International Cybersecurity Law Review
https://doi.org/10.1365/s43439-023-00081-2

Alternatives for an adequate structuring of the national data protection authority (ANPD) in its independent profile: proposals to overcome the technological challenges in the age of digital governance

Gabrielle Bezerra Sales Sarlet · Daniel Piñeiro Rodriguez

Received: 20 October 2022 / Accepted: 10 January 2023

Abstract This article aims to identify the necessary elements for the independent and democratic structuring of the National Data Protection Authority (ANPD) in its definitive legal profile, as an autarchy under a special regime, so that it can achieve the technical and decision-making autonomy that it was granted by the Brazilian Data Protection Law (LGPD). Drawing on documentary research and findings on similar foreign authorities, it is possible to point out, as a partial result of this analysis, the insufficiency of entrusting such a mission to its recent formal separation from the Direct Administration, being also possible to conclude that the success of the state modernization in the Digital Age will depend, to a large extent, on intertemporal choices able to direct the ANPD towards a structure attentive to technological innovations. To this end, the training and continuing education of the institution's staff, as well as possible agreements to be signed by the entity, such as the alternatives sought by the Courts of Accounts in the field of information and communications technology (ICT), emerge as a determining factor.

Keywords Data protection · State · Constitutional law · Brazil · Technology

1 Introduction

In Brazil, after decades of discussion about its Data Protection Law (LGPD) in Congress, a special public body was created and tasked with guaranteeing the multiple projections of human beings in the new global context, particularly regarding the digital realm, viz. the National Data Protection Authority (ANPD). The anxiety that preceded its creation is not surprising: according to 2019 data made known by

✉ Gabrielle Bezerra Sales Sarlet
Pontifícia Universidade Católica do Rio Grande do Sul, Fortaleza, Ceará, Brazil
E-Mail: gabriellebezerrasales@gmail.com

Published online: 13 February 2023

the Brazilian Institute of Geography and Statistics (IBGE), 82.7% of the Brazilian households have internet access, which represents a 3.6% increase in relation to 2018, with advances in all age groups [2]. Although this reality can be seen as a positive one as it promotes more access to information, it also activates a state duty of protection and consequently of education as to the risks present in this new locus of public debate. The number of information security incidents that preceded the creation of the ANPD—some of them of national proportions—demonstrate the harmful effects caused by Brazil's delay in creating a regulatory body in the area of data protection.

This article aims to identify the weaknesses in the present national context involving the protection of personal data as far as the actions of the newly created Brazilian authority is concerned, through documentary research, in comparison with foreign experiences in the structuring of their regulatory agencies in the area of data protection, particularly concerning the degree of independence from the central government's power in the age of digital innovation. It intends to highlight the elements which, beyond their mere formal separation from the direct administration, are apt to lead to a democratic and impartial state structuring that aims at an management that is effective and, above all, responsive to technological evolution.

2 What is the state good for (in the digital turning point)? Updating a central question

The development of technology has potentiated the degree of surveillance to which society submits itself. In the area of consumption, for instance, people experience an increasingly intense communicational coercion, in which personal data are extracted by big corporations for different purposes, including eminently commercial ones. In the area of public security, in turn, there is a growth in the unbridled use of face recognition technologies in police investigations, but in Brazil there is a lack of protective legislation applicable to this sector—whereas the European Data Protection Supervisor (EDPS), moving to a diametrically opposite direction, points to a greater restriction of their use in public spaces, taking into account what it called "extremely high risks of deep and non-democratic intrusion into individuals' private lives", prompting some countries to even call for a moratorium [14].

This concern is not unreasonable considering the present scenario of blatant lack of protection of the Brazilian state's information systems. In 2020 it became public that data of 243 million Brazilians were exposed in the registry base of the Health Ministry [20], right after the occurrence of an incident involving the leakage of passwords in the system that enabled access to data on other 16 million citizens diagnosed with COVID-19 [32]. The perpetrators are still unknown and the mega-leakage is being investigated by the Federal Police since February 2021 upon request of the ANPD. In the realm of the Judiciary there have also been cybernetic attacks against the website of the Superior Court of Justice—which is the responsible court for standardizing the interpretation of federal law throughout Brazil [31]—and of the Brazilian Supreme Court [27].

Such a succession of cybernetic attacks exposing the fragility of the government's information systems seems to have finally awakened the concern of Brazilian civil society to the resurgence of vigilantism in general and to state surveillance in particular. It is a fact that as a natural collector of data the state has legitimacy to process information on the population not only aiming at a good execution of public policies but also of several legal functions as provided by the LGPD (Article 7, items II and III).

