BLAVATNIK SCHOOL OF GOVERNMENT

UNIVERSITY OF OXFORD

LEMANN FOUNDATION PROGRAMME

THE PATH FORWARD FOR THE BRAZILIAN NATIONAL DATA PROTECTION AUTHORITY (ANPD)

STRENGTHENING CAPACITY AND AUTONOMY

POLICY QUESTIONS

- What are the autonomy and capacity gaps in the new Brazilian Data Protection Authority (*Autoridade Nacional de Proteção de Dados – ANPD*), the main body responsible for regulating online and offline personal data in the country, after it became an autonomous agency in June 2022?
- How might these gaps be closed in order to regulate the collection and processing of personal data in Brazil more effectively?

THE ISSUE

Brazil has recently been moving towards increasing the capacity and autonomy and further strengthening its National Data Protection Authority (ANPD). At the time of writing (October 2022), it is highly likely that the Provisional Measure that turned the ANPD into an autonomous agency in June 2022 — as opposed to a body attached to the presidency — will be approved by Congress and so establish this change's permanency. Thereafter, details of the "new" ANPD's design are due to be fleshed out during a transition period lasting until 31 December 2024. During the transition, the General-Secretariat of the Presidency will continue to provide administrative support to ANDP's activities[i], while its regulatory structure will be developed. Assuming congressional approval of the measure that more concretely establishes the ANPD's status as a federal agency — which has broad political support of the political left and right, and actors both inside and outside of government[ii] — a regulatory decree will provide further details about the ANPD's governance, its procedure for nomination of political appointees, and recruitment of the public servants who will work for the agency.

But there would still be three undefined aspects to the ANPD's institutional design: (1) how it would interact with the wider ecosystem of regulators with oversight over digital technologies in Brazil; ii) measures to avoid the risk of regulatory capture; and iii) measures to address budgetary restrictions and increase the revenue of the authority. Based on primary research,[iii] this policy brief discusses these key challenges and suggests ways to address them.

Key recommendations[1]:

- **Strengthening inter-agency coordination**: While the ANPD has led efforts to establish formal connections with several government institutions in its first two years of operation (for example, through the signing of technical cooperation agreements), there is room to increase the agency's political autonomy and build a more resilient culture of inter-agency cooperation beyond personal ties of staff members.

[1] This policy brief was developed by Beatriz Kira, postdoctoral research associate, under the supervision of Anna Petherick , as part of the work of the Lemann Foundation Programme for the Public Sector at the Blavatnik School of Government, University of Oxford. It was developed from primary research in Brasilia. This research involved many interviews, all with individuals who are closely involved in the ANDP, bodies with which it interacts, or are expert observers of its activities. Policy recommendations reflect discussions with interviewees, whom we thank for their involvement, as well as with members of the Lemann Foundation Programme team, João Pedro Caleiro, Lia Pessoa and Lucilla Dias.

— By drawing lessons from the recent experience of inter-agency coordination around the changes in the Terms of Service (ToS) of WhatsApp, **members of staff within each agency could be empowered to as 'cooperation hubs'** responsible for leading on the engagement with other agencies.

— **The Brazilian Internet Steering Committee (CGI.br) could be staffed and resourced to act as a digital coordinator across federal agencies**, managing a regulatory network similar to the UK Digital Regulation Cooperation Forum (DRCF).

- **Building resilience against regulatory capture**: To ensure that the pursuit of the public interest remains at the core of ANPD's mission, the agency should continue to communicate its key decision-making procedures and regulatory proposals transparently and effectively. As well as making drafts of regulations available to expert scrutiny, for example, the agency should submit these to public consultation and hold public hearings.

  — To avoid soft or partial regulatory treatment of powerful companies that is incentivised by agency personnel seeking career advancement in those companies at some future date – 'revolving door' problems – **post-public employment arrangements should be reviewed and modernised**. Specifically, the six-month cooling off period that applies to officials of the federal government should be more precisely tailored to match the conflict of interest threats that are particular to the nature of the work conducted by the ANPD. This would require formal legal amendments or new legislation.

- **Increasing revenue through a supervisory fee**: In light of its severe budgetary constraints, and despite the high level of commitment of officials working at the ANPD, there are significant human and financial capacity constraints preventing effective regulation of data in Brazil. One way of increasing the agency's capacity would be to expand its revenue sources (listed in article 55-L of the Data Protection Law). Since the ability of the ANPD to charge fees was vetoed by President Bolsonaro and not included in the Provisional Measure text, this would have to be the object of amendments or new legislation.

  — New procedural fees should be introduced to firms that process large amounts of data to cover the costs of their regulatory supervision. One example is the yearly supervisory fee of up to 0.05% of annual worldwide net income that the European Commission will charge to providers of very large online platforms and search engines, intended to cover the costs involved in monitoring their compliance with the Digital Services Act (DSA). Another example is the data protection fee charged by tie Information Commissioner's Office (ICO) in the UK and that varies according to a company's size and turnover. In Brazil, following a similar model, companies that process personal data could be required to register and be licensed by the agency to conduct business in the country.

BROADER CONTEXT AND CONTRIBUTION:

- The discussions around the ANPD are set against the broad backdrop of ongoing and growing policy concerns that have emerged with the digitalisation of the economy. In response, governments around the world have sought to adopt new regulatory frameworks, and to create new institutions or reform existing agencies, to regulate and supervise digital platforms more effectively, including the collection and processing of personal data.

- To inform the design of the ANPD, this policy brief discusses in detail two key dimensions of good public institutions: capacity and autonomy. In doing so, the brief discusses relevant criteria to assess these two dimensions and how they would be relevant features to incorporate in the agency. It also touches on the relationship between capacity, autonomy, and integrity, suggesting how the ANPD could become an 'island of excellence' or 'pocket of integrity' in the Brazilian regulatory landscape.

- Effective digital regulation in Brazil is not limited to the activities of the data protection authority and the adequate enforcement of the Data Protection Law. Because digital technologies and the digitalisation of the economy have implications across multiple policy domains beyond personal data – such as competition, consumer protection, and law enforcement – this brief also addresses how digital regulation permeates the activities of several government institutions in Brazil and emphasizes effective inter-agency coordination. Therefore, it shows that alternative design options may ensure coordination by making interactions between agencies and regulators less dependent on personal relationships, and increase resilience in these institutions.

STRUCTURE:

1. INTRODUCTION

What are the key features of good public institutions and how can those involved in the design or reform of institutions ensure that these features are embedded in government agencies? Designing effective institutions is a difficult task for all governments, across all sectors, but is particularly challenging when it comes to institutions tasked with the supervision of digital technologies. Digital technologies bring new complexities to policy and regulation in part because evolve fast, challenging governmental institutions to keep up with constant innovation. Considering the pace of digitalisation of the economy and in society, how can one ensure that public agencies, including regulators, are up for the complex task of regulating digital technologies effectively? In short, how to mitigate risks while unlocking the full benefits and potential of these technologies?

