data processing capabilities. The Chilean data protection law authorizes the processing of any data that is accessible to the public, which brings little guarantee to the data subjects.

129 Art. 95, Constitution.

130 Consejo para la Transparencia. "CPLT apunta a exposición desproporcionada de datos personales vía padrón electoral". August 1st, 2020. Available at: consejotransparencia.cl...

In the electoral field, Chilean legislation has a personal data loophole in the publication of voter rolls. Servel is obliged to publish a list of all eligible voters before each election or plebiscite, along with their personal information.

The electoral and data protection legislation does not seem to create any safeguards against profiling by private companies, such as Instagis. Although such practices may have some legal support, it is widely criticized by media and experts. They argue that the companies that conduct election campaigns through voter profiling violate the data protection legislation because they process information about political preferences, which is a special category of data.

Yet, the absence of a data protection authority makes enforcement difficult. The Council for Transparency's jurisdiction is restricted to the State Administration's bodies, and there is no history of Servel's prominent role in data protection.

MEXICO

USE OF DATA BY CAMPAIGNS

Voter profiling and microtargeting. However, these strategies do not seem to be as relevant to the election results as the more traditional campaign strategies.

DATA PROTECTION FRAMEWORK

Constitutional right to privacy, constitutional right to data protection, constitutional right of a data subject to access, rectify and delete their personal data (art. 242). **Two Data protection laws**: one for public authorities and bodies, and the other for private entities (General Law on Protection of Personal Data in Possession of Obliged Subjects and the Federal Law on Protection of Personal Data Held by Private Parties).

SENSITIVE DATA

Data that refer to the most intimate sphere of the subject or whose improper use may lead to discrimination. Examples provided by the legislation: personal data that may reveal aspects such as racial or ethnic origin, present or future health status, genetic information, religious, philosophical and moral beliefs, sexual orientation, as well as **political opinions**.

EXCEPTIONS

Personal data from publicly-accessible sources. Under the law, public access sources are webpages; telephone directories, official newspapers or bulletins, means of social communication and public records.

DATA PROTECTION AUTHORITY

INAI (*Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*), an independent agency.

ELECTIONS MANAGEMENT BODY

National Electoral Institute (*Instituto Nacional Electoral*), a legally independent agency with the power to enact regulations regarding the electoral process.

ACCESS TO VOTER ROLL DATA?

Political parties have access to voter rolls. While voter rolls are not publicly accessible, there have been numerous cases in which this database was misused or sold illegally.

ELECTORAL PROVISIONS ON PERSONAL DATA PROCESSING?

No specific provision.

ENFORCEMENT

There are cases of sanctions by INE in connection to the illegal sale of the voter rolls.

1 CONTEXT OF THE USE OF PERSONAL DATA IN POLITICAL CAMPAIGNS

Mexico has a population of 120 million.[131] In 2019, 70.1% of the population had access to the internet.[132] Facebook is the most important social media in Mexico; almost 94% of internet users access the social media. Behind Facebook, WhatsApp (89%) and Instagram (71%) are among the most popular social media in the country.[133]

While not on the scale seen elsewhere, political campaigns in Mexico have been increasingly adopting data-driven digital strategies, including segmentation and geo-targeting. At each election, political campaigns have invested more resources in digital advertising.[134] WhatsApp plays an important role in Mexican political campaigns. Political parties use the app to send direct and personalized messages. According to a study by Tactical Tech and *Artículo 12*, the leading companies in this field are Audiense[135] and Nation Builder.[136] The study also showed that Cambridge Analytica worked with one of the political parties in Mexico.[137] However, it is unclear if this political profiling technique based on microtargeting on social media was effective. Even though the number of internet users is increasing, television and more traditional political campaigning practices are still very relevant in the country.[138]

131 According to 2015 Encuesta Intercensal (EIC). Available at: inegi.org.mx/...

132 According to Instituto Nacional de Estadística y Geografía (INEGI). Available at: en.www.inegi.org.mx/...

133 According to a study developed by We Are Social, in 2020. The research is available at: yiminshum.com/...

134 According to INE, in 2018, the electoral campaign spent 159 million pesos in advertising on the internet, being the second largest advertising expenditure of the campaigns. See more at: reuters.com/...