However, the absence of clearcut limits to the sharing and use of data in the public sector, v. g., may lead to the shaping of a super-powerful state whose *informational unity* [34, p. 135] would invert even the Hobbesian logic of the modern state: far from having in the guarantee of law and order its primary duty, such a novel tacit pact between the state and the market may ultimately aim at the maintenance of political power through surveillance, thus creating a super-vigilant and potentially oppressive Leviathan that disrespects human and fundamental rights, informational self-determination of individuals and, in effect, the premises of the rule of law.

The reflection proposed in this article reveals the need to awaken the state from its old and already traditional *immobilism*, so that it follows and fulfills its constitutional mission in the midst of the transformations of the *Fourth Revolution* that is shaped from the bottom-up [19, pp. 211–213] without slow-down, so that the government takes part in it. What is ultimately at stake is the preservation of what is viewed as the minimum duty of a state entity, viz. the preservation of law and order in a democratic regime—but now in the midst of cyberspace. Therefore, it is crucial to have a speedy—but attentive—independent structuring of the ANPD, the architecture of which is discussed below based on traditionally consolidated experiences.

3 The ANPD: genealogy, structure and functions

By creating the ANPD Brazil became part of the list of countries aligned with the international legislative trend of assigning to the state a duty of protection of the fundamental rights, guarantees and freedoms connected to the protection of personal data. It should be noted, however, that the initial version of the draft bill of the ANPD (Bill of Law no. 5.276/16) did not provide for the entity, which only occurred after the drafting of the technical opinion of a special commission of the Chamber of Deputies, which planned it as an *autonomous federal agency with a special regime*—thus belonging to the indirect administration [24, p. 165].

In this case there was a clear intention of distancing it from the center of political power. That drafting, however, was vetoed by the President because it involved a rise of expenditures—which would, consequently, attract a competence privative of the President regarding the legislative proposal. Attempting to overcome this hindrance and nonetheless maintain the creation of the essential entity in the LGPD, the text passed instituted it "without increase of expenditures" and as an agency of the direct administration as a part of the Presidency of the Republic (Article 55-A).

The connection of the new state agency to the Presidency has raised doubts about the possibility of guaranteeing the independence necessary for the performance

of its functions. Not without reason, in a report published in October 2020 the Organization for Economic Cooperation and Development recommended that the Brazilian government should "Re-evaluate and amend the conditions establishing the National Data Protection Authority [...] to ensure that the Authority operates with full independence from the date of its establishment" [21].

This critique had been expected and anticipated by the legislator, who, in its prospective remarks, introduced a temporal trigger in the LGPD by providing for the *transitoriness* of this regime: According to Article 55-A, the legal nature of the ANPD was transitory and could be transformed by the Executive Power into an entity of the indirect federal public administration, submitted to a special autonomous regime. In the next paragraph the legislator determines that the assessment about the mentioned transformation should take place within two years from the date of the entry into force of its structuring regime (§ 2). However, because of a curious legislative construction in Presidential Order no. 10,474, issued on August 20, 2020, the effectiveness of that regiment was conditioned to the appointment of the agency's first Director-President, which only occurred on November 6, 2020, after the approval of the five directors at the Senate's confirmation hearing.

Finally, in June 2022, Provisional Measure no. 1.124, altering the nature of an agency of the Presidency of the Republic, transformed the ANPD into a federal autarchy under a special regime, with its own assets and headquarters and jurisdiction in the Federal District, according to the new wording given to article 55-A of the LGPD [6]. In October of this same year, this Provisional Measure was converted into Law (Law n. 14.460/2022) and, more recently, the Presidential Decree No. 11.348/2023 has changed ANPD's further vinculation from Republic Presidency to the Ministry of Justice, as the original bill.

After the overcoming of possible criticisms of the entity's troubled entry into the national scenario, it must be acknowledged that other countries also faced tardily the challenges involving the creation of an independent regulatory agency in the field of data privacy. For this reason, it is salutary to consider their respective regulatory experiences.

Prominent in this respect is the case of Argentina, whose regulatory authority experienced a long period of structural transition. The National Directorate for the Protection of Personal Data, initially created as a body of the direct administration subordinated to the Justice Ministry, became a part of Agency of Access to Public Information in 2017, thus becoming a part of the indirect administration. As pointed out by a comparative study of the main data protection authorities in Latin America [26, p. 13] conducted by the Brazilian Consumer Protection Institute, that restructuring resulted from a recommendation made by the European Union in its decision about the country's level of adequacy to the European block, and it intended to provide an institutional design that will in fact guarantee an actual hierarchical distancing from the state and thus to enable the exercise of the agency's supervisory and regulatory tasks in a more independent manner.