Digital technologies should be understood and regulated not only with regards to the content that is created and shared online, but also as a growing industry with promising and innovative business models. Digital regulation, as such, is used here broadly to describe different sets of laws, policies, and institutions that aim to manage the impact that digital technologies and activities can have on individuals, companies, the economy and society.[iv] Getting digital regulation right is important to ensure that the gains of digital technologies are inclusive, and to prevent harms.

Considering the growing pervasiveness of the digital economy, designing public institutions able to regulate and supervise online data effectively will be key to mitigate the risks associated with digitalisation while harnessing its benefits. In the Brazilian context, this task is as important as it is complex. Digitalisation has huge potential to promote economic growth, create jobs, and modernise the economy.[v] At the same time, it raises new and complex public policy issues, which require the update of regulatory models and enforcement practices.

Data regulation is a key aspect of digital regulation, and a pressing policy development area for Brazil. Brazil is considered a hotspot for data leaks globally and there are considerable risks both for business and for the public sector associated with poor data practices.[vi] Data regulation encompasses both online and offline collection and usage of data, including, for example, data made available voluntarily by consumers in brick-and-mortar shops or telemarketing services. However, online data protection has grown in its importance, in line with the development of hardware and software that allows the collection and processing of personal data of increasingly diverse types, and at ever greater speed and volume.

The themes of digital regulation and personal data regulation are best visualised as a Venn Diagram, in which the latter shifts over time to become increasingly overlapping with the former. This brief discusses both issues – digital regulation and personal data regulation – in parallel, with a stronger focus on person data regulation as that is the ANPD's core responsibility.

2. THE LEGAL AND INSTITUTIONAL CHALLENGES OF REGULATING DIGITAL PLATFORMS AND DATA

The term 'digital regulation' is often used to describe the regulatory responses to challenges that arise from the operation of 'digital platforms', that is, the business models and arrangements emerging from the digitalisation of the economy. These platforms offer a plethora of goods and services, including social media platforms, such as Facebook and Twitter, streaming platforms such as Netflix and YouTube, search engines such as Google and Bing, messaging apps such as WhatsApp, and e-commerce services such as Amazon and eBay.

As the impact of digitalisation of the economy is widespread and the nature of regulatory challenges have evolved over time, and, as a result, there is no settled definition of digital platforms. Nonetheless, they share two common characteristics that have given rise to novel challenges: one, they serve multiple groups of users (and are also called multi-sided platforms); and two, these platforms collect and process large amounts of data.

Evans and Schmalensee defined multi-sided platform as one that "has (a) two or more groups of customers; (b) who need each other in some way; (c) but who cannot capture the value from their mutual attraction on their own; and (d) rely on the catalyst to facilitate value – creating interactions between them".[vii] Key to this definition is the intermediary role played by platforms: they offer connections and access to users, and create value that could otherwise not be obtained without their intermediation and coordination.[viii]

Platforms also receive the label 'digital' when they use digital technologies[ix] as a medium for connection and rely on the collection and processing of data to operate. That is, digital platforms collect and process vast amounts of data, and these activities are crucial for the provision of goods and services through these platforms.[x] These types of data include, but are not restricted to i) information that is voluntarily shared with a platform when registering for a service (e.g. name and email address), ii) observed information collected automatically via the use of a service or device (e.g. metadata), iii) data from tracking and observing users' activities and preferences (e.g. browsing history, likes, follows).[xi] These different types of data are at the core of new and rapidly growing business models, and the movement of data or information across groups of users underpins the activities of these firms.

Whereas digital platforms offer a range of benefits for individuals and economies alike, they also present enhanced risks of harm to users, particularly as to how personal data is used by these platforms. Around the world, governments have been grappling with the challenge of regulating new digital technologies effectively, not only to mitigate some of the associated harms but also to unlock their potential for innovation and economic growth. To respond to this challenge, some

governments have adopted new data protection laws or updated existing legislation that had been passed in an analogue past. At the same time, others have created new data protection authorities, new regulatory agencies to regulate data, and have sought to equip existing institutions with the capacity required to supervise the collection and processing of data by digital platforms more effectively.

Getting the design of data protection authorities correctly is not a trivial task. Due to the complexity and opacity of the business models of digital platforms and in light of the interconnected nature of the regulatory challenges associated to them, institutional design is key in determining to what extent the data regulator will be able to fulfil its public purpose.

Some experts have suggested that rather than adopting a piecemeal approach, new specialised agencies should be created to focus specifically on digital platforms. They would have powers akin to sector regulators, responsible not only for establishing *ex ante* prescriptive behavioural rules, but also for investigating and eventually fining companies that violate these rules.[xii] While the creation of a new institution (i.e. a 'Digital Regulator' or a 'Digital Watchdog') could avoid long administrative or judicial procedures and expedite the identification of harms and adoption of remedies, it would not necessarily solve all institutional challenges associated with regulating digital platforms.

Overall, crucial questions remain regarding the institutional design of data and digital regulators – for example, how they should be funded, how to avoid industry capture, ensure intra-agency coordination and facilitate convergence between agencies with overlapping mandates while minimising conflicting decisions.[xiii] While some of the specific challenges that emerge with digital platforms and data regulation are new, many of these questions have been addressed by legal and political science scholars in other contexts. Their insights into the role of state regulation and on the design of good institutions provide valuable lessons to the future of the data protection authority. More specifically, one helpful approach is to draw on the concepts of capacity and autonomy for effective governance.[xiv]

3. MEASURES OF GOVERNANCE AND THEIR RELATIONSHIP WITH DIGITAL GOVERNANCE

Political science commentaries and empirical studies have argued that two important dimensions of good governance are capacity (conceived of as resources and professionalisation), and autonomy (the independence of bureaucrats from political principals and industry interests). One example is Fukuyama's dual framework, centred around capacity and autonomy.[xv] Another, focusing on the Brazilian context, is the scholarship of Bersch et al, which investigates the relationship between two dimensions of governance in the countries' federal agencies: capacity (more effective bureaucracies, including aspects such as resources and professionalisation), and autonomy (measure of the overall politicisation of the bureaucracy).[xvi] Similarly, Pires and Gomide examined the governing arrangements supporting the implementation of federal public policies in Brazil, evaluating their technical-administrative and political-relational state capacities.[xvii] This policy brief offers a step forward by proposing measures of capacity and autonomy of Brazilian federal public institutions from a legal perspective, and by discussing the relevance of these dimensions to regulate digital platforms.

