


CIVIC COMPASS

A CIVIC HOUSE unit

Data Protection Laws and Civil Society: Navigating the GDPR Impact



Cecilia Galvan (Civic House - University of Buenos Aires)
Orla Lynskey (London School of Economics and Political Science)
Katherine Nolan (Ulster University)
Gaston Wright (Civic House, Torcuato Di Tella University)

Introduction

Data protection is essential for individuals, businesses, and governments in the digital age. As vast amounts of data are collected, processed, and stored, ensuring the privacy, security and fair use of such data has become a significant challenge. Policymakers worldwide have adopted various data protection laws to safeguard individual privacy and data protection while pursuing other objectives, including economic growth and securing human rights. One influential data protection regulation is the European Union's General Data Protection Regulation (GDPR), which has had profound implications for various sectors, including non-governmental organisations (NGOs)² and has served as a model for data protection laws worldwide.

This paper delves into the relationship between data protection laws and civil society, particularly the potential repercussions for actors in civil society. The GDPR is a rigorous law that aims to safeguard individuals' rights, particularly data protection and privacy, setting a global benchmark for data protection standards. However, while such laws aim to protect individuals, they also have consequences for civil society. Drawing insights from the implementation of GDPR in Europe and juxtaposing it with the case of Brazil in Latin America, we aim to shed light on some of the challenges and lessons learned. We also aim to explain the impact of strict data protection laws on NGOs, focusing on the challenges and implications for non-profit organisations with limited compliance capacity. By understanding the multifaceted effects of data protection regulations, we hope this paper provides valuable information for policymakers regarding the risks of adopting a 'copy-paste' model of GDPR without having regard to local context.

The analysis proceeds as follows. In section 1, we outline how the GDPR works. In section 2, we introduce some of the critical challenges associated with the GDPR. In section 3, we offer initial thoughts on how some of these challenges might be mitigated. Then, in section 4, we delve into the impact a law like GDPR can have on civil society organisations. In section 5, we discuss Brazil's General Data Protection Law (LGPD) and its implications for NGOs, focusing on the particular context of Bolsonaro's government. Finally, in section 6, we summarise the advantages and disadvantages of comprehensive frameworks for data protection, and we provide a series of recommendations for policymakers.

¹This research was made possible through the generous support of the Mott Foundation and Luminate. We extend our sincere gratitude for their commitment to advancing knowledge and understanding in this field. Additionally, we would like to express our gratitude to Katia Peirano, Research Assistant at the University Torcuato Di Tella, for her dedicated assistance throughout this study.

²Schmitt, Miller, & Skiera (2021).

1. Understanding the GDPR

In this section, we introduce three key elements to aid in understanding the GDPR. First, we explain the basic structure and operation of the GDPR. Second, we introduce the influence of EU data protection laws in other jurisdictions, including the connection to the rules on data transfers under the GDPR. Third, we discuss the broader legal context in which the GDPR operates.

1.1. Lawful data processing

The GDPR replaced the 1995 Data Protection Directive³, which was the first piece of data protection legislation adopted at the EU level.

The GDPR provides a broadly applicable framework for the legality of data processing, though it sits alongside complementary legislation⁴ and there are exclusions to its application.⁵

The GDPR applies to the processing of personal data wholly or partly by automated means or processing of data in filing systems⁶. The main regulated person under the GDPR is known as the 'data controller', who can be a natural or legal person.

The obligations under the GDPR to which the data controller is subject are extensive⁷. Additionally, data subjects are granted rights which they can exercise against data controllers (rights of access, to rectify, to erasure, to restriction, to portability and to object)⁸. The GDPR also creates an enforcement structure to oversee the law's implementation and application⁹. Integral to this enforcement structure is the role of independent data protection authorities tasked with monitoring and ensuring its enforcement.

1.2. The influence of EU data protection laws in other jurisdictions

EU data protection law has been very influential around the world¹⁰ and has been observed by Bradford as an example of the 'Brussels effect'¹¹, the de facto and de jure impact of EU law beyond the EU's borders¹². Several factors contribute to the replication of EU data

³ DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23/11/1995, p 31-50).

⁴ See section 2.3 below.

⁵ See further section 3.1 below.

⁶ Article 2(1), GDPR.

⁷ See section 3.2.

⁸ Articles 15-21, GDPR.

⁹ See section 3.4

protection style laws in other jurisdictions. One crucial factor is the EU's rules regarding data transfers outside the EU.

The default position under the GDPR, and its predecessor Directive, is that transfers of data outside the EU are prohibited unless certain conditions are in place.¹³ There are broadly three ways of legitimising a data transfer: relying on an adequacy decision,¹⁴ ensuring appropriate safeguards are in place¹⁵ or relying on a derogation (such as consent or contractual necessity).¹⁶

The European Commission adopts adequacy decisions, which legitimise data transfers to particular countries or territories. The GDPR empowers the Commission to assess the legal regimes of non-EU states (or territories or sectors thereof) and issue an adequacy decision where it deems that the country 'ensures an adequate level of protection'¹⁷. In Latin America, Argentina¹⁸ and Uruguay¹⁹ were deemed adequate by the Commission under the Data Protection Directive. Ordinarily, these decisions should be kept under regular review; however, this periodic review policy has not been applied consistently. The first review of the adequacy decisions adopted under the Data Protection Directive was reported on 15 January 2024, and the Commission determined that all countries deemed adequate under the Data Protection Directive continued to provide an adequate level of protection.²⁰ The adoption of laws which mirror the protections of the Data Protection Directive or the GDPR has been influential in the making of an adequacy decision by the Commission, one factor which has led to the mirroring of the GDPR in other jurisdictions.

¹⁰ See e.g. Graham Greenleaf, 'Now 157 Countries: Twelve Data Privacy Laws in 2021/22' (2022) 176 *Privacy Laws & Business International Report* 3.

¹¹ Such was the case in initiatives that later became law in Brazil, Paraguay and more recently in Ecuador, that adopt to a greater or lesser extent some standards and good practices collected by said regulation. This milestone was preceded by other regional developments, such as the creation of the "Standards for the protection of personal data" by the Ibero-American Data Protection Network.

¹² Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020) xiv.

¹³ Article 44, GDPR; Article 25, Data Protection Directive.

¹⁴ Article 45, GDPR; Article 25, Data Protection Directive.

¹⁵ Article 46, GDPR; Article 26(2), Data Protection Directive.

¹⁶ Article 49, GDPR; Article 26(1), Data Protection Directive.

¹⁷ Article 45(1), GDPR; Article 25(1), Data Protection Directive.

¹⁸ 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.

¹⁹ 2012/484/EU: Commission Implementing Decision of 21 August 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data (notified under document C(2012)5704.

²⁰ Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC, Brussels, 15.1.2024 COM(2024)7 final.

https://commission.europa.eu/system/files/2024-01/JUST_template_comingsoon_Report%20on%20the%20first%20review%20of%20the%20functioning.pdf

1.3. Understanding the GDPR in context

The GDPR should be contextualised within the EU legal order to acknowledge (i) that the GDPR exists alongside other data processing laws, (ii) that the GDPR is connected to the EU's fundamental rights initiatives, and (iii) that the GDPR is implemented into the domestic legal systems of EU Member States.