135 audiense.com

136 nationbuilder.com

137 The Mexican data protection opened an investigation regarding Cambridge Analytica in Mexico. However, as of writing, there have been no significant discoveries or developments regarding the company's operations in the country. See more at: br.reuters.com/...

138 InternetLab. "'Acho que nenhum mecanismo é eficaz para enfrentar uma guerra suja tão grande', diz candidata a deputada no México sobre a campanha na rede". August 24, 2018. Available at: www.internetlab.org.br/...

Irregular practices adopted by political campaigns, such as the purchase of votes, have also been deployed through internet campaigns, with the help of personal data collection.[139] In 2017, for example, Alfredo del Mazo Maza, a gubernatorial candidate, collected data from voters to send them cards called *"tarjetas rosas"* (pink cards) that held an amount of money to be activated if he candidate won the election.[140] Ahora, a civil society organization, reported the case to the Mexican electoral authority, the National Electoral Institute (*Instituto Nacional Electoral* – INE).[141] However, INE did not sanction Del Mazo for the pink cards. According to the Institute, the data collected for the pink cards only had electoral campaigning purposes and was not used for buying votes. In his defense, Del Mazo argued that citizens had the choice of offering or not their data to obtain the card.[142]

2 LEGAL FRAMEWORK

A THE MEXICAN ELECTORAL SYSTEM AND THE POLITICAL ADVERTISING

The Constitution provides that political parties and independent candidates can use the media — radio and television — to run electoral ads in accordance with the guidelines about time and days established by INE. Placing paid ads in the media is prohibited. The constitutional text does not contain any provision regarding the use of personal data or the internet for electoral purposes. The electoral rules within the Constitution are limited to television and radio ads.

The main law governing the electoral process is *Legipe*, the General Law on Electoral Institutions and Procedures[143] and, like the Constitution, it does not go into campaigning on the internet. Legipe provides that the electoral campaign is "the set of activities carried out by national political parties, coalitions and registered candidates to obtain the vote." It can be through any "set of writings, publications, images, recordings, projections and expressions produced and disseminated during the electoral campaign by political parties, registered candidates and their supporters, with the purpose of presenting candidates to the public".[144]

139 Tactical Tech, Artículo 12. "Mexico: How Data Influenced Mexico's 2018 Election". June, 2018. Available at: ourdataourselves.tacticaltech.org/...

140 Ibidem.

141 Aristegui Notícias. "Denuncia 'Ahora' entrega de tarjetas en Edomex para favorecer a Del Mazo". May 21, 2017. Available at: aristeguinoticias.com/...

142 Aristegui Notícias. "Castiga INE tarjetas rosas del PRI en Coahuila, pero perdona las de Del Mazo en Edomex". July 14, 2017. Available at: aristeguinoticias.com/

143 Ley General de Instituciones y Procedimientos Electorales, from 2014. Available at: diputados.gob.mx...

144 Art. 242, Ley General de Instituciones y Procedimientos Electorales.

According to interviewed experts, even though the law does not explicitly mention political campaigning on the internet, INE position is is that the requirements on ad spending by liticalparties also apply to social media and the internet.[145] *Legipe* requires political parties to be transparent about campaign expenditures, including on the internet. There are no provisions on data processing or permitted campaigning strategies on the internet.

B THE MEXICAN DATA PROTECTION FRAMEWORK

The Mexican Constitution enshrines the right to data protection, as well as data subjects' rights to access, rectify and delete their data.[146] Below the Constitution, major data protection laws are the General Law on Protection of Personal Data in Possession of Obliged Subjects[147] and the Federal Law on Protection of Personal Data Held by Private Parties.[148] The former applies to political parties, any authority or body in the Executive, Legislative and Judiciary, and autonomous bodies, trusts and public funds. The latter covers any natural or legal persons who process data privately. It is important to stress that even if the natural or legal person receives public money or performs acts of public authority, they will respond to the private data protection law.[149]

Both data protection laws are governed by the principles of legality, purpose, fairness, consent, quality, proportionality, information and accountability in the processing of personal data.[150] Only tacit consent is required unless the law expressly provides for explicit consent[151] Tacit consent is roughly equivalent to an opt-out: it is obtained if the information about the processing has been made available and the data subject has not objected to the processing. Explicit consent can be obtained orally, in written or by any other means.Explicit consent is required for sensitive data[152] Under the law, "sensitive data" is defined as those data that refer to the most intimate sphere of

145 Tactical Tech, Artículo 12. "Mexico: How Data Influenced Mexico's 2018 Election". June, 2018. Available at: ourdataourselves.tacticaltech.org/...