The dimension of **capacity** reflects the existence of professionalised bureaucracies and effective inter- and intra-government management mechanisms. The political science literature underscores that the existence of expert career paths and coherence of purpose (or hierarchy of purposes) within agencies enhance their performance. For example, Evans and Rauch proposed a measure of Weberian bureaucracy that incorporates these elements and showed that effective bureaucracies are positively associated with meritocratic recruitment and the offer of predictable, rewarding, long-term careers in the civil service.[xviii] Drawing on this evidence, Bersch et al suggest a measure of capacity within Brazilian federal agencies that considers the proportion of civil servants in expert careers, career longevity, staff requisitioned from other agencies, and average salaries.[xix]

Here, we suggest that capacity can also be examined in terms of two aspects: the decision-making process of appropriately interpretating and applying in context legal provisions, and the extent to which the institution is able to fully implement the law. In the case of data protection authorities, elements of note in the decision-making process would include considerations on whether decisions relating to opening investigations and adopting remedies are made by individuals or by a composite body, or how the agency develops and implements its regulatory agenda. To regulate data and digital technologies effectively, government agencies and regulators need to be able to recruit and retain qualified professionals who have been trained to understand how digitalisation strains traditional legal frameworks, and how to regulate innovative industries.

The dimension of **autonomy** can be examined both from the perspective of political autonomy and from the perspective of regulatory autonomy. From the political perspective, the notion of autonomy is often associated with control and supervision over institutional resources – including budget and personnel – while maintaining a level of separation in relation to other organisations, including the level of interference that elected politicians have over the bureaucracy.[xx] In this sense, the measurement of autonomy proposed here also incorporates data related to the available budget of the institution, the legal framing of the institution, and the powers legally attributed to it.[xxi]

Another aspect that the literature has highlighted as being relevant for autonomy is the relationship between the institution and other agencies, including the existence of channels and procedures to coordinate with other institutions.[xxii] In a wide sense, coordination can be understood both as a process and as and outcome. As a process, the term can generally be used to describe the means through which decisions are brought together by different government organisations. But coordination can also be considered as the outcome of that process, and used to describe and measure the level of policy coherence that can be achieved through the interaction of government programmes and organisations.[xxiii]

In this policy brief, we draw on Bouckaert et al to discuss coordination as a process, focusing on the instruments and mechanisms, both formal and informal, that enhance the alignment by Brazilian federal regulators. As such, the analysis is centred around horizontal coordination between organisations within the national level. Given the complexity of digital platforms, effective coordination will be key to ensuring timely and adequate responses to fast-moving technology markets, whose business models are constantly changing and evolving.[xxiv]

From the regulatory perspective, autonomy can be associated with resilience against business or regulatory capture. That is, the regulators' ability to counter the disproportional influence of economically powerful actors in the design and implementation of regulation.[xxv] Simply put, the theory of regulatory capture proposes that regulated industry actors – especially monopolies or those in sectors dominated by few, large economic agents – have power as well as incentives to influence the regulator, in order to capture 'regulatory rents.' The regulator typically ends up more closely aligned with the preferences of a few, concentrated interests (typically large corporations), than to the preferences of a much greater number of diffuse interests, such as those of the public or 'citizens at large.' In this way, the regulator is 'captured' by industry.

While the idea of regulatory capture has been questioned from several fronts as the literature on regulation and public policy evolved,[xxvi] it has contributed to the understanding of how regulation is shaped by emphasising the relationship between multiple interest groups and between these interests and the state. Importantly, this notion of capture also paved the way to fundamental debates about the role played by institutional design in regulatory processes, and mechanisms to reduce the possibility of capture. For example, theory suggests that developing

cross-sector agencies that oversee different industries – as data protection authorities do – could make the regulator less vulnerable to the grip of any one single industry.[xxvii]

Capacity and autonomy are also related to an institution's **integrity**. Even in contexts of institutionalised corruption or predominance of dysfunctional institutions, one can find "pockets of efficiency" (*bolsões de eficiência*) or "islands of excellence" (*ilhas de excelência*).[xxviii] Increasing capacity and autonomy can help, to some extent, to insulate institutions the inefficiencies and problems (such as corruption) of the wider public administration. But capacity and autonomy can also improve institutional integrity in other ways than merely making it harder for corrupt practices, common outside the organisation, to enter to take root.

Institutions are integrous when they legitimately pursue a public purpose, doing their best with the resources available to them.[xxix] By strengthening their autonomy and reducing the ability of political and industry actors to lead them astray, institutions can focus on their purposes, thereby raising their integrity. Moreover, increased capacity can make the institutions better able to deliver and fulfil their public commitments, by making them more capable of managing their resources and to achieve their purposes efficiently, and more resilient to deal with instabilities and pressures.[xxx] Therefore, improving capacity and autonomy can also help to create islands of excellence in the public administration.

4. THE BRAZILIAN CONTEXT

Brazilians are avid users of digital technologies, with recent data showing that the country had 242 million smartphone devices in June 2022, an average of 1.1 device per inhabitant or 113% per capita, above the world average of 91%. There are also 205 million active users of computers in Brazil, representing 96% of the population, and placing the country above the world average of 84% of computer users.[xxxi] Internet penetration continues to rise. In 2020, 81% of Brazilians 10 years old or over were internet users, an estimated 152 million people, an increase in comparison to 70% of internet users in 2018.[xxxii]

Meanwhile, the rules and institutions required to ensure Brazilians can safely benefit from the digital economy have not evolved at the same pace. In early 2021, for example, Brazil suffered one of the largest data breaches in world history, encompassing 223 million personal records and exposing valuable information, from taxpayer registration numbers to credit rating assessments – including data from deceased Brazilians.

Brazil has adopted major regulatory frameworks, including the Civil Rights Framework for the Internet (*Marco Civil da Internet*), a new data protection law, and has strong institutions, such as the competition authority (*Conselho Administrativo de Defesa Econômica* – CADE) and the Central Bank (*Banco Central do Brasil* – BCB). Importantly, the right to data protection has been recognised by the Brazilian Federal Supreme Court (*Supremo Tribunal Federal* – STF) and included in the Brazilian Constitution as a fundamental right.

At the same time, legal and institutional challenges remain as well as questions related to the capacity of governmental institutions to understand digital platforms and regulate them effectively. Furthermore, the regulatory framework remains specialised and fairly fragmented, and there are not yet clear rules and processes establishing when and how different institutions, with different mandates, should work together.[xxxiii]

Based on the literature and the experience of other sectors, it is crucial to avoid conflicting decisions and duplication of work.[xxxiv] Recent events in Brazil have highlighted the need to seriously consider 'who does what' – that is, which federal agencies and institutions have jurisdiction over digital platforms, what are their responsibilities, and how they should interact with one another.

4.1. HOW HAVE DATA AND DIGITAL PLATFORMS BEEN GOVERNED IN BRAZIL?

In Brazil, as of today there is no overarching regulator responsible for supervising digital platforms. Instead, there are different agencies and regulators that share responsibility for enforcing the rules that govern digital platforms, focusing on specific policy and legal areas. This is the institutional arrangement in most countries, developed and developing alike, with digital being a cross-cutting issue under the jurisdiction of multiple government agencies and regulators. In Brazil, the following agencies have some level of oversight of digital platforms:

- **Data protection**. The Brazilian National Data Protection Authority (*Autoridade Nacional de Proteção de Dados* – ANPD) was created in 2019 (Law 13853/2019) and officially started to work in 2020. The ANPD is the body responsible for implementing and enforcing the Brazilian Data Protection Law (Law 13709/2018 – LGPD). Because of budgetary restrictions and political disputes involving the adoption of the law, the ANPD was not created as an independent agency but as a body of the federal government attached to the Presidency. [xxxv] In June 2022, through Provisional Measure (MP) 1124/2022, President Bolsonaro changed the legal status of the Data Protection Authority, turning it into an agency (*autarquia de natureza especial),* independent from the Presidency. While this agency has the jurisdiction to regulate the collection and processing of data by public and private institutions in Brazil (both through digital and analogue means), it is not an overarching digital regulator as it deals only with personal data.