First, the GDPR exists within a broader legal landscape. While the GDPR might be said to provide the baseline protection for personal data in EU law, there are parallel and intersecting laws that also address data protection, privacy, and related matters. Complementary legislation exists to protect personal data and privacy within electronic communications, including rules about tracking communications metadata and the deployment of tracking technologies like cookies.²¹ Separate legislation exists to protect the use of personal data for law enforcement purposes,²² and within the EU institutions.²³ The Data Governance Act provides rules for certain re-use of data by public sector bodies, for data intermediation services and concerning data altruism.²⁴

The recently adopted Digital Markets Act²⁵ and Digital Services Act²⁶ create additional rules for certain 'gatekeeper' providers of core platform services and rules regarding online platforms, with additional responsibilities for Very Large Service Providers and Search Engines. These platform rules have certain functional overlaps with the data processing governed by the GDPR. The new Data Act²⁷ and proposed European Health Data Space Regulation,²⁸ when implemented, will also have overlaps with the GDPR.

²¹ DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31/7/2002, p 37-47) 200. Note, a legislative proposal to reform this Directive has been made, though agreement on reform has not yet been made.

²² DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4/5/2016, p 89-131).

²³ REGULATION (EU) 2018/1725 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21/11/2018, p.39-98).

²⁴ REGULATION (EU) 2022/868 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (OJ L 152/1, 3/6/2022, p.1-44).

²⁵ REGULATION (EU) 2022/1925 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (OJ L 265/1, 12/10/2022, p.1-66).

²⁶ REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277/1, 27/10/2022, p.1-102).

Second, the GDPR should be understood as connecting to the EU's fundamental rights protections. The GDPR gives expression to the fundamental right to data protection, a right protected by Article 8 of the Charter of Fundamental Rights of the European Union (the 'Charter'), but more broadly in its subject matter, it has a fundamental rights mission. Article 1(2) of the GDPR provides that it 'protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.' The Charter, alongside the right to respect for private life under the European Convention on Human Rights, has played a crucial role in developing EU data protection law. Other rights, particularly freedom of expression and the right to an effective remedy, are frequently cited and balanced by the European Court of Justice ('ECJ') in data protection cases.

Third, we recall that the GDPR is implemented within EU Member State legal regimes. Although it is an EU regulation, there are a number of areas where Member States are permitted to restrict the GDPR's protections.²⁹ Additionally, there are areas where the GDPR permits variable levels of data protection, and Member States are permitted to vary the GDPR standard in their domestic systems.³⁰ Because EU Member States largely have autonomy over national procedural law, there is also variance in local enforcement and oversight procedures.³¹

²⁷ *REGULATION (EU) 2023/2854 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act) (OJ L 2023/2854, 22/12/2023), p.1-71).*

²⁸ *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space COM/2022/197 final.*

²⁹ *See section 4.3 below.*

³⁰ *For example, the GDPR provides a default age of 16 as the age at which children may consent to data processing in relation to certain information society services, but Member States may adopt an age between 13-16. Article 8(1), GDPR.*

³¹ *Though note that the Commission opened a consultation to provide for some administrative harmonisation in this space in early 2023.*

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13745-Further-specifying-procedural-rules-relating-to-the-enforcement-of-the-General-Data-Protection-Regulation_en

2. Key challenges of GDPR

There are four particular challenges of the GDPR model which we highlight for attention: (i) its broad scope of application, (ii) the one-size-fits-all model of responsibility, (iii) the impact on freedom of expression and (iv) potential enforcement consequences.

2.1. Scope

One persistent criticism of the GDPR is its overly broad material scope. Purtova named EU data protection law the 'law of everything' because of its broad reach.³² This criticism is heard from both those who believe the GDPR is overreaching (i.e. improperly regulating data usage, which should not be subject to the law) and also from those who are concerned that the breadth of the law's application undermines its enforceability.

The material scope of the GDPR is defined by reference to the processing of 'personal data'. Processing is understood very broadly, essentially applying to any use of data, including the collection of data without further use.³³ Personal data is defined as 'any information relating to an identified or identifiable natural person ('data subject')'.³⁴ 'Personal data' has also been confirmed to have a wide interpretation, and the threshold for identifiability of underlying individuals is relatively low. Notably, the ECJ has continually emphasised the importance of taking a broad interpretation to ensure adequate protection of data subjects.³⁵

In turn, the exclusions to the GDPR's application are generally narrowly interpreted. The GDPR does not apply to the processing of personal data, which falls outside the scope of EU law, notably Member States' national security purposes.³⁶ Nevertheless, the ECJ has determined that this exception does not apply where service providers are retaining personal data for national security purposes, and EU law does apply.³⁷ The GDPR does not apply to the processing of personal data 'by a natural person in the course of a purely personal or household activity'³⁸. Again, this has been interpreted narrowly and does not apply to placing data online, rendering it accessible to an indefinite number of people.³⁹

³² Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 *Law, Innovation and Technology* 40.

³³ Article 4(2), GDPR.

³⁴ Article 4(1), GDPR.

³⁵ See e.g. *Case C-582/14 Breyer* (ECLI:EU:C:2016:779); *Case C-434/16 Nowak* (ECLI:EU:C:2017:994).

³⁶ Article 2(a) and (b), GDPR.

³⁷ *Case C-623/17 Privacy International* (ECLI:EU:C:2020:790).

³⁸ Article 2(c), GDPR.

³⁹ *Case C-101/01 Bodil Lindqvist* [2003] ECR I-12992. See also *Case C-212/13 Ryneš* (ECLI:EU:2014:2428) and *Case C-25/17 Jehovan todistajat* (ECLI:EU:C:2018:551).

2.2. Model of responsibility

The GDPR primarily operates on a 'one-size-fits-all' approach to regulation, with most obligations attaching to the regulated 'data controller'. These obligations are quite onerous and can involve compliance costs, with limited accommodation of small-to-medium enterprises and no exclusions for not-for-profit entities.

The 'data controller' is defined as 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'.⁴⁰ The data controller is the main entity regulated by the GDPR, though entities which process data on their behalf ('data processors') are also subject to some obligations. The concept of the data controller is to be interpreted broadly according to the ECJ to ensure effective and complete protection of data subjects.⁴¹ Notably, where more than one entity has influence over the data processing, those entities can be deemed joint data controllers. In a series of ECJ cases, this notion of joint data controllers has been widely interpreted to mean that in some cases, users of social media or other online tools, such as plug-ins or analytics tools, can lead to those users being regarded as joint or co-controllers of data processed by the tool in question.⁴²

The obligations a controller faces to process data lawfully are significant and relatively complex. To lawfully process data, controllers must be able to demonstrate they comply with the data protection principles,⁴³ and have a legal basis to process data (e.g. consent or a legal obligation).⁴⁴ Heightened rules are in place for the processing of some special categories of data.⁴⁵ Additionally, controllers have transparency and compliance obligations, which can involve the requirement to appoint a data protection officer.⁴⁶ Special rules are in place governing data transfers out of the EU,⁴⁷ for data security and responses to data breaches,⁴⁸ regarding automated decision making,⁴⁹ and requiring the data controller to engage in data protection by design and by default.⁵⁰

⁴⁰ Article 4(7), GDPR. Note that in certain cases that the controller might be defined in legislation, where the processing to be conducted is set out in such legislation.

⁴¹ Case C-131/12 *Google Spain and Google* (ECLI:EU:2014:317).

⁴² Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein* (ECLI:EU:C:2018:388); Case C-25/17 *Jehovan todistajat* (ECLI:EU:C:2018:551).

⁴³ Article 5, GDPR.

⁴⁴ Article 6, GDPR.

⁴⁵ Article 9, GDPR.

⁴⁶ Articles 12-14, GDPR; Chapter IV, GDPR.

⁴⁷ Chapter V, GDPR.

⁴⁸ Articles 32-34, GDPR.

⁴⁹ Article 22, GDPR.