146 Art. 16, Constitución Política de los Estados Unidos Mexicanos.

147 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, from 2017. Available at: diputados.gob.mx/...

148 Ley Federal de Protección de Datos Personales en Posesión de los Particulares, from 2010. Available at: diputados.gob.mx/...

149 Art. 1 "(...) *Los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal serán responsables de los datos personales, de conformidad con la normatividad aplicable para la protección de datos personales en posesión de los particulares*.". Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

150 Art. 16, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados and art. 6, Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

151 Art. 21, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

152 Art. 9, Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

the subject or whose improper use may lead to discrimination. The law provides some examples for which data could be considered sensitive: personal data that may reveal aspects such as racial or ethnic origin, present or future health status, genetic information, religious, philosophical and moral beliefs, sexual orientation, as well as political opinions.

Consent, tacit or explicit, is not required for personal data that can be found in "public access sources".[153] Under the law, public access sources are (i) webpages; (ii) telephone directories, (iii) official newspapers or bulletins, (iv) means of social communication and (v) public records. Data illegally made available in public access sources fall outside this exception.[154]

The data protection law is quite permissive regarding data sharing, just as it is permissive regarding data processing. The subject's consent is not required for data sharing in the cases mentioned above and when sharing is necessary for the conclusion of the contract.

Beyond those aspects, in terms of enforcement, the law also presents problems. Non-compliance with the law can lead to sanctions, mainly fines, but it can even get to prison terms in some cases.[155] However, according to experts, the sanctions are rarely imposed; when they are, fines are typically not substantial enough to discourage new violations; and are at any rate challenged in administrative and judicial courts — seriously limiting enforcement of the law.

There are still issues regarding the scope of the two data protection laws. As mentioned above, the federal data protection law covers natural or legal persons, while the general data protection applies to political parties and public authorities. However, political parties usually hire private companies to carry out political campaigns and advertising strategies. As a rule, private companies respond under the terms of the private data protection law, but companies may also be understood as controllers (*encargado*)[156] under the law for obligated subjects. The law does not provide clear criteria for dealing with these cases, being left to the discretion of the electoral authority and the data protection authority.

153 Art. 22, VII Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados and art. 10, II, Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

154 Art. 5, Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

155 Art. 67-69, Ley Federal de Protección de Datos Personales en Posesión de los Particulares

156 Art. 3, XV. "Encargado: La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable". Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

B OTHER LEGISLATIONS

Mexico has a Consumer Protection Act that, among other provisions, regulates the practice of spam.[157] According to the law, it is prohibited to send advertising to consumers who have expressly stated their wish not to receive it; and companies are prohibited from using the data collected for marketing for other purposes. However, this provision is not applicable to electoral and political content, since the consumer protection law is only applicable to the provider (*proveedor*), which is the legal or natural person who distributes, sells or grants the use of goods, products or services.

3 OVERSIGHT AND ENFORCEMENT

The electoral management body in Mexico is the National Electoral Institute (*Instituto Nacional Electoral* – INE). INE is in charge of organizing, developing and counting the vote, and it is also responsible for regulating electoral advertising. It is a legally independent entity, and it can issue regulations regarding the electoral process.[158]

INE's main body is the General Council (*Consejo General*), composed of a president and ten electoral counselors. Legislative counselors may express opinions on the decisions of the CNE but without the right to vote. The members of the General Council are elected by the Chamber of Deputies.[159]

INE's decisions can be challenged in the Superior Electoral Court (*Superior del Tribunal Electoral del Poder Judicial de la Federación*).[160] There are concerns around the electoral court's capacity to act and be seen as acting in an independent, even-handed manner, insulated from partisan politics.[161]