- **Competition.** The Brazilian Competition Law (Law 12529/2011) prescribes specific anticompetitive coordinated and unilateral conducts by firms and establishes rules for the review and approval of concentrations with significant effects on competition. Public enforcement of competition law in Brazil is undertaken by the Administrative Council for Economic Defence (*Conselho Administrativo de Defesa Econômica* – CADE), the Brazilian competition authority, with horizontal powers to supervise competition in all markets.

- **Consumer protection.** The Brazilian Secretariat of Consumer Protection (*Secretaria Nacional do Consumidor* – Senacon) was established in 2012 (Decree 7738/2012) and is part of the Ministry of Justice. Its legal roots can be found in article 106 of the Consumer Protection Code, as the government body responsible for developing, coordinating, and executing the National Policy of Consumer Relations, with the goal of protecting consumers' rights (both online and offline), ensuring the harmonisation of consumer relations, and working with other agencies and government bodies across the country and internationally on issues of consumer protection.

- **Internet governance.** The Brazilian Internet Steering Committee (*Comitê Gestor da Internet no Brazil* – CGI.br) was created in 1998 (Portaria Interministerial 147/1995) and amended in 2003 (Presidential Decree 4829/2003). It is a multistakeholder body that gathers representatives from the government, academia, private sector, and the civil society. It has been empowered through the enaction of the Brazilian Civil Rights Framework for the Internet (*Marco Civil da Internet*, Law 12965/2014) and is responsible for the establishment of strategic guidelines related to the use and development of the internet in Brazil, as well as for recommending procedures, norms, and technical operational standards for the internet in Brazil.

- **Law enforcement.** The Federal Prosecution Service (*Ministério Público Federal* – MPF) is an independent federal law enforcement agency, responsible for conducting investigations and the prosecution of criminal offences at the federal level, as well as of civil and administrative wrongdoing related to the federal government and corresponding public interest. MPF is not a regulator, but its mandate includes investigating and prosecuting offences related to data and digital technologies.

Despite this fairly fragmented institutional landscape, there are promising signs that these agencies have started to work together to address issues emerging from digital platforms. For example, in May 2021 CADE, ANPD, Senacon, and MPF issued a joint declaration directed at WhatsApp and Facebook and its application's new privacy policy.[xxxvi] Further, the ANDP, even before it was structured as an autonomous agency, had already signed technical cooperation agreements with other institutions, including CADE, SENACON and CGI.br, vowing to share documents, information, and experiences, and to promote meetings, training courses, and events joining civil servants from both agencies.

However, there is little detail established as to how the relationship between these agencies will play out in practice. The joint declaration about Facebook and WhatsApp could be a first step towards more cooperation, however, differences in the investigatory powers and the pace of investigations may have presented challenges, in those instances, preventing more coherence in outcomes. It is noteworthy that the report summarising the findings of the joint investigation (led by the data protection authority) highlighted not only areas of agreement between the agencies, but also discrepancies and areas where further investigation might be required, to be conducted by each agency individually.[xxxvii] For example, the Federal Prosecutor's Office expressed a series of caveats, and specific areas where the commitments agreed with Facebook and WhatsApp may not be enough to address MPF's concerns.[xxxviii]

5. WHAT IS AT STAKE IN THE DESIGN OF THE FUTURE OF THE ANPD?

As previously mentioned, the change initially establishing ANDP as an independent agency was enacted by President Bolsonaro. At time of writing (October 2022), Congress still needs to vote on the issue. Assuming that it goes through without amendments, as observers expect, there would still be remaining challenges in shaping the ANPD, which are discussed below:

5.1. THE RELATIONSHIP BETWEEN THE ANPD AND OTHER AGENCIES

The absence of specific procedures or formal institutions for cooperation between agencies mean that future cases involving digital platforms and multiple policy areas could be handled differently. While the UK has taken a step towards stablishing an umbrella structure to facilitate cooperation (the Digital Regulation Cooperation Forum), in Brazil there is emerging evidence that the interaction between the agencies is currently very much dependent on personal relationships between senior members of their staffs, and their individual ability to recognise the importance of working with others. That is, the relationship between the ANPD and other agencies is currently shaped by informal institutions.[xxxix]

From a public policy perspective, coordination should be taken seriously because both the "underlying and resulting problems [of lack of coordination] are related to a loss of governments' policy capacity".[xl] That is, the low level of coordination not only reveals a problem in the decision-making process of the agencies, but also leads to worse policy decisions. In contrast, greater levels of coordination can lead to better policy outcomes – including more coherence, less redundancy and contradictions within and between policies, and less conflict between government agencies.

One way of distinguishing types of coordination is to them negative or positive. Negative coordination is the basic level of coordination, one in which there is an agreement (tacit or explicit) between organisations that they would not interfere in each other's policy agendas, reducing the likelihood of conflict between them. Positive cooperation, on the other hand, requires organisations and actors to take positive steps to consider and engage with the agenda of other actors and organisations, and can require some level of compromise between them in order to achieve a greater goal.[xli] The relevance of both types of coordination increases with policy fragmentation, and should be at the core of efforts to enhance the capacity and autonomy of the Brazilian ecosystem of regulators, especially if the number of bodies with oversight over digital issues increases.

Considering the relevance of effective mechanisms of coordination within the federal government for high-quality government generally – and the considerable overlap between policy areas that are typical of digital platforms specifically – this is a gap that Bolsonaro's Provisional Measure is not able to close. Closing the gap and making the interaction between agencies and regulators less dependent on personal relationships will require participation from multiple stakeholders and careful consideration of the alternative design options for more effective coordination.

5.2. AVOIDING THE RISK OF REGULATORY CAPTURE

The ANPD oversees and regulates the activities of all individuals and institutions that processes personal data, both in the public and the private sector. The ANPD is, as such, a horizontal regulator, responsible for supervising a policy area across multiple industries, as opposed to a sector regulator, that oversees multiple aspects of a given industry (eg telecommunications, or energy). Given the pervasiveness of data processing activities in today's economy, there is a large universe of firms whose activities fall under supervision of the ANPD, ranging from small enterprises to large multinational corporations. In this scenario, a key concern in terms of capacity and autonomy is the movement of personnel between public and private sector jobs, and the threats that this mobility can pose to public integrity.