Uruguay's regulatory experience is different. According to the "Report on Data Transference between Europe and Brazil" [33, p. 16] by the Institute of Technology and Society of Rio de Janeiro (ITS-Rio), Uruguay had its adequacy recognized by the European Commission as early as in 2012, although it instituted a regulatory

authority that was part of the direct administration—which, therefore, did not have a legal personality of its own, as is the case of autonomous government agencies. Once the Data Protection Law was passed, the Personal Data Control and Regulatory Unit (URCDP) was also established as an agency disconnected from the Agency for the Development of Government e-Government and the Information and Knowledge Society (AGESIC). Act no. 18,331 of 2008 gave technical autonomy to that Unit. Thus, despite belonging to the direct administration, Uruguay has succeeded in demonstrating sufficient autonomy, thus conforming to the requirements set by the General Data Protection Regulation (GDPR).

It can be seen that the independence necessary for the data protection regulatory authorities is not *exclusively* derived from their formal separation from the direct administration but from a complex structuring that enables them to proceed freely, in a way impervious to political influence. It is in this sense that Brazil's LGPD attempts to bring instruments that will make up for the lack of formal alignment by providing not only for its transitory nature but also through countless provisions that typify an independent profile. This applies, e.g., to Article 55-B of the LGPD, which, in the image of Uruguay's legislation, gave the ANPD technical and decisional autonomy [5] or to the provision that the entity's Administrative Board will be made up of members with term limits who have passed a confirmation hearing and have been appointed by the President of the Republic (Article 55-D, §§ 1 and 3).

In fact, the essential autonomy of the ANPD has been a subject of constant debates. Besides its formal connection to the Presidency of the Republic, members of the Legislative Power[1] have already raised concerns about what they call a "double filter" exercised by the Executive Power at the appointment of its *consultative body*, the National Council for the Protection of Personal Data and Privacy. This is due to the fact that the Presidential Order no. 10,474/20, which provisionally structures the Authority, conditioned the appointment of representatives of civil society and the labor sector to the preparation of a triple list by the Board of Directors of the ANPD,[2] which is the entity's highest governing body.[3] Taking into consideration that the Administrative Board is made up exclusively of members appointed by the President's Chief of Staff, in addition to the lack of objective criteria to guide the preparation of the triple list, the legislative intention of establishing a consultative body with representation from multiple sectors may be harmed. For this reason, in 2020 the OECD recommended that Brazil should "Ensure that the rules for appointing the ANPD's [acronym in Brazilian Portuguese] Administrative Board and the National Council for the Protection of Personal Data and Privacy (CNPDP [acronym in Brazilian Portuguese]) are transparent, fair and based on technical expertise".

[1] Regarding this topic, Legislative Decree no. 394/2020, which attempts to suspend points of Presidential Order no. 10,747—which, in the Parliament's member view, mitigate the autonomy given the ANPD by the LGPD—is pending in the Chamber of Deputies.

[2] "Art. 15 ... Upon receiving the appointments, the Administrative Board will prepare a triple list of regular members and deputy members, representatives of each one of the entities which § 5 refers to, for each office described by items XI to XV of the head, which will be sent to the president's Chief of Staff for appointment by the President of the Republic" (Brasil, 2020).

[3] "Art. 55. The ANPD is made of: I—Administrative Board, highest directive body ..." [5].

It should be noted that, by stressing the role of democratic legitimacy of the entity's consultative body, the LGPD raises the participation in the National Council to a *performance of a relevant public service* (Article 58-A, § 4) insofar as it is tasked with: (i) proposing strategic guidelines and offering contributions to the working out of the National Policy for the Protection of Personal Data and Privacy; (ii) submitting annual reports evaluating the execution of its actions; (iii) suggesting actions to be undertaken by the ANPD; (iv) conducting studies, promoting debates and public hearings and (v) disseminating knowledge about the topic among the population (Article 58-B). Hence the urgency of ensuring its free composition as it plays a structural role in the construction of a democratic, inclusive and plural data protection culture.

But there are other controversial provisions in the Order structuring the ANPD that raise doubts about the purpose of their insertion. Outstanding among them is the wording of Article 2, item XX, which, although replicating the competence already provided in the LGPD to "deliberate, in the administrative sphere, in a terminative manner, about the interpretation of this Act, its competences and unforeseen cases", introduces an initial exception to the duties assigned to the General Counsel for the Federal Government