157 Art. 18 bis, Ley Federal de Protección al Consumidor.

158 Art. 41, Constitution.

159 Ibidem.

160 Art. 35, IX, 5°, Constitution.

161 Pizaña, Felipe. "Hacia una garantía efectiva de la autonomía e independencia de los tribunales electorales locales". Nexos: Cobertura especial Justicia Electoral. April 9, 2018. Available at: eljuegodelacorte.nexos.com.mx/... García, Ariadna. "Advierte Córdova que la autonomía electoral está en riesgo". El Universal. September 9, 2020. Available at: eluniversal.com.mx/... ; Letras Libres. "El INE en la mira". November 19, 2019. Available at: letraslibres.com/...

Mexico also has a data protection authority, the *Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*, known as INAI. The Institute is composed of seven commissioners, appointed by the Senate after consultation with society. The appointment can be challenged by the President within 10 days. The president of INAI is chosen through commissioners' secret voting. From an administrative point of view, INAI is an autonomousbody.[162] However, it is not completely financially autonomous since the Chamber of Deputies establishes, every year, the annual budget for the Institute, which can lead to financial pressure.[163]

In case of violation of the data protection law in the electoral context, both authorities can act. Under the terms of the law, the investigation must be conducted by the electoral authority,[164] and INAI must issue technical advice to the National Electoral Institute regarding the issues related to data protection. However, INAI can also sanction the political party in the event of misuse of personal data.[165] The decisions issued by INAI can be challenged in Court.[166]

According to the interviewed experts, in general, each authority tries to stay limited to its scope and avoid overstepping their jurisdiction, but they can work together if it is necessary. For example, in 2018, through an official communication,[167] INAI announced that it would be "a partner of the [electoral] guarantor bodies" and that it would be "able to verify, inspect and monitor the fulfillment of the institutional obligations of transparency, especially of personal data".[168]

The data protection and the electoral authorities have been involved in cases regarding voter rolls. Mexico voter rolls contain the voters' personal data, and, unlike other Latin American countries, they are not publicly accessible; only political parties have access to the database. There are many cases where this database has been illegally sold or has been misused.[169] In 2018, INAI started an investigation against a candidate for misuse of the voter rolls.[170]

162 Art. 18, Ley Federal de Transparencia y Acceso a la Información Pública.

163 Art. 22, Ley Federal de Transparencia y Acceso a la Información Pública

164 Art. 163, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

165 Art. 166, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

166 Art. 162, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

167 Comunicado INAI/114/18. April 20, 2018. Available at: inicio.inai.org.mx/...

168 In the original: "El INAI será compañero de los órganos garantes porque en selectivos, pero importantísimos momentos podremos verificar, inspeccionar y acompañar los cumplimientos de los deberes institucionales de transparencia, sobre todo de datos personales".

169 Onofre, Julio Sánchez. "Base de datos del padrón electoral nunca ha sido vulnerada: INE". El Economista. January 26, 2017. Available at: eleconomista.com.mx/...

170 Huerta, Juan Carlos. "INAI investiga a Marichuy por mal uso del padrón electoral". El Financiero. January 25, 2018. Available at: elfinanciero.com.mx/...

In 2020, the *Revolucionario Institucional* Party was sanctioned by INE after placing the database for sale on *Mercado Libre*, an online buying and selling platform.[171] The political party was fined an amount of 84,3 million pesos.

In summary, both INAI and INE can investigate and sanction misuse of personal data in the electoral context. However, except in the most dramatic cases regarding the voter rolls, there is no evidence of prominent action by the authorities. INAI is seen as lacking teeth, and INE is perceived as not taking data protection to be one of its priorities.

4 OUTLOOK: DIGITAL CAMPAIGNING STILL NOT FRONT AND CENTER, REGULATION OF THE USE OF PERSONAL DATA NOT TOP PRIORITY

The use of personal data in political campaigns, as well as digital advertising, has grown in Mexico. However, television and more traditional campaign tactics still seem to be the most important strategies for advertising.

Mexican electoral legislation — even though it has been enacted recently, in 2014, — does not address electoral campaigns on the internet or electoral advertising based on personal data. Most of the regulation on data protection and elections is concentrated on transparency obligations.