The ANPD's broad reach means that there is a significant demand for qualified professionals in the private sector who are able to navigate the intricacies of the data protection law in Brazil. However, the offer of trained professionals has not yet caught up to meet this demand. For example, a search in the course database of the Brazil's largest public university (the University of São Paulo) revealed that since the Data Protection Law was enacted in 2018, only four courses (two for undergraduate students, and two for graduate students) included a mention to this legislation in their syllabus – and all these courses were optional, rather than part of the core curriculum.[xlii] Law degrees offered by smaller, less well-resourced higher education institutions, in particular based in regions other than the southeast of the country, likely struggle even more to teach data protection and prepare students to work in this policy area. Given this state of affairs, it would serve the ANPD's long-term interests to reach out to universities and professional training schools and associations offering to clarify the knowledge and skills required and desired in data protection regulation. Over time, doing so would help to augment the limited pool of talent that currently faces high demand from the market, and thus partially alleviate ANDP's institutional concern around public officials moving into private roles, in a job market where the ANPD is seen as the main training institution .

The literature has also pointed out the risk that current public servants would seek to enhance their future private sector employment prospects by giving preferential treatment to industry actors.[xliii]. Many countries have adopted measures to mitigate some of these 'revolving doors' problems and to minimise the threat of post-employment conflict of interest in the public administration.[xliv] The revolving door can move in two directions. In Brazil, it is not easy to re-enter the public service after leaving it. So, while professionals from the private sector can end up working for the regulator and potentially carry with them sensitive information from firms, this is not salient concern in Brazil and not a strong concern from a public policy perspective. The other direction of movement revolving door requires attention, however. Brazil's Data Protection Law establishes that the directors of the agency are required to observe the rules and procedures set out by the Brazilian Conflict of Interest Law (Law 12813/2013), which applies to federal government officials when they leave their post. This includes a general prohibition to, at any point, share, disclose or use privileged information that they have had access to through their position in the government, and requires them to observe a six-month cooling off period.

During this cooling-off period, former directors would be generally banned from working in private sector activities related to their previous role or institution, or that could benefit from information or contacts that they have had access to while in government.[xlv] The Public Ethics Committee (CEP) or the Office of the General Comptroller (CGU) are responsible for applying this provision and could also offer exemptions to allow former directors to work in the private sector based on a case-by-case assessment.

The Brazilian conflict of interest law (Law nº 12.813/2013), however, has not given the CEP or the CGU the power to tailor the cooling-off period according to the perceived risk of conflict of interest. They can either require that officials comply with the six-month rule or exempt them from the requirement altogether. Notably, only directors of the ANPD are required to comply with the cooling off period, while the law is silent with regards to civil servants fulfilling two other leadership positions within the agency: coordinators and project managers.

Even though bringing forward legislative changes could be challenging, this brief recommends that the law is improved to allow the CEP and the CGU to decide the length of the cooling off period according to the perceived conflict of interest threat in each case, within reasonable restrictions, and to apply to other leadership roles rather than only the directors of the agency. The cooling off period should be carefully tailored to ensure it enhances, rather than undermines, capacity and autonomy. In establishing the appropriate length of the restriction, CEP and CGU would have to strike a delicate balance between preventing unduly cosy relationships between public and private agents and securing a reasonable level of employment freedom to ensure that federal public service careers remain attractive to skilled professionals.

5.3. ADDRESSING BUDGETARY RESTRICTIONS

A key concern of lawmakers and government officials involved in the creation of the data protection authority since the initial discussions were related to fiscal responsibility and the considerable costs associated with creating and staffing a new agency from scratch.[xlvi] Indeed, this has been presented by the Brazilian federal government as the main reason why the data protection authority was initially created under the office of the presidency, rather than as an autonomous agency.

The law that originally created the ANPD (Law 13853/2019) established that the authority would be temporarily a body of the federal executive government, that would not require increase in public expense, and would use the human and financial resources of the presidency office. That is, the authority would not have control over its budget and expenses.

Beyond the more noticeable limitation in terms of political independence, the choice of design at the time also significantly affected the authority's financial independence. The initial version of the law creating the ANPD was approved with a provision allowing it to charge supervisory fees. That is, one of the sources of revenue of the authority, according

to that version, would be the collection of fees to be paid by regulated entities, as a compensation for the state for the regulatory costs associated with their activities.[xlvii]

However, when submitted to presidential approval, the provision allowing the ANPD to collect fees was vetoed by President Bolsonaro. The justification for the veto was that the ANPD was created as a body subordinated to the Presidency only on a provisional basis, which would prevent it from being legally able to charge fees.[xlviii] The ANPD would, therefore, be solely funded by the federal budget unless its legal framing changed.

In June 2022, the Provisional Measure by Bolsonaro changed the legal framing of the ANPD and turned it into an autonomous agency, responsible for managing its own budget. However, the Provisional Measure did not include any mention of the possibility of charging fees. In other words, the justification for the previous veto was extinct, but the legal provision that would ensure that the new ANPD would have more sources of revenues was not reintroduced.

6. POLICY RECOMMENDATIONS

This policy brief has examined the design of the new Brazilian National Data Protection Authority (ANPD), that recently gained the legal status of independent agency, outlining a series of legal and policy proposals to enhance cooperation between the ANPD and other agencies in Brazil, and to enhance its autonomy and capacity to supervise data more effectively.

The recommendations below draw on the analysis of the previous sections and interviews with senior officials in Brazil. They lay out policy avenues for policymakers and government officials to engage in negotiations around the future of the ANPD and aim to provide guidance to Congress, as it scrutinises the bill and to inform future legislative proposals, and to the Executive when writing the regulatory decree that will be issued after the approval of the law. They are combined into three thematic groups: strengthening inter-agency coordination, building resilience against regulatory capture, and increasing revenue though a new supervisory fee.

6.1. STRENGTHENING INTER-AGENCY COORDINATION

The ANPD has led efforts to establish formal connections with several government institutions in its first two years (for example, through the signing of technical cooperation agreements), and the joint declaration around WhatsApp's Terms of Service (ToS) gives positive signs of engagement with the wider ecosystem of digital platform regulators in Brazil. However, there is room to build a more resilient culture of inter-agency cooperation that would extend beyond specific personal ties of staff members.

There are strong reasons to consider the establishment of a more robust infrastructure to facilitate the relationship between difference agencies, in the shape of a regulatory network. This regulatory network would not be a fully-fledged, new agency with a broad mandate to supervise digital platforms – that is, it would not have the status and mandate of a 'digital watchdog'. Rather, it would be comprised of existing agencies and managed by a 'digital coordinator' who would act as an umbrella infrastructure to enhance their links.

In practical terms, establishing this network would also require each agency to clearly identify their 'cooperation nodes', that is, members of staff or units within each organisation responsible for leading on the engagement with other organisations. This would be facilitated by the digital coordinator, who would not have an overlapping mandate with other institutions, but rather the main responsibility to provide channels to enhance the links between government agencies that oversee digital platforms.