⁵⁰ Article 25, GDPR and Articles 35-36, GDPR.

2.3. Relationship with freedom of expression

One continual tension seen in EU data protection law is its relationship with freedom of expression. Formally, both are recognised as fundamental rights under the EU Charter, but balancing these rights can be challenging. Some perceived overreach has been noted by critics of the GDPR's impact on freedom of expression/public access to information.

Formally, the GDPR recognises the need to balance the right to data protection with freedom of expression in a number of specific provisions. The right to erasure may be limited where necessary for the exercise of freedom of expression.⁵¹ Member States are required to reconcile the right to data protection and freedom of expression and information in domestic law, including processing for journalistic purposes and the purposes of academic, artistic and literary expression.⁵² For such purposes, Member States are to provide exemptions or derogations from many of the GDPR's obligations.⁵³

The ECJ has articulated the balance between freedom of expression and data protection in the context of a series of cases on the so-called 'right to be forgotten'. Established in *Google Spain*, the right to be forgotten entitles a data subject to have certain URLs delisted from search engine.⁵⁴ It is founded on a balance between the data protection and privacy interests of the data subject and the public interest in the availability of the information. In *Google Spain*, controversially, the ECJ found that a data subject's privacy and data protection rights 'override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name.'⁵⁵ The ECJ accepted that the public interest in the information would be more significant in certain cases (e.g. if the data subject was a public figure), and this informs the balancing test that search engines must conduct.⁵⁶ This was more clearly explained to involve a balancing of privacy/data protection rights and the right of freedom of information under Article 11 of the Charter in the subsequent case of *GC and Others*.⁵⁷ Yet once again, the data subject's rights to privacy and data protection were said to 'override, as a general rule, the freedom of information of internet users'.⁵⁸

⁵¹ Article 17(3)(a), GDPR.

⁵² Article 85(1), GDPR.

⁵³ Article 85(2), GDPR.

⁵⁴ *C-131/12 Google Spain and Google* (ECLI:EU:2014:317).

⁵⁵ *Case C-131/12 Google Spain and Google* (ECLI:EU:2014:317), para 97.

⁵⁶ *Ibid.*

⁵⁷ *Case C-136/17 GC and Others* (ECLI:EU:C:2019:773), para 59.

⁵⁸ *Ibid.*, para 66.

This seeming prioritisation of the right to data protection may suggest a lack of respect for the right to freedom of expression, though this is likely premature. These cases are framed concerning the right to freedom of information, for one, and they are highly contextual interpretations of the balance in question. Nevertheless, they reinforce the need to regard the appropriate relationship between freedom of expression and data protection in adapting new data protection laws.

2.4. Enforcement model

The GDPR contains an enforcement architecture to oversee the substantive rules that protect personal data. National supervisory authorities, the judiciary and data subjects all have a role to play, and the consequences for data controllers can be significant.

Each EU Member State is required to have an independent supervisory authority, which is to be endowed with investigative and enforcement powers (including handling complaints and imposing sanctions, including fines).⁵⁹ A coordination mechanism has been created to allow the national supervisory authorities across the EU to cooperate,⁶⁰ and the European Data Protection Board was created to oversee consistency of enforcement across the EU.⁶¹ Sanctions are potentially very significant. Fines can be issued up to 20 million euros, or up to 4% of total worldwide annual turnover.⁶²

Data subjects are entitled to make a complaint to their local supervisory authority⁶³ or to seek a judicial remedy (against either a supervisory authority or a controller), including compensation.⁶⁴ Collective representation of individual data subjects by non-for-profit entities is also provided for.⁶⁵

Much of the criticism of the GDPR relates to its enforcement. There are two primary reasons; first, there is a perception of under-enforcement or lack of substantial impact on unlawful data practices. Second, there is the perception of uneven enforcement, with some supervisory authorities (particularly the Irish and Luxembourgish regulators) characterised as less likely to impose sanctions or finalise decisions.

⁵⁹ Chapter VI, GDPR.

⁶⁰ Chapter VII, GDPR.

⁶¹ Articles 68-76, GDPR.

⁶² Article 83, GDPR.

⁶³ Article 78, GDPR.

⁶⁴ Chapter VIII, GDPR.

⁶⁵ Article 80, GDPR.

3. Mitigating challenges of GDPR?

In this section, we consider where there is space to mitigate the challenges of the GDPR, with a view to suggestions that civil society organisations want to present to legislators adopting data protection laws.

3.1. Other models of data protection

While the GDPR and the Data Protection Directive before it, have been highly influential, EU data protection is not the only model of data protection globally. In particular, the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108') is a notable alternative.⁶⁶

Convention 108 has shaped some of the core aspects of EU data protection law: the understanding of personal data, the regulation of the 'controller', and key obligations such as the data protection principles, rules regarding special categories of data, data security and data subject rights. This Convention is less prescriptive than the GDPR but equally seeks to protect fundamental rights in the context of digital data processing. Many countries in Latin America, including Argentina, Mexico, and Uruguay, have ratified it.

A modernised version of the Convention, Convention 108+,⁶⁷ was opened for signature in 2018. It seeks to update the Convention and adds rules in relation to the lawfulness of data processing, additional special categories of data, more specified data subject rights and the nature of sanctions and remedies to be created. It has been ratified by Argentina and Uruguay in Latin America.

3.2. Independent oversight

A key aspect of EU data protection law is the role of the national supervisory authority. Two important points should be made regarding their role.

First, a well-resourced and independent regulatory authority can be an important check on the abuse of the law, such as data protection law being used to censor speech.

⁶⁶ *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981.*

⁶⁷ <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1>

Adequate resourcing of supervisory authorities in the EU has been a challenge in some cases, with the consequence that the authorities can be out-resourced by the controllers whom they seek to regulate.

Second, we note the importance of the independence of those authorities. The independence of the regulatory authorities is a matter of primary EU law.⁶⁸ The European Commission has an enforcement role to ensure that such independence is maintained, and a number of cases have been brought against Member States where the independence of the relevant authority was seen to be compromised.⁶⁹

3.3. Derogations to protect freedom of expression, SMEs

Finally, the GDPR allows Member States to restrict the application of its requirements in certain instances. Any country modelling their laws on an EU approach should also have regard to where derogations might be suitable to their national or regional contexts. These rules in the GDPR – the prohibitions and specific ex-ante requirements – apply least consistently across different Member States.

Article 23 of the GDPR allows for restrictions of certain obligations of the GDPR, provided that such restrictions satisfy a fundamental rights analysis (including proportionality).⁷⁰ Restrictions may be made for national security, public security, the protection of judicial independence and judicial proceedings, the protection of the rights and freedoms of others, and the enforcement of civil claims, amongst other grounds.

Additionally, we note that the GDPR acknowledges the different positions of smaller organisations. Certain organisations that have less than 250 employees do not have to engage in the full record-keeping obligations, provided they are not engaging in certain types of high-risk processing.⁷¹ Given the human rights context in which the GDPR sits, the principle of proportionality – in particular, the idea that measures should not go beyond what is necessary to achieve their stated purposes – may have a role to play. However, this has yet to be fleshed out by Courts. Some modification of the nature of obligations may be appropriate for low-risk or small-scale processing.

⁶⁸ Article 8(3), Charter.

⁶⁹ Case C-518/07 *Commission v Germany* [2010] ECR I-01885; Case C-614/10 *Commission v Austria* (ECLI:EU:2012:631); Case C-288/12 *Commission v Hungary* (ECLI:EU:C:2014:237).

⁷⁰ Article 23, GDPR.

⁷¹ Article 30, GDPR.