The data protection legislation leaves much to the interpretation of the data protection authority, which has not yet taken any bold action in implementing data protection law. The rules regarding tacit consent make room for extensive data processing, including in the electoral context.

Finally, the enforcement of the law by the electoral authority and the data protection authority appears insufficient. The cases involving the voter rolls evidence a systematic problem in data security, data protection and accountability.

171 Infobae. "Intento de vender el padrón electoral en Mercado Libre le costará 84.3 mdp al PRI por sanción del INE". November 27, 2020. Available at: www.infobae.com/...

PARAGUAY

USE OF DATA BY CAMPAIGNS

Digital campaign strategies that seem as relevant to electoral results have not been identified.

DATA PROTECTION FRAMEWORK

Constitutional right to intimacy (art. 33). Private Information Law, which provides the economic or patrimonial data privacy (Law No. 1682/2001). **No data protection law.**

SENSITIVE DATA

Those that promote prejudice and discrimination, or affect dignity, privacy, domestic intimacy and the private image of individuals or families, such as those that refer to racial or ethnic belonging, political preferences, individual health status, religious, philosophical or moral beliefs.

EXCEPTIONS

The storage and processing of sensitive data is allowed only for scientific, statistical, opinion polls, or market research purposes. There is no mention of the need for consent regarding databases that contain: name and surname, id, address, date and place of birth, occupation or telephone number.

DATA PROTECTION AUTHORITY

There is **no data protection authority** in Paraguay.

ELECTIONS MANAGEMENT BODY

Superior Electoral Court of Justice, part of the **judiciary.**

ACCESS TO VOTER ROLL DATA?

Political parties have access to the voter rolls a month before elections.

ELECTORAL PROVISIONS ON PERSONAL DATA PROCESSING?

There is no specific provision.

ENFORCEMENT

There are no reports of investigations regarding the use of personal data by political campaigns.

1 CONTEXT

Paraguay has a population of 7 million.[172] In terms of Internet usage in 2018, the percentage of mobile broadband penetration was 53.70%, while the penetration of fixed broadband Internet was only 4.8%.[173] According to the Economic Commission for Latin America and Caribe (ECLAC), the country maintains high inequality rates on internet access between the richest quintile of its population and the poorest, about 20 percentage points; and a similar connection gap exists between urban and rural areas in Paraguay.[174] The most important social media in the country is Facebook, with 3.8 million users, followed by Instagram, with 3.6 million users.[175]

Since 2017, the increasing use of social media in an electoral context has attracted the attention of parties and social movements, especially after the *Asociación Nacional Republicana* (ANR), also known as *Partido Colorado,* presidential primaries. According to the NGO *Tecnología y Comunidad* (TEDIC), between November 2017 and January 2018, 150.000 tweets were published about the Party's internal disputes.[176] Subsequent general elections took place on 22 April 2018. During the election campaign, the main presidential candidates were Mario Abdo of the Colorado Party (ANR) and Efrain Alegre, from *Alianza Ganar*, a coalition composed by the Liberal Party (PLRA), *Frente Guasu* and other left-leaning parties. During the electoral campaigns period, March 15 to May 3.2018, 104.515 tweets were shared from those that used hashtags or handles of campaigns and candidates.[177]

According to TEDIC, "currently, the generation of content on Twitter does not reflect what happens outside social media. The political groups that were most popular on Twitter did not win the elections. Moreover, there are no signs of high polarization since in both elections, over 80% of the accounts that generated content were 'neutral', which means they did not support any political group. It was possible to identify accounts with features of bots and fake accounts in both elections."[178]

172 countrymeters.info/es/Paraguay

173 TEDIC. Como és la infraestrucutra de internet en paraguay. Available in: tedic.org/...

174 ECLAC. Estado de la banda ancha en América Latina y el Caribe repositorio.cepal.org/...

175 latamclick.com/...

176 TEDIC. El Rol De Twitter En Las Elecciones Generales De Paraguay 2018. Available at: www.tedic.org/...

177 ibid.