The UK experience provides a useful example. Launched in 2020, the Digital Regulation Cooperation Forum (DRCF) joins together the Competition and Markets Authority (CMA), the Information Commissioner's Office (ICO), the communications regulator (Ofcom), and more recently the Financial Conduct Authority (FCA). Its goal is to support regulatory coordination in digital platforms, and foster cooperation on areas of mutual importance.[xlix]

While prior to the creation of the DRCF these regulatory agencies already had a history of cooperation, the forum was created based on the understanding that the regulation of digital platforms brings unique challenges that require even deeper regulatory cooperation. Alongside reducing the risks of conflicting decisions, the forum also aims to enhance regulatory capacities by pooling knowledge and resources from multiple organisations, for example through the conduction of joint investigations and joint research.

In the case of Brazil, establishing a similar regulatory network would contribute to enhancing capacity and autonomy not only with regards to data protection, but also across the wider ecosystem of digital regulators. To save resources, rather than creating a digital coordinator from scratch, this role could be played by the CGI.br. As a multistakeholder institution, the CGI.br has previous expertise in providing the space for dialogue and mediating discussions between different organisations, as well as a broad mandate to oversee internet governance, an area connected to many of the key policy issues around digital regulation.

To be sure, the current structure of CGI.br is inadequate to support the management of a regulatory network, as it lacks the human and financial resources to do so.[l] The

membership structure of CGI.br includes representatives of government line ministries, civil society organisation, industry, and academia, who serve part-time and on a voluntary basis. If the CGI.br was to gain further responsibilities, including the task of acting as a digital coordinator, it would require further resources and at least a permanent secretariat to support the development of the regulatory network proposed here.

The proposed changes would require the introduction of new legislation. Congress is already discussing a bill that would change the structure and the responsibilities of CGI.br, giving it more powers to oversee the activities of internet platforms, in an attempt to enhance transparency and responsibility on the internet.[li] As Brazilian legislators, and the society at large, rethinks the role of this important multi-stakeholder organisation, the moment is ripe to give it powers to act as a digital coordinator.

6.2. BUILDING RESILIENCE AGAINST REGULATORY CAPTURE

As the agency's regulatory power and portfolio salience increases,[lii] it is also more likely to become subject to industry's pressures. In the absence of further concrete measures to reaffirm its autonomy, the data protection authority could become increasingly more prone to special interests (those that benefit specific groups) and could be driven away from pursuing the public interest. In terms of the composition of the workforce, the change in the legal nature of the ANPD - from a body under the Presidency to an independent agency - means that the data protection authority will no longer be able to choose and recruit civil servants from other organisations to work for ANPD.

As an agency, ANPD will only be able to hire civil servants from the general pool of Public Policy Specialists (*Especialistas em Políticas Públicas – EPP*) from 1 January 2027. These people are recruited to work in all areas of the federal public service. This means that the workforce is likely to become less specialised in data protection. Further, the demand for qualified professionals from the private sector could undermine the agency's ability to recruit and retain personnel, giving rise to 'revolving doors' problems while at the same time undermining the agency's capacity.

Various measures could help to mitigate these concerns, the main one involving enhancing post-employment controls to prevent conflicts of interest. This brief recommends that lawmakers should expand the scope of the cooling off requirement to apply not only to directors of the ANPD, but also to other civil servants who are in leadership roles – including general coordinators (*Coordenadores-Gerais*) and project managers (*Gerentes de Projeto)* – and who could therefore face relevant conflicts of interest when they move to the private sector. This could be done either through amendments to the Provisional Measure or through the introduction of specific legislation.

Further, and more widely, the conflict of interest law should be reformed to allow the CEP or the CGU to decide whether the baseline cooling off period of six months should be reduced or increased in each case. The assessment of the conflict of interest threat could be based on the specificities of each case, considering aspects such as the seniority of the public agent, their length of service, the nature of the job in the private sector, salary, among others. However, we recognise that it could be challenging to advance a modification of a law that concerns the entire federal government solely for the purposes of the ANPD.

Regardless, the supervisory role of the CEP and the CGU could also be strengthened. The conflict of interest law gives them the mandate to monitor compliance and to establish rules, procedures, and mechanisms aimed at preventing and addressing conflict of interest. While ensuring compliance with post-public employment measures can be difficult once officials have left their post, measures could be taken to improve existing standards and practices.

Specifically, CEP and CGU could adopt procedures to assess the extent to which the cooling off period is being observed and gather data to inform the design of more effective risk assessment tools. A well-calibrated tool to assess the gravity of the potential conflict of interest threat posed by each individual, coupled with a higher level of flexibility to establish the length of the cooling off period on a case-by-case basis, could go a long way toward ensuring that post-employment measures are proportional, and that the policy strikes the right balance between building integrity while attracting talent to the public service.

Promoting better training is another means to reducing conflict of interest pressures, by reducing job market pressures in the long run. While there is now a growing range of executive education courses, both online and in-person, that promise to prepare data protection lawyers, they are mostly offered by private institutions that charge high admission fees. Ideally, ANPD should support high-quality resources made available to professionals with different income levels and based in all parts of Brazil. The free online training courses offered by Brazil's National School of Public Administration (*Escola Nacional de Administração Pública* – ENAP) designed for civil servants (but available to anyone) is a good example of resource that could help to expand and diversify the pool of data protection professionals.[liii]

Furthermore, to ensure that the pursuit of the public interest remains at the centre of the ANPD's activities, it is important that the agency continue to submit its key decision-making procedures and regulatory proposals to public scrutiny and accountability. For the past two years, the ANPD has consistently used digital platforms to run public consultation and

to collect contributions from different sectors of the society, both around its wider regulatory agenda and on specific proposed regulations.

The authority has also provided detailed responses to the contributions, justifying choices, and explaining the reasons to accept or reject specific proposals, a practice that increases transparency and inhibits more flagrant forms of regulatory capture. These are examples of good practices that contribute to the pursuit of the agency's public purpose, and should continue to be adopted as the ANPD gains full administrative independence.

6.3. INCREASING REVENUE THROUGH INTRODUCTION OF A SUPERVISORY FEE

In light of severe budgetary restrictions, and despite the commitment of existing public officials working at the ANPD, there remain significant human and financial capacity constraints that prevent more effective regulation of data in Brazil. A robust way of increasing the agency's capacity would be expand its revenue sources (listed in article 55-L of the Brazilian Data Protection Law). The most straightforward way of doing so would be through the introduction of procedural fees to be charged to firms that process large amounts of data to cover the costs involved in their regulatory supervision.

This measure has already had the support of Congress in the past, as it was included in the original bill that created the ANPD – but was then vetoed by Bolsonaro.[liv] Reinstating this provision would require amending the Provisional Measure, or introducing a new bill aimed at amending the Data Protection Law, but observers pointed out that welcoming modifications to the text could open the way for a new wave of amendments and run the risk of defusing the legislation.