4. NGOs and Data Management

Having reflected on some of the general challenges associated with the GDPR, we consider how these challenges might be particularly relevant to actors in civil society, including NGOs. Civil society actors, just like other economic, public or private actors, are likely subject to data protection regulation. Still, lack of administrative, financial, and human resources capabilities may hinder their ability to achieve their civic missions.

Studies on civil society and its organisations have documented, from various approaches, the importance of a robust civil society for constructing democratic societies⁷². As shown above, some key challenges of applying GDPR-like laws are scope, responsibility models, its impact on freedom of expression and the enforcement model. However, NGOs differ in size, sustainability models, activities, and missions when considering civic society actors. In particular, as was shown in section 2, a model based on an overly broad material scope like GDPR, in combination with bureaucracies that enjoy little autonomy, may create risks of adverse effects on freedom of expression. To assess potential risks and impact on NGOs, in this section, we first consider some of the critical ways NGOs use and manage data and then determine what this would mean for NGOs' compliance with data protection legislation.

4.1. Data usage and management by NGOs

In terms of data use and management, many NGOs have moved towards digital transformation with other actors. This movement implies using web-based, GIS (Geographic Information Systems), virtual, and mobile technologies in the context of civic technologies. ('Civic technologies' refers to information and communication technologies and strategies adopted to benefit citizens. The term was pioneered in the Knight Foundation report⁷³, which identified different purposes of civic organisations, including crowdfunding, P2P sharing, open data, data utility, data visualisation and mapping, community platforms, voting tools, and democratic accountability actions.)

⁷² Carew Boulding NGOs, Political Protest, and Civil Society. In *NGOs, Political Protest, and Civil Society* (p. 1). Cambridge: Cambridge University Press (2014).

⁷³ <https://knightfoundation.org/features/civictech/>

Some key elements of NGO's data use and management practices⁷⁴ are:

- i. Diverse Applications of Technology:** Public and private organisations, businesses, and individuals worldwide use a wide range of web-based, GIS, virtual, and mobile technologies to experiment with and develop civic technologies. These technologies are used to address various societal and community-related challenges.
- ii. Collaboration and Civic Platforms:** Collaborative efforts are common, with various stakeholders coming together to work on civic tech projects. Online communities are crucial in facilitating collaboration and providing a platform for peer-to-peer networks, stakeholder mobilisation, and partnership engagement. Civic platforms can serve as incubators for innovative ideas.
- iii. Data Analytics:** Digital data analytics methods are highlighted as powerful tools for building community capacity. Online platforms collect structured and unstructured data, which can be analysed to gain insights and inform decision-making.
- iv. Challenges in Technology-Powered Engagement:** Technology-driven engagement in civic tech communities offers many opportunities but presents various design and management challenges. These challenges may include privacy and data protection, security, and the effective use of technology in non-business contexts.

These practices illustrate the significance of technology and data analytics to civic tech communities. A tension exists between adequate compliance with data protection rules and the maintenance of desirable channels for freedom of expression. For example, a study by Berdou and Shutt has shown that only half of a sample of twenty African and Asian civic tech projects acting as “crowdsourcing intermediaries” had a published privacy policy. Also, they recorded that six of them failed to explain the sequence of actions that submitted information would trigger⁷⁵. This study may also be relevant to the Latin American context, which has been lagging concerning the development of regional data protection regulatory frameworks and where it is necessary to strengthen the channels of expression of vulnerable groups.

⁷⁴ Mačiulienė, Monika and Skaržauskienė, Aelita (2020) Building the capacities of civic tech communities through digital data analytics, *Journal of Innovation & Knowledge*, Volume 5, Issue 4, 2020, Pages 244-250, ISSN 2444-569X, <https://doi.org/10.1016/j.jik.2019.11.005>.

⁷⁵ Berdou, E. and Shutt, C. (2017) *Shifting the spotlight: understanding crowdsourcing intermediaries in transparency and accountability initiatives*, Making All Voices Count Research Report, Brighton: IDS

NGOs, particularly those with limited resources, are uniquely positioned. While they are not profit-driven like businesses, they often still handle vast amounts of personal data related to vulnerable populations. The stringent requirements of data protection laws can pose challenges to these organisations, and some NGOs are unlikely to be able to comply with these laws.

Civil society organisations often deal with a diverse range of data, depending on their area of focus. This can include personal data about beneficiaries, donors, volunteers, staff, community members and research subjects. Such data can encompass names, addresses, contact details, health information, payment data, political affiliation, interests, income and social security benefits. Also, NGOs gather operational data related to their projects, including budgets, timelines, and outcomes. NGOs also collect field data from on-the-ground activities, surveys, and other research. For instance, as documented⁷⁶, an NGO focusing on health might collect data on disease prevalence, vaccination rates, and health infrastructure in a particular region. Finally, a critical component of NGO data is communication and fundraising data related to outreach, advocacy, awareness and donor campaigns, including feedback, engagement metrics, and impact assessments.⁷⁷

Data-driven insights help NGOs decide where to allocate resources, which projects to prioritise, and how to design interventions effectively. NGOs rely on data to measure the impact of their initiatives, ensuring that they are achieving their goals and making a positive difference⁷⁸. By maintaining clear data records, NGOs can demonstrate transparency to donors, stakeholders, and communities. Also, data is strategic for better resource allocation. The data gathered helps NGOs identify areas of need, ensuring that resources are directed where they are most required⁷⁹.

The challenge of complying with data protection regulations often requires NGOs to invest in technology, training, and processes. For NGOs with limited resources, these investments can strain their budgets, diverting funds from core activities. On another note, the increased internal bureaucracy implementing data protection measures can lead to increased administrative tasks. NGOs might need to set up dedicated teams or departments to handle data protection, leading to potential bureaucratic delays in decision-making and operations.

⁷⁶ Dash and Mishra (2014).

⁷⁷ See Iñarra (2023)

⁷⁸ See Rhode, Rana, & Edwards (2017)

⁷⁹ See e.g. <https://hazrevista.org/tercersector/2023/10/formacion-movilidad-globales-captacion-fondos-fundraising/>

As highlighted by Buckley, Caulfield, & Becker (2021), there is also a potential for data audits or other enforcement activity to be used as tools of retaliation. Governments might inundate NGOs with investigations⁸⁰, not out of genuine concern for their data practices, but to overwhelm and disrupt the organisation's operations.

4.2. Non-compliance implications for NGOs

As we see above, the journey to compliance might be challenging. However, it offers several benefits and silver linings. NGOs can ensure more efficient and secure operations by modernising their data operations and enhancing risk management processes⁸¹. These improvements can lead to better decision-making, more effective interventions, and a heightened ability to measure impact. Furthermore, compliance with data protection regulations can be a powerful signal of trustworthiness. In an age where data misuse and privacy concerns are rampant, an NGO's commitment to data protection can set it apart, bolstering its reputation and fostering deeper trust with donors, beneficiaries, and the broader public⁸².

The implications of non-compliance with data protection regulations for NGOs are multifaceted and can have profound consequences on their operations and reputation. NGOs failing to adhere to these regulations face potential legal penalties and fines. For instance, under the GDPR, organisations can be fined up to 4% of their annual global turnover or €20 million, whichever is greater.⁸³ Such financial penalties could be crippling for NGOs, many of which operate on tight budgets and rely heavily on donor funding. Even where the maximum sanctions are not likely in response to minor breaches of the law, the mere threat of sanction may impact operational decisions.