178 TIDIC. T*witter and elections in Paraguay*. Available at: tedic.org/...

The perceived low significance of digital campaigning might reflect the country's low connectivity rate, particularly in rural areas. According to the Final Report to Election Observation Mission of the European Union in Paraguay,[179] despite the great importance of social media, citizenships continue to fundamentally depend on the traditional media to be informed on political matters, and newspapers are the ones that determine the agenda of the electronic media. It is compounded by the lack of legislation in the country related to online election advertising.

2 LEGAL FRAMEWORK

A THE PARAGUAYAN ELECTORAL SYSTEM AND THE POLITICAL ADVERTISEMENT

In Paraguay, elections are governed by the 1996 Electoral Code.[180] The Superior Electoral Court of Justice (SCEJ) is the Paraguayan electoral management body, organizing and monitoring general, departmental and municipal elections.

The Code distinguishes between political advertising and electoral advertising. Political advertising is defined as advertising aimed at communicating political doctrines and information to affiliates in particular and public opinion in general (article 286), and electoral advertising is defined as the communication of the electoral platform aimed at eliciting electoral support (article 290). While political advertising is guaranteed throughout the year, electoral advertising is subject to the terms within the election framework. The Electoral Code authorizes the use of public spaces and media – radio, television and newspapers – to place electoral advertisements, but contains no provision regarding the use of personal data or the internet for electoral purposes.

Regarding paid electoral advertising, the only provision of the Electoral Code is that the mass media are obliged to issue to the Electoral Tribunal of the constituency their ordinary tariffs for the advertising space sold. However, this article (article 299) does not define what can be considered "mass social media"; therefore, it is ambiguous whether social media platforms can fall into this category.

179 Report produced by the European Union Election Observation Mission to the Republic of Paraguay and presents the mission's findings on the 2013 general elections. Available at: aceproject.org/...

180 Electoral Code. Available at: www.bacn.gov.py/...

B THE PARAGUAYAN DATA PROTECTION REGIME

Under the Paraguayan Constitution,[181] two provisions are important to data protection. The first of them is article 33, which regulates private life as "Right to intimacy" (*Intimidad*):[182]

> Personal and family intimacy, as well as the respect of private life, is inviolable. The behavior of persons, that does not affect the public order established by the law or the rights of third parties[,] is exempted from the public authority. The right to the protection of intimacy, of dignity, and of the private image of persons is guaranteed.[183]

Following these guidelines, in 2001, Law 1682/2001 (Private Information Law - PIL)[184] was enacted, and a year later, Law 1969/2002 specified its requirements.[185] Both laws aim to preserve the privacy of Paraguayan citizens. They provide a definition of sensitive data in Article 4: those that refer to racial or ethnic belonging, political preferences, individual health status, religious, philosophical or moral beliefs; sexual intimacy and, in general, those that promote prejudice and discrimination, or affect dignity, privacy, domestic intimacy and the private image of individuals or families.

The PIL allows the collection, storage and processing of data only for scientific, statistical, opinion polls, or market research purposes. However, it does not mention the need for consent, besides allowing the publication of databases that contain: name and surname, id, address, date and place of birth, occupation or telephone number. Regarding sanctions, the PIL prevents them only in case of disclosure of economic or patrimonial data.

Due to the PIL limitations, on 26 March 2019, a bill was filed before parliament. This project is currently under review by Paraguay's legislature for the purposes of creating a more comprehensive data protection regulatory regime.[186] This bill aims to strengthen the position of rights holders. It is divided into six chapters, which aim to incorporate new principles and basic rights regarding personal data protection, such as intimacy, informational self-determination,

181 Paraguay's Constitution of 1992 with Amendments through 2011. Available at: www.oas.org/...

182 The other is the article 135, that enshrines the right to habeas data: All persons may access information and data about themselves, or about their assets, kept in official or private registries of a public character, as well as to know the use made of the same and of their end. [All persons] may request, before the court with jurisdiction, the rectification or the destruction of such information, if inaccurate or illegitimately affecting their rights.