There are concrete examples of regulators in Brazil and other jurisdictions that rely on regulatory fees as one of their sources of revenue. For example, the Brazilian competition authority (CADE) charges a procedural fee of 85,000 reais (around 16,500 US dollars) to review and approve mergers and acquisitions notifications submitted by firms. In the EU, the recently approved Digital Services Act (DSA) establishes a yearly supervisory fee of up to 0.05% of annual worldwide net income that the European Commission will charge to providers of very large online platforms and search engines, intended to cover the costs involved in monitoring their compliance with the new regulation. The ability to charge a supervisory fee would strengthen the ANPD' budgetary autonomy and enable the agency to more effectively pursue its public purpose.

ENDNOTES

[i] The transition period was established by Portaria Conjunta SG-PR/ANPD No. 141/2022. See: https://www.in.gov.br/en/web/dou/-/portaria-conjunta-sg-pr/anpd-n-141-de-29-de-setembro-de-2022-433106635

[ii] See, for example, the note published by the National Council for the Protection of Personal Data and Privacy (CNPD) in support of the Provisional Measure and of the change in the legal status of the ANPD, but warning against amendments that would introduce changes in substantive provisions in the data protection law: https://www.gov.br/anpd/pt-br/cnpd-2/nota-de-apoio-a-conversao-da-mpv-1-124-2022

[iii] The analysis and recommendations in this brief were informed by semi-structured interviews with individuals, speaking in their personal capacity, who work or have worked at federal agencies in Brazil, including the National Data Protection Authority (ANPD), the competition authority (CADE), the Secretariat for Consumer Protection (Senacon), the Internet Steering Committee (CGI.br), and the Federal Prosecutor's Office (MPF). Interviews were conducted online and in person between January and March 2022. This research has been reviewed by, and received ethics clearance through, the University of Oxford Central University Research Ethics Committee (Reference number: SSH/BSG_C1A-21-02).

[iv] Digital Regulation: Driving growth and unlocking innovation. UK Government, June 2022.

[v] For a detailed analysis of how digital technologies can support economic development, see Pathways for Prosperity Commission. (2018). Charting Pathways for Inclusive Growth: From Paralysis to Preparation. Oxford, UK: Pathways for Prosperity Commission.

[vi] Bruna Arimathea and others, 'Brasil é Terreno Fértil Para Vazamento de Dados e Ações de Cibercriminosos' Estadão (25 April 2021) https://www.estadao.com.br/infograficos/link,brasil-e-terreno-fertil-para-vazamentos-de-dados-e-acoes-de-cibercriminosos,1162667.

[vii] David s evans and richard schmalensee, matchmakers: the new economics of multisided platforms (harvard business review press 2016). On definitional problems and the lack of consensus regarding what constitutes a multisided platform, see michael katz and jonathan sallet, 'multisided platforms and antitrust enforcement' (2018) 127 yale law journal 1742.

[viii] Evans and Schmalensee (n 2).

[ix] The World Bank's 2002 ICT Sector Strategy defines digital technologies as "hardware, software, networks, and media for collection, storage, processing, transmission, and presentation of information (voice, data, text, images)", and this definition remains relevant today (World Bank, 2002).

[x] On the central role played by big data in the digital economy and the challenges it creates for competition law, consumer protection, and protection of privacy, see Caio Mario da Silva Pereira Neto and Bruno Polonio Renzetti, 'Big Data Entre Três Microssistemas Jurídicos: Consumidor, Privacidade e Concorrência' in Caio Mario da Silva Pereira Neto (ed), Defesa da Concorrência em Plataformas Digitais (FGV Direito SP 2020) http://bibliotecadigital.fgv.br/dspace/handle/10438/30031.

[xi] CMA, 'Online Platforms and Digital Advertising Market Study' (Competition and Markets Authority 2020) Market Study Final Report https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study accessed 20 july 2020

[xii] For example, the Stigler report suggests that a sectoral regulator, named Digital Authority, should have the power to conduct merger review in digital markets. Fiona Scott Morton and others, 'Committee for the Study of Digital Platforms: Market Structure and Antitrust Subcommittee' (George J Stigler Center for the Study of the Economy and the State 2019). Guggenberger argues that effective antitrust enforcement requires expertise and resources that would require a specialised agency to act as de facto regulator. Nikolas Guggenberger, 'Essential Platforms' (2021) 24 Stanford Technology Law Review p. 342-343.

[xiii] On the interplay between competition authorities and sectoral regulators for the design and implementation of remedies, see Filippo Lancieri and Caio Mario S Pereira Neto, 'Designing Remedies for Digital Markets: The Interplay Between Antitrust and Regulation' [2021] Journal of Competition Law & Economics nhab022.

[xiv] For example, Van Loo argues that creating effective public digital regulators require adequate funding, anticapture mechanisms, performance metrics, and full information-collection powers, but the author warns that a regulator with these characteristics could amass too much power, requiring the adoption of countervailing and accountability mechanisms. Rory Van Loo, 'The Rise of the Digital Regulator' (2017) 66 Duke Law Journal 1267. Fiona Scott Morton and others emphasise the importance of capacity, arguing that a regulator with sectoral expertise and enough staff are required for effective digital platform governance. Fiona M Scott Morton and others, 'Equitable Interoperability: The "Super Tool" of Digital Platform Governance' (2021) Policy Discussion Paper No 4.

[xv] Fukuyama argues that effective governance institutions are endowed with two key features: capacity, conceived of as resources and professionalisation, and autonomy, the independence of bureaucrats from political principals. Francis Fukuyama, 'What Is Governance?: Commentary' (2013) 26 Governance 347.

[xvi] The authors examine how these two variables interact with a third variable: the political dominance of individual parties within each agency. These dimensions of governance are important because they are found to influence corruption. For example, low capacity and low autonomy are associated with higher corruption.

[xvii] Roberto Rocha Coelho Pires and Alexandre de Ávila Gomide, 'Governança e Capacidades Estatais: Uma Análise Comparativa de Programas Federais' (2016) 24 Revista de Sociologia e Política 121.

[xviii] Peter Evans and James E Rauch, 'Bureaucracy and Growth: A Cross-National Analysis of the Effects of "Weberian" State Structures on Economic Growth' (1999) 64 American Sociological Review 748.

[xix] Katherine Bersch, Sérgio Praça and Matthew M Taylor, 'Bureaucratic Capacity and Political Autonomy Within National States: Mapping the Archipelago of Excellence in Brazil' in Miguel A Centeno, Atul Kohli and Deborah J Yashar (eds), States in the Developing World (1st edn, Cambridge University Press 2017) https://www.cambridge.org/core/product/identifier/9781316665657%23CT-bp-6/type/book_part accessed 11 July 2022.

[xx] It is important to acknowledge that the component variables of each of the two dimensions – capacity and autonomy – are also related. For example, institutions with higher relative budgets are arguably more likely to develop higher capacity, by increasing their abilities of hiring more expert bureaucrats.

[xxi] Barbara Geddes, 'Building "State" Autonomy in Brazil, 1930-1964' (1990) 22 Comparative Politics.

[xxii] The term 'coordination' has been used in the political science literature to label a wide-range of issues. The diversity in the literature reflects the fact that coordination problems have multiple causes, can exist in different levels, and can be often created or resolved through different process and mechanisms, in different contexts.

[xxiii] Geert Bouckaert, B Guy Peters and Koen Verhoest, The Coordination of Public Sector Organizations: Shifting Patterns of Public Management (Palgrave Macmillan 2010).

[xxiv] For example, Lancieri and Pereira Neto propose four criteria to guide the allocation of regulatory powers between enforcement agencies with overlapping jurisdictions: (i) differences in legal mandates; (ii) the need for technical expertise; (iii) the relative risks of regulatory capture; and (iv) the costs of an administrative regime. See Filippo Maria Lancieri and Caio Mario da Silva Pereira Neto, 'Designing Remedies for Digital Markets: The Interplay between Antitrust and Regulation' [2021] FGV Direito SP Research Paper Series https://papers.ssrn.com/sol3/papers.cfm?Abstract_id=3704763. P. 35-37.

[xxv] In general terms, regulatory capture is associated with orthodox accounts of the economic theory of regulation, which challenges the idea that regulation is primarily designed to protect and advance some notion of the public interest. According to Stigler, regulation would be "acquired by the industry and is designed and operated primarily for its benefit". See George Stigler, 'The Theory of Economic Regulation' (1971) 2 The Bell Journal of Economics and Management Science 3. P. 3.

[xxvi] For a summary of the criticism directed to the theory of regulatory capture and alternative accounts proposed by the literature, see Robert Baldwin, Martin Cave and Martin Lodge, 'Explaining Regulation', Understanding Regulation: Theory, Strategy, and Practice (Oxford University Press 2011).

[xxvii] ibid.

[xxviii] Katherine Bersch, Sérgio Praça and Matthew M Taylor, 'State Capacity, Bureaucratic Politicization, and Corruption in the Brazilian State: State Capacity, Bureaucratic Politicization, and Corruption' (2017) 30 Governance 105.

[xxix] More specifically, Heywood & Kirby argue that a public institution has public integrity "if it has a robust disposition to pursue its purpose, efficiently, within the constraints of legitimacy, and consistent with its commitments."

[xxx] An accompanying working paper will expand on the relationship between capacity, autonomy and institutional integrity when it comes to the regulation of digital technologies.

[xxxi] Pesquisa Anual do Uso de TI, EASP FGV, June 2022, available at https://eaesp.fgv.br/producao-intelectual/pesquisa-anual-uso-ti

[xxxii] However, inequalities remain between segments in different socioeconomic levels, with 95% of individuals in the higher level of income being internet users, in comparison with 57% in the lower income brackets. There are also rural-urban divides, with the proportion of individuals who lived in rural areas of the country and who were internet users reaching 53% in 2019. Nic.br, 'ICT Households: Survey on the Use of Information and Communication Technologies in Brazilian Households' (Comitê Gestor da Internet no Brasil 2020) *https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nos-domicilios-brasileiros-tic-domicilios-2019/*.

[xxxiii] For a detailed analysis of the complexities involved in the enforcement of the Brazilian data protection law, taking into consideration the pluralistic legal and institutional environment in Brazil, see Miriam Wimmer, 'Os Desafios Do Enforcement Na LGPD: Fiscalização, Aplicação de Sanções Administrativas e Coordenação Intergovernamental' in Laura Schertel Mendes and others, Tratado de Proteção de Dados Pessoais (Editora Forense 2021).

[xxxiv] Bouckaert, Peters and Verhoest (n 21).

[xxxv] https://www12.senado.leg.br/noticias/materias/2022/06/14/mp-concede-autonomia-de-autarquia-a-autoridade-nacional-de-protecao-de-dados

[xxxvi] http://www.mpf.mp.br/pgr/noticias-pgr/mpf-cade-anpd-e-senacon-recomendam-que-whatsapp-adie-entrada-em-vigor-da-nova-politica-de-privacidade

[xxxvii] http://www.mpf.mp.br/pgr/documentos/ataconjunta.pdf

[xxxviii] https://www.poder360.com.br/justica/mpf-pede-ajustes-na-politica-de-privacidade-do-whatsapp/

[xxxix] For a discussion of formal and informal institutions and organisations, drawing on the concepts first proposed by Douglas North, see Natalia Boliari and Kudret Topyan, 'Conceptualizing Institutions And Organizations: A Critical Approach' (2011) 5 Journal of Business & Economics Research (JBER) https://clutejournals.com/index.php/JBER/article/view/2507 accessed 11 July 2022.

[xl] Bouckaert, Peters and Verhoest (n 21). P. 12.

[xli] ibid.

[xlii] The courses offered by the University of Sao Paulo that mention the Brazilian Data Protection Law in their syllabus, as of August 2022, include: DFD0218 - Direito e Tecnologia: Privacidade e Proteção de Dados (undergraduate); DES5891 - O Direito Administrativo e Empresarial da Proteção de Dados Pessoais (postgraduate); DCO5891 - Direito ao Espaço Virtual (postgraduate); and DCV5953 - A Lei Geral de Proteção de Dados Brasileira (undergraduate).

[xliii] OECD, Post-Public Employment: Good Practices for Preventing Conflict of Interest (OECD 2010) https://www.oecd-ilibrary.org/governance/post-public-employment_9789264056701-en accessed 31 August 2022.

[xliv] See generally OECD (n 1).

[xlv] Rules established in article 6 of Law 12813/2013.

[xlvii] The bill approved by the Congress included the following provision: "Art. 55-L. The revenue of the ANPD include: (...) V – the outcome of the fees charged for services rendered".

[xlviii] See the reasons for the vetoes here: https://www2.camara.leg.br/legin/fed/lei/2019/lei-13853-8-julho-2019-788785-veto-158685-pl.html

[xlix] For more details about the DRCF, see https://www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-202122/digital-regulation-cooperation-forum-plan-of-work-for-2021-to-2022

[l] The CGI.br is a committee whose current structure was established in 2014, with the approval of the Marco Civil da Internet (MCI) that with responsibility to develop guidelines related to the use and development of the internet in Brazil, and to support the protection of the principles that guide internet use in the country – including privacy and network neutrality. https://www.cgi.br/publicacao/o-cgi-br-e-o-marco-civil-da-internet/91

[li] This proposal is included in Bill 2630/2020, also known as 'fake news bill' (PL das Fake News). More details here: https://www.camara.leg.br/noticias/863031-relator-apresenta-nova-versao-do-projeto-sobre-fake-news-conheca-o-texto/

[lii] For a detailed discussion around portfolio salience and patronage in Brazil, see Cesar Zucco, Mariana Batista and Timothy J Power, 'Measuring Portfolio Salience Using the Bradley–Terry Model: An Illustration with Data from Brazil' (2019) 6 Research & Politics 205316801983208.

[liii] See, for example, the course Introduction to the Brazilian Data Protection Law: https://www.escolavirtual.gov.br/curso/153

[liv] https://www2.camara.leg.br/legin/fed/lei/2019/lei-13853-8-julho-2019-788785-veto-158685-pl.html