Beyond the potential financial implications, there is also the looming threat of a damaged reputation. NGOs, by their very nature, are built on trust. They rely on this trust to raise funds, recruit volunteers, and carry out their missions. Any perceived breach of this trust, especially in data protection, can have long-lasting repercussions. Donors, volunteers, and the general public may become wary of supporting or associating with an NGO that

⁸⁰ One case that might be seriously analysed is Mexico. See this column for one point of view: <https://elpais.com/opinion/2021-10-23/la-sociedad-civil-en-tiempos-de-amlo.html> or <https://www.lapoliticaonline.com/mexico/politica-mx/amlo-agencias-de-eu-son-complices-de-corrupcion-por-financiar-organizaciones-contra-la-4t/>

⁸¹ See the work done by organisations such as Wingu in developing technical infrastructure specially geared towards NGOs <https://winguweb.org/>

⁸² Buckley, Caulfield, Becker (2021).

⁸³ Articles 83-84, GDPR.

has shown negligence in protecting sensitive data. This erosion of trust can make it challenging for NGOs to fulfil their missions and even lead to declining donor contributions. Additionally, non-compliance can strain relationships with other organisations. Partners and collaborators might hesitate to share or access data with NGOs who are non-compliant or perceived as such, limiting joint initiatives and project opportunities.

Moreover, NGOs are susceptible to data breaches without robust data protection and cybersecurity measures. Such violations could expose sensitive information, including donor details, employee records, and beneficiary data. A data breach compounds the reputational harm and can lead to additional legal challenges and investigations.

Regulatory bodies might initiate investigations into NGOs suspected of non-compliance, leading to formal enforcement actions. Such investigations or enforcement actions can divert critical resources and attention from the NGO's core activities, further hampering their effectiveness.

In sum, while the path to data protection compliance might come with challenges, NGOs can reinforce their commitment to ethical operations, enhance operational efficiency, and deepen their trust with stakeholders by investing in data protection.

To consider how NGOs can marry these competing demands, we can look to the experiences of implementing comparator laws in neighbouring countries. While all Latin American countries recognise privacy in some form in their constitutions,⁸⁴ several countries have also enacted data protection laws⁸⁵, which have many commonalities with the GDPR. Brazil is one example; we can examine the Brazilian experience as a case study.

The following section will delve into the complexities of applying the new data protection law and how the Brazilian administration's contentious relationship with certain NGOs highlights the risks of states using the law as a weapon to pressure NGOs.

⁸⁴ See, Rodríguez, Katitza, "Análisis comparado de las leyes y prácticas de vigilancia en América Latina", *Necesarios & Proporcionados*, Electronic Frontier Foundation (EFF), 2016, disponible en: <https://necessaryandproportionate.org/es/comparative-analysis-surveillance-laws-and-practices-latin-america/#resumenejecutivo>, October 2023.

⁸⁵ See <https://adc.org.ar/wp-content/uploads/2019/06/023-A-El-sistema-de-protecci%C3%B3n-de-datos-personales-en-Am%C3%A9rica-Latina-Vol.-I-12-2016.pdf>

5. The General Data Protection Law (LGPD) of Brazil: An Analysis of its Evolution and Implications for NGOs⁸⁶

The Brazilian General Data Protection Law⁸⁷ (LGPD, Lei 13.709/2018), enacted in 2018 and operationalised in 2020 following eighteen modifications, is a legal framework designed to ensure individual privacy and control over their data, expansively defined. In common with the EU's GDPR, the LGPD encompasses a broad spectrum of personal data and mandates stringent consent requirements for data processing.

Like the GDPR, one central aspect of the LGPD is processing based on specified legal grounds (including unequivocal and free consent from data subjects) and transparency regarding data collection and specific utilisation. The law also heralded the establishment of Brazil's National Data Protection Authority (ANPD) to oversee and penalise non-compliance, with sanctions ranging from warnings to fines up to 2% of a company's revenue and potential operational suspension. Applicable across both public and private sectors, the LGPD prescribes legal bases upon which controllers can process data (including consent and the data controller's legitimate interests), in addition to imposing general data protection principles, safeguarding fundamental rights of data subjects, and imposing obligations and constraints regarding processing personal data.

While Brazil has over 40 legal provisions for privacy and personal data, the LGPD supersedes and complements the extant sectoral regulatory framework to provide legal clarity and certainty. However, the transition from the adoption of the legislation to implementation coincided with the COVID-19 pandemic, marked by a significant incident involving data use by the Brazilian government⁸⁸. Investigations revealed data acquisition endeavours by the federal government and 14 state governments to coordinate pandemic responses involving third-party agreements for data collection, manipulation, and storage. This incident highlighted governmental vulnerabilities in security and transparency. A significant concern was the absence of anonymisation tools, especially given the sensitivity of health data.

In April 2020, the Brazilian government issued Executive Order N° 954, requiring telecommunication companies to share customer data with the Brazilian Institute of Geography

⁸⁶ *The Inter-American Human Rights System (SIDH) through the American Convention on Human Rights (CADH); the American Declaration of the Rights and Duties of Man (DADD); the jurisprudence and advisory opinions issued by the Inter-American Court of Human Rights (IACHR); as well as case reports, thematic and by country, issued by the Inter-American Commission on Human Rights (IACHR) together form the basic legal framework in Latin America.*

⁸⁷ https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

⁸⁸ *Q&A: Brazil's Highest Court Just Strengthened Data Privacy Rights. (2020, July 20). See <https://www.opensocietyfoundations.org/voices/q-and-a-how-civil-society-in-brazils-is-defending-privacy-rights>.*

and Statistics (IBGE) for statistical purposes during the COVID-19 pandemic. This included names, telephone numbers, and addresses. The Brazilian Bar Association and political parties filed lawsuits arguing constitutional violations.

On April 24, the Supreme Federal Court suspended the executive order, citing privacy, dignity, and due process concerns. Data Privacy Brasil contributed as *amicus curiae*⁸⁹, emphasising personal data protection as a fundamental right. Finally, On May 7, the Supreme Federal Court confirmed the suspension with a 10-1 vote. Key arguments included the need for more precise definitions, collision with constitutional protection, absence of fundamental safeguards, and the unnecessary and disproportionate nature of the data collection, given existing resources.

The ruling highlighted the need for specificity in data use, compliance with constitutional limits, implementation of safeguards, and the exploration of less invasive alternatives for research. The Supreme Court⁹⁰ suspended the surveillance program's implementation without a timeframe, thereby setting a pivotal precedent nationally and globally⁹¹.

Beyond this initial judicial action, broader perspectives on judicial enforcement in Brazil are also worth considering. Recent research⁹², analysing over 400 appellate decisions in 2022 sought to discern the judiciary's application of Brazil's new data privacy regulation. Four salient trends emerged: (1) courts do not automatically grant compensation to data breach victims, necessitating proof of tangible or intangible harm; (2) nearly half of the analysed decisions pertained to personal data processing for debt collection or credit protection purposes; (3) courts consistently ruled in favour of fraud victims; and (4) courts exhibited rigour when personal data was used for secondary purposes, especially if processing agents lacked transparency measures. Predominantly, rulings favoured data protection, attributable in part to the amendment of Article 5 of the Brazilian Constitution⁹³, which enshrines personal data protection, including digital, as a fundamental right⁹⁴.

⁸⁹ https://www.dataprivacybr.org/wp-content/uploads/2020/05/dpbrr_roteiro_sustentacao_stf_english_final.pdf

⁹⁰ *Case REFERENDO NA MEDIDA CAUTELAR NA AÇÃO DIRETA DE INCONSTITUCIONALIDADE 6.387 DISTRITO FEDERAL:* <https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2021/02/OAB-v-Bolsonaro.pdf>

⁹¹ For more information on the political dynamics of Brazilian court decisions see Lage-Freitas, A. Allende-Cid, E. Santana, O. Oliverira-Lage, I (2022, March) *Predicting Brazilian Court Decisions*. In *PeerJ Computer Science*.

⁹² *Relatório Anual de Jurimetria 2022* <https://opiceblum.com.br/wp-content/uploads/2019/07/09-relatorio-jurimetria-2022.pdf>

⁹³ *Brazilian Congress approves personal data protection amendment to the constitution.* (2022, February 23). <https://iapp.org/news/a/brazilian-congress-passes-personal-data-protection-amendment-to-constitution/>

⁹⁴ *The incorporation of a right into the Federal Constitution through amendments is a guarantee of consensus and stability, since they require the support of 60 percent of the members of each of the Chambers of Congress, while an ordinary law requires a majority of the members present (Art. 60, Federal Constitution, Brazil).*

The ANPD introduced specific regulations for small businesses⁹⁵ in January 2022 to further refine the law. This aimed to balance LGPD provisions and smaller private sector entities' unique challenges. Regulators understood that small businesses have compliance challenges similar to the ones we have described for NGOs. Through iterative reviews and civil society contributions, the ANPD ensured these businesses' smoother alignment with the law's standards.

A noteworthy aspect of the law's application is the ANPD's "receptive approach," emphasising dialogue over immediate sanction imposition. While seemingly lenient, this approach, underpinned by the abovementioned developments, has been argued to foster a culture of privacy and best practices⁹⁶.

In conclusion, Brazil's LGPD endeavours to safeguard user privacy and personal data control, instituting rigorous consent requirements and penalties for non-compliance. Despite initial implementation challenges, the law has been bolstered by Supreme Court enforcement, setting a significant global precedent. The Brazilian Judiciary has applied the law in a manner favourable to the claims initiated by citizens, backed by a constitutional amendment that raises data protection to the rank of a fundamental right. Additionally, specific regulations for small businesses and a receptive stance by the ANPD further underscore the law's comprehensive nature.

5. 1. The effects of LGPD on NGOs

In response to the operationalisation of the LGPD, non-governmental organisations (NGOs) found themselves at a crossroads, balancing their mission-driven work with the demands of stringent data protection.⁹⁷

One of the most palpable shifts was in the realm of data collection. Traditionally embedded in grassroots community work, NGOs had to re-evaluate their methods. For instance, an NGO dedicated to child welfare in the favelas of Rio de Janeiro had always relied on community trust. Their outreach programs, which collected data about families and

⁹⁵ Brazilian data protection authority improves LGPD to ease regulations for small businesses. (2022, January 31). IAPP. <https://iapp.org/news/a/brazilian-data-protection-authority-improves-lgpd-to-ease-regulations-for-small-businesses/>

⁹⁶ Mari, A. (2021, August 4). Brazilian data protection body pledges to enforce "responsive regulation." ZDNET. <https://www.zdnet.com/article/brazilian-data-protection-body-pledges-to-enforce-responsive-regulation/>

⁹⁷ We carried out interviews with major NGOs in Brazil who participated in parliamentary discussion leading to the approval of the data protection law. The findings from those interviews have been anonymised in this report. For more information on the role of civil society vis a vis LGPD see Kira, B. Tambelli, C. (2017) Data Protection in Brazil: Critical Analysis of the Brazilian Legislation. InternetLab. <http://www.internetlab.org.br/wp-content/uploads/2017/03/Legal-Framework-Analysis-Brazil.pdf>

children for better resource allocation, had to be restructured. The introduction of digital forms, equipped with explicit consent checkboxes and detailed explanations in Portuguese, became the norm. This ensured compliance with the LGPD and reinforced trust; however, the implementation costs had negatively impacted the organisation's financial capacity.

The challenges were even more pronounced for NGOs dealing with sensitive data. An organisation working on health for underserved communities, operating mobile clinics across Brazil's vast rural landscape, faced a dual challenge. They had to ensure that patient data, often collected in remote areas with limited connectivity, was securely stored and educate their ground staff about the importance of data protection. Investing in secure cloud storage solutions was just one part of the equation; they also initiated training programs, ensuring that every team member, from doctors to volunteers, understood the implications of the LGPD.

Fundraising, the lifeline for many NGOs, also underwent evolution. For example, an environmental NGO working in the Amazon had a vast database of international donors. With the LGPD in effect, they couldn't simply send their annual fundraising emails. The process became more intricate, involving reconfirming consent, explaining data usage, and even offering donors an insight into how their data contributed to the NGO's mission.

The interview with the Director of a civic tech organisation in Brazil⁹⁸ added evidence of NGOs' fundamental obstacles when a restrictive law is enacted. For this NGO, this process took nine months. The organisation's Executive Director highlighted the difficulty it caused them to redesign their work with different audiences (they had to change how they tagged the content and the consequences of profiling). Furthermore, they noticed that restrictions included in the legislation created more friction for users to donate, making the online process of becoming a donor extraordinarily long and complex. The positive aspects of the new data protection law became a challenge to the survival of the organisation's engagement model with users, as well as the promotion and sustainability of this important civic tech organisation, which promotes digital democracy and online participation.

⁹⁵ Brazilian data protection authority improves LGPD to ease regulations for small businesses. (2022, January 31). IAPP. <https://iapp.org/news/a/brazilian-data-protection-authority-improves-lgpd-to-ease-regulations-for-small-businesses/>

⁹⁶ Mari, A. (2021, August 4). Brazilian data protection body pledges to enforce "responsive regulation." ZDNET. <https://www.zdnet.com/article/brazilian-data-protection-body-pledges-to-enforce-responsive-regulation/>

⁹⁷ We carried out interviews with major NGOs in Brazil who participated in parliamentary discussion leading to the approval of the data protection law. The findings from those interviews have been anonymised in this report. For more information on the role of civil society vis a vis LGPD see Kira, B. Tambelli, C. (2017) Data Protection in Brazil: Critical Analysis of the Brazilian Legislation. InternetLab. <http://www.internetlab.org.br/wp-content/uploads/2017/03/Legal-Framework-Analysis-Brazil.pdf>

⁹⁸ The interview was held on 15th August 2023.

One aspect mentioned in the interview was children's voices. Before the LGPD existed, the platform allowed children to express and post content. This capacity to participate on the platform now is limited, as children under the age of 16 require parental authorisation⁹⁹. The modifications to the platform in response to the LGPD altered the prospects for different voices to be heard via the platform, and thus impacted freedom of expression.

These interviews revealed challenges some NGOs experienced in implementing the LGPD, reinforcing that organisational and financial resources to respond to data protection can significantly impact their capacity to serve their civic missions.

5.2. Bolsonaro's Government and NGOs

Since its inception, Brazil's LGPD has been hailed as a landmark piece of legislation aiming to protect the data rights of Brazilian citizens. However, in the complex political landscape under President Jair Bolsonaro's administration, the LGPD's implications extended beyond its primary intent. Two primary concerns arise, first, that the LGPD will be an ineffective source of protection of data against state surveillance and data processing activities. Second, the concern arises that just as the GDPR has been criticised for improperly recognising freedom of expression, that the LGPD can be used to constrain speech and reduce civic space.

Bolsonaro's government is known for its scepticism towards NGOs, particularly those advocating for environmental and indigenous rights.¹⁰⁰ The stakes are high in the Amazon rainforest, where environmental NGOs work to combat deforestation and protect indigenous rights. These NGOs often collected data on the environment and indigenous communities, their health, and their interactions with the outside world. This data was crucial for advocacy, research, and international collaboration. Bolsonaro's administration has frequently been at odds with these environmental and human rights NGOs, particularly those operating in the Amazon region, for what he perceives as interference in Brazil's sovereignty and economic development¹⁰¹. In 2019, the Bolsonaro government faced criticism from international donors (including Germany and Norway) over concerns about deforestation in the Amazon¹⁰². These countries decided to withhold funds from the

⁹⁹ For a summary of the legal discussion on LGPD and children and adolescents see <https://iapp.org/news/a/el-tratamiento-de-los-datos-de-ninos-y-adolescentes-en-brasil-un-escenario-de-incertidumbres/>

¹⁰⁰ <https://elpais.com/internacional/2021-07-18/el-metodo-bolsonaro-un-atalaia-a-la-democracia-a-camara-lenta.html>

¹⁰¹ Escobar, H. (2019). "Bolsonaro's first moves have Brazilian scientists worried." *Science*, doi:10.1126/science.aaw9464.

¹⁰² *The Guardian*, 08/16/2019

<https://www.theguardian.com/world/2019/aug/16/norway-halts-amazon-fund-donation-dispute-brazil-deforestation-jair-bolsonaro>

Amazon Fund, which supports projects to combat deforestation. In response, Bolsonaro's administration has criticised NGOs, suggesting they might be behind the forest fires to tarnish Brazil's image¹⁰³.

Regulatory changes have also marked the administration's approach towards NGOs. In 2019, Bolsonaro issued a provisional measure that gave the government more control over the appointment of NGO representatives in federal councils, a move seen as an attempt to diminish the influence of these organisations in public policy¹⁰⁴. Global organisations such as Human Rights Watch raised concerns about abuses and the use of legislation aimed at different purposes by Bolsonaro's administration¹⁰⁵.

The LGPD has not been an effective safeguard of data protection in the wake of data processing by the Bolsonaro government and other state entities. It is important to reiterate that the LGPD created an agency under the name of ANPD (Autoridade Nacional de Proteção de Dados), and that the ANPD has not been an effective check on activities by Bolsonaro's government, particularly in relation to the electoral process¹⁰⁶. Research by Coding Rights and Tactical Tech Collective has uncovered various practices in online electoral campaigns that appear to conflict with existing data protection law¹⁰⁷. Notably, political parties have been engaging in agreements with marketing firms, categorised as corporate donations, a tactic deemed unconstitutional by the country's Federal Supreme Court in a 2015 ruling¹⁰⁸. The absence of any interventions from the data protection agency in the light of such data use is concerning. Additionally, there is evidence from the same research of use of external databases for direct marketing in these campaigns, which raises concerns about potential illegal acquisition or use of data for unintended purposes. Moreover, the recent amendments to the electoral law and new regulations for online electoral advertising, which permit content promotion, have inadvertently led to the unconsented and undisclosed collection of personal data aimed at creating diverse voter profiles¹⁰⁹.

¹⁰³ Reuters, 08/21/2019 <https://www.reuters.com/article/us-brazil-politics-idUSKCN1VB1BY>

¹⁰⁴ Londoño, E., & Casado, L. (2019). "Under Bolsonaro, Amazon Protections Slashed and Forests Fall." *The New York Times*.

¹⁰⁵ Human Rights Watch, March 2021 <https://www.hrw.org/news/2021/03/11/crisis-brazilian-amazon>

¹⁰⁶ <https://www.bnamericas.com/es/noticias/implicaciones-de-los-vetos-de-bolsonaro-a-la-ley-de-proteccion-de-datos>

¹⁰⁷ Public Consultation: Coding Rights and others (2019) "Desinformación en Internet en Contextos Electorales en América Latina y el Caribe" See Asociación por los Derechos Civiles, https://adc.org.ar/wp-content/uploads/2019/06/Consulta-publica-desinformacion-en-contextos-electorales_contribucion-regional-Al-Sur.pdf

¹⁰⁸ See <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=10329542>

¹⁰⁹ *Ibidem*.

There is a further concern that the LGPD may become one of “policy weapons” used by the administration¹¹⁰, as a tool to exert pressure on NGOs or other dissenting voices. In other Latin American countries, we are seeing populist leaders use existing legitimate laws and regulations to put pressure on civil society (sometimes this phenomenon is described as the “reduction of the civic space”). In the context of an already difficult relationship with NGOs, and concerns relating to emerging legislative projects to regulate misinformation and “fake news”, there is also the danger that the LGPD may be used as a potential tool to exert pressure. There are a number of factors which highlight this risk. First, while the law was nominally designed to safeguard data and ensure transparency, its requirements provided various avenues for rigorous enforcement, which could be selectively applied. Second, as we have described, the ANPD has not provided oversight of questionable data practices by the state, raising concerns about its independence as the responsible data protection agency. Third, the lack of clarity on how the law would be implemented gave political leverage to the new administration to manipulate critical aspects of the law. For example, as Venturini explained, the final version of the text notably omits administrative penalties initially proposed for severe or recurrent data breaches following President Bolsonaro's vetoes. These penalties included the possibility of partially or entirely suspending and outright banning the data processing activities of the entities in violation. This approach was akin to the measures outlined in the European Union's General Data Protection Regulation. Congress is yet to review these and other vetoes for further consideration¹¹¹.

In light of the contentious relationship between the Bolsonaro administration and NGOs, this is an important reminder of the limits of data protection laws, and the significance of careful consideration of how it will be integrated into the broader legal and political landscape. The impact of the LGPD is felt not only in the compliance costs created but also in the broader political environment, the tools governments can adopt to target their critics, and the inability of paper laws to constrain state non-compliance without effective and independent oversight.

¹¹⁰ Palau, M. (2021) *Detrás de la peligrosa batalla brasileña sobre las noticias falsas*. *Americas Quarterly*, October. <https://americasquarterly.org/article/detras-de-la-peligrosa-batalla-brasilena-sobre-las-noticias-falsas/>

¹¹¹ Venturini, J. (2019). *¿Bajo qué términos se protegerán los datos en Brasil?*. *Derechos Digitales*, July. <https://www.derechosdigitales.org/13499/bajo-que-terminos-se-protegeran-los-datos-en-brasil/>

6. Final comments

The intricate relationship between data protection laws and civil society, particularly non-governmental organisations (NGOs), presents a complex set of challenges and opportunities. The European Union's GDPR and Brazil's LGPD have set significant benchmarks in data protection, underscoring the importance of safeguarding personal data in the digital age. However, the stringent requirements of these regulations have profound implications for NGOs, which often operate with limited resources and compliance capacity.

The broad scope of the GDPR, its one-size-fits-all model of responsibility, the tension with freedom of expression, and the enforcement model present unique challenges for NGOs. These organisations play a critical role in democratic societies, and their ability to manage data effectively is often crucial for their operations. Digital transformation has led NGOs to embrace various technologies, making data analytics integral to their decision-making processes. However, balancing compliance and maintaining channels for freedom of expression remains delicate.

NGOs, particularly those with limited resources, are in a precarious position. While not profit-driven, they handle vast amounts of personal data, often related to vulnerable populations. Given the vulnerability of these stakeholders, data protection is essential, and it is crucial to think about strategies that aim to implement the new regulatory framework while supporting NGOs. Non-compliance implications are severe, with potential legal penalties and fines that can weaken these vital organisations. Also, the political use of legislation could lead to non-democratic practices.

In light of these challenges, policymakers must consider the unique position of NGOs when drafting and implementing data protection laws. A more nuanced approach, incorporating exemptions or tailored NGO obligations, could alleviate some of these organisations' burdens. Additionally, providing technology, training, and resource support could enable NGOs to comply with data protection regulations without compromising their core activities.

As we navigate this complicated terrain, it is essential to learn from the European experience and the regulatory pitfalls in Brazil and propose a series of policy recommendations that balance the imperatives of data protection with the vital role NGOs play in democratic societies.

Tailored Compliance Standards for NGOs: Policymakers should consider the unique status of NGOs and their distinct data management needs. Implementing tailored compliance

standards for NGOs, commensurate with their resource limitations and operational contexts, can reduce the compliance burden while still upholding data protection standards. These standards could include simplified reporting requirements and consent mechanisms that do not hinder participation or exemptions for specific types of data processing central to NGO activities. Small to medium enterprises in the private sector have been granted such tailored approaches in other jurisdictions, and similar approaches to small to medium NGOs could be modelled on such approaches.

Capacity Building and Resources: Recognizing NGOs often lack the financial and technical resources to meet stringent data protection requirements, governments and international organisations should support capacity building, including from funders and global philanthropic entities. This support could encompass funding for data protection technology, training for NGO staff, and guidance on best practices for data management. By empowering NGOs with the necessary tools and knowledge, they can achieve compliance without jeopardising their core missions. National data protection authorities can play an important role in educating data controllers and generating guidance and resources for NGOs.

Simplification of reporting requirements: To safeguard NGOs from potential misuse of data protection laws, authorities responsible for oversight should simplify additional requests for compliance reports from NGOs, and we suggest the enforcement authorities should be required to report on their engagement with civic sector organisations in annual reports. Such oversight can help ensure that data protection laws are applied fairly and do not obstruct the important work of NGOs.

Multi-Stakeholder Dialogue: Establishing specific spaces to engage in a joint enterprise can foster dialogue and allow multiple stakeholders to cooperatively engage in a common enterprise. NGOs, government authorities, and data protection regulators can facilitate a mutual understanding of data protection challenges and solutions. These spaces can serve as forums for discussing potential amendments or implementations to existing data protection laws that better understand the specific needs of NGOs.

In light of these policy recommendations, policymakers must consider the unique position of NGOs when drafting and implementing data protection laws. A more nuanced approach, incorporating exemptions or tailored NGO obligations, could alleviate some of these organisations' burdens. Additionally, providing technology, training, and resource support could enable NGOs to comply with data protection regulations without compromising their core activities.

Given the risks associated with data misuse, protecting personal data remains paramount. However, it is equally important to ensure that the laws designed to safeguard this data do not inadvertently hinder the operations of organisations that are essential for the

fabric of our democratic societies. A balanced approach recognising the unique challenges NGOs face is crucial for developing data protection laws that protect individual privacy rights while enabling civil society to thrive.

Recognising the importance of data protection and NGOs' work, policymakers should strive to strike this balance, ensuring that the digital era is characterised by both strong data protection and the flourishing of civil society.

References

Berdou, E. and Shutt, C. (2017) **Shifting the spotlight: understanding crowdsourcing intermediaries in transparency and accountability initiatives, Making All Voices Count** Research Report, Brighton: IDS

Boulding, C. (2014). **NGOs, Political Protest, and Civil Society.** In *NGOs, Political Protest, and Civil Society* (p. 1). Cambridge: Cambridge University Press.

Buckley, G., Caulfield, T., & Becker, I. (2021). **"It may be a pain in the backside, but..." Insights into the impact of GDPR on business after three years.** ArXiv, abs/2110.11905.

Camacho Gutiérrez, Olga y Velásquez Veloza, Lina (2022) **Iniciativas legislativas sobre privacidad y protección de datos en Argentina, Brasil, Chile, Colombia, Ecuador, México, Guatemala, Paraguay y Perú, período 2019-2021,** CELE.

https://www.palermo.edu/Archivos_content/2022/cele/papers/iniciativas-legislativas-sobre-privacidad.pdf

Coding Rights and others (2019) **"Desinformación en Internet en Contextos Electorales en America Latina y el Caribe.**

https://adc.org.ar/wp-content/uploads/2019/06/Consulta-publica-desinformacion-en-contextos-electorales_contribucion-regional-AISur.pdf

Dash, Kailash Chandra and Mishra, Umakant, **Critical Considerations for Developing MIS for NGOs** (March 26, 2014). Available at SSRN: <https://ssrn.com/abstract=2416294> or <http://dx.doi.org/10.2139/ssrn.2416294>

Escobar, H. (2019). **"Bolsonaro's first moves have Brazilian scientists worried."** *Science*, doi:10.1126/science.aaw9464.

Fabretti Moraes, H., & Vainzof, R. (2023, 15 de febrero). **The study analyses how Brazilian courts apply the LGPD.**

<https://iapp.org/news/a/study-analyzes-how-brazilian-courts-apply-the-lgpd/>

Iñara, M. (2023)

<https://hazrevista.org/tercersector/2023/10/formacion-movilidad-globales-captacion-fondos-fundraising/>

Kira, B. Tambelli, C. (2017) **Data Protection in Brazil: Critical Analysis of the Brazilian Legislation.** InternetLab.

<http://www.internetlab.org.br/wp-content/uploads/2017/03/Legal-Framework-Analysis-Brazil.pdf>

Lage-Freitas, A. Allende-Cid, E. Santana, O. Oliverira-Lage, I (2022) **Predicting Brazilian Court Decisions.** In *PeerJ Computer Science*.

Londoño, E., & Casado, L. (2019). **"Under Bolsonaro, Amazon Protections Slashed and Forests Fall."** *The New York Times*.

Mačiulienė, Monika and Skaržauskienė, Aelita (2020) **Building the capacities of civic tech communities through digital data analytics**, *Journal of Innovation & Knowledge*, Volume 5, Issue 4, 2020, Pages 244-250, ISSN 2444-569X, <https://doi.org/10.1016/j.jik.2019.11.005>.

Mari, A. (2021, August 4). **Brazilian data protection body pledges to enforce “responsive regulation.”**<https://www.zdnet.com/article/brazilian-data-protection-body-pledges-to-enforce-responsive-regulation/>

Palau, M. (2021) **Detrás de la peligrosa batalla brasileña sobre las noticias falsas**. *Americas Quaterly*, October.

Q&A: **A: Brazil’s Highest Court Just Strengthened Data Privacy Rights.** (2020, July 20). www.opensocietyfoundations.org.
<https://www.opensocietyfoundations.org/voices/q-and-a-how-civil-society-in-brazils-is-defending-privacy-rights>.

Rhode, Matilda & Rana, Omer & Edwards, Tim. (2017). **Data Capture & Analysis to Assess Impact of Carbon Credit Schemes.**

Rodríguez, Katitza (2016) **“Análisis comparado de las leyes y prácticas de vigilancia en América Latina”**, Necesarios & Proporcionados, Electronic Frontier Foundation (EFF), 2016, disponible en:<https://necessaryandproportionate.org/es/comparative-analysis-surveillance-laws-and-practices-latin-america/#resumenejecutivo> , último acceso: 27 de octubre de 2023.

Schmitt, Julia and Miller, Klaus and Skiera, Bernd, **The Impact of Privacy Laws on Online User Behavior** (October 1, 2021). HEC Paris Research Paper No MKG-2021-1437 , Available at SSRN: <https://ssrn.com/abstract=3774110> or <http://dx.doi.org/10.2139/ssrn.3774110>

Venturini, J. (2019). **¿Bajo que términos se protegerán los datos en Brasil?. Derechos Digitales** <https://www.derechosdigitales.org/13499/bajo-que-terminos-se-protegeran-los-datos-en-brasil/>