183 "*La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables. La conducta de las personas, en tanto no afecte al orden público establecido en la ley o a los derechos de terceros, está exenta de la autoridad pública. Se garantizan el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas.*"

184 Available at: bacn.gov.py/...

185 Available at: bacn.gov.py/...

186 This bill is the result of an intersectoral effort in the country. More information about the project and its formulation is available at: tedic.org/...

liberty, data security, duty of secrecy, and fair processing. It designates the Central Bank of Paraguay (BCP) as the supervisory authority for credit information and the relevant entities which process the same. Furthermore, it establishes the Consumer Protection Secretariat as the supervisory authority for every other type of entity that processes personal data. It deals with infringements and sanctions for breaches of the law and combines the sanctions already contemplated in the law with new ones created under any regulations made pursuant to the law. It also provides for sanctions in different degrees of severity. The project, however, is still subject to final approval.

C OTHER LEGISLATION

Paraguay has an anti-spam law that prohibits unauthorized advertisements on cell phones, Law 5830/17.[187] This law creates a National Registry in which consumers and users can register to prevent providers from making commercial contacts through their mobile phone numbers. This provision, however, does not apply to electoral and political content.

3 OVERSIGHT AND ENFORCEMENT

The leading authority in electoral matters in Paraguay is the Superior Electoral Court of Justice (SCEJ), which is part of the structure of the judiciary. Among the many duties bestowed thereto by Law 635/1995,[188] which regulates the electoral justice, are the call and declaration of nullity of elections; control, patrimonial auditing, and organization of the internal elections in political parties; setting the number of seats corresponding to each province in the House of Representatives and the provincial boards; distribution of state economic contributions and subsidies to political parties; resolution of electoral appeals; and the proclamation of elected candidates.

The SCEJ co-directs the Civil Registry and the Department of Identifications of the National Police of Paraguay, given the significant role both institutions play in the identification of adults entitled to vote. Decisions of the SCEJ can only be challenged before the Supreme Court of Justice and only through an unconstitutionality process. In its highest hierarchy level, the Court is headed by three magistrates treated as ministers. These magistrates are elected by the Senate, which votes in groups of three candidates proposed by the Magistracy Council.

187 Available at: digesto.senado.gov.py/...

188 Available at: bacn.gov.py/...

Since magistrates are necessarily elected in virtue of a pact between political forces capable of reaching a majority in the Senate, it is informally deemed they represent one of the three main political parties. Indeed, magistrates declare their political affiliation openly, and this is not deemed incompatible with their necessary independence as electoral arbitrators.[189]

The Electoral Justice structure in Paraguay is composed also of tribunals, electoral courts, and civic boards. Electoral tribunals replicate the structure of the SCEJ at provincial levels. Included in their duties are: head and audit elections, audit voters' registry, resolve recourse against electoral courts' decisions under their jurisdiction, perform provisionary counts of the elections (totaling district results) and integrate civic boards.

Apart from the electoral tribunals, there are courts and electoral prosecutors for each province. Among the more noticeable attributions of electoral tribunals and courts are: resolving challenges, recusals and inhibitions of judges and prosecutors of their jurisdiction; designating polling stations and the members of the electoral tables; receiving and organizing the distribution of materials; certifying representatives of the political parties; and conforming the civic boards. Civic Boards are the last step in the structure of the electoral administration. They are provisional bodies constituted between 60 days before and 30 days after elections in every country district. They are made of five members designated by the electoral tribunals upon a proposal of the parties, always based on the representation of the parties in the Senate. The boards are responsible for proposing polling stations, certifying suppliers, and receiving and distributing voting materials.

Regarding privacy protection, the Private Information Law does not create or provide for a specific data protection authority; consequently, when faced with infringements, individuals or legal entities are required to file individual complaints before civil courts. Therefore, if there are violations during electoral campaigns, these will be dealt with by SCEJ and its subordinate bodies. As previously mentioned, there is a draft law under discussion that aims to turn the Consumer Protection Secretariat into a data protection authority, but this is still an embryonic process.

4 OUTLOOK: AS CONNECTIVITY GROWS, PARAGUAY STILL LACKS A DATA PROTECTION LAW

In Paraguay, considering the low universalization of internet access, the electoral advertisement system is still very focused on traditional media, such as television, radio and newspapers. However, the internet and social media have garnered the interest of parties and social movements, making platforms a space for public debate, especially in urban centers. However,

189 Currently composition of the SCEJ, available at: tsje.gov.py/...

the country's electoral laws are not keeping up with this movement, not regulating the use of these tools in election campaigns. At the same time, the data protection system remains incipient, focusing only on commercial data, without a data protection authority or a comprehensive data protection law in accordance with international standards.

CONCLUSION: THE MISSING BRIDGES BETWEEN ELECTORAL MANAGEMENT AND DATA PROTECTION FRAMEWORKS

The landscape in Latin America is quite diverse. Throughout the region, campaigns have adopted digital strategies to different degrees, seemingly at pace with the increase in internet access rates in each of the countries we analyzed. In Argentina, Brazil and Chile, where connectivity is higher, candidates and political parties have increasingly turned to digital ads; and the news has reported some engaged the notorious Cambridge Analytica services — with unclear results. In Colombia and Paraguay, lower connectivity has meant discussions around digital campaigns are not as conspicuous. In Mexico, where connectivity reaches just above 70% of the population, agencies offered their services, yet that was perceived as playing a minor role compared to more traditional campaigning.

The outlook of data protection also varies considerably. Paraguay still lacks a data protection law. The Brazilian General Data Protection Law has only very recently entered into force. Chile, a pioneer in the region, struggles to enforce its data protection legislation without a data protection authority. In Mexico, enforcement action by the data protection authority is still incipient, and, in Colombia, questions about the real independence of authority members have been raised. The authority in Argentina stands out, having issued, in 2019, guidelines on personal data processing for elections. However, it is still unclear how parties and campaigns have been compliant with the guidelines.

Enforcement action of data protection law in the electoral context in the region has been episodic at most, and generally lacking. In Brazil, the Superior Electoral Court has long monitored and enforced rules on digital campaigning, although that has not stopped serious questions being raised around the last presidential elections. If regulation was initially focused on promoting a level playing field for the electoral process to take place — banning electronic addresses databases from being sold —, with the entry into force of the new General Data Protection Law (LGPD), the electoral court revised its rules to also include the data subject's interest in data protection. However, it is still too soon to assess the impact of that change.

A common thread in data protection law in the region is categorizing data on political opinions or affiliation to political organizations as sensitive data, subject to stricter processing requirements. That could be an important factor in governing ad strategies that relies on voter profiling, for instance. Yet this has not been featured in discussions on data protection and elections.

Electoral law and electoral management bodies are a particular point of comparison in the countries we analyzed. In some countries, elections are held and overseen by an agency, with more (Chile) or less (Colombia, Mexico) autonomy from elected officials and distance from partisan politics. In Brazil, Argentina and Paraguay, organizing the elections and enforcement of electoral law fall upon the judiciary. Except for the Brazilian EMB and the very general guidelines issued by the Argentine EMB, electoral management bodies have not issued regulations about data protection for electoral contests. They are also not seen as actively monitoring campaign use of personal data — and neither are the data protection agencies.

In fact, in many of the countries (Argentina, Chile, Mexico), not only are electoral authorities not leveraging data protection law to ensure elections are fair, but the reverse has happened: transparency requirements around voter rolls (*padrones electorales*) are seen as exposing excessive personal data from voters, and creating opportunities for abuse, both by campaigns and other actors, including those unconnected to elections. Argentina has amended its electoral legislation to ban the use of voter rolls data for commercial purposes, including by creating a criminal offence. However, the impact for the efficient protection of personal data is yet to be determined.

Our study finds that enforcement of data protection in the electoral context is of growing significance in the region — and unlawful processing has led to rescinded contests (Colombia). However, neither electoral nor data protection authorities have adopted a comprehensive approach to regulating actors. Enforcement action by authorities generally faces three challenges:

- a lack of coordination by electoral and data protection authorities, leading to neither regarding itself as responsible;
- concerns over the independence of authorities that lack autonomy from the executive or partisan politics, leading to distrust of their capacity to apply data protection law without compromising competition between candidates and parties and, finally,
- a serious lack of information about campaign use of personal data and the role of data in digital campaigning — when present, transparency requirements are limited to expenditures and official account registration.

With campaigns increasingly adopting digital strategies, data protection is key to ensuring that the electoral process is fair. Data protection experts and officials and their electoral counterparts must engage with each other to achieve that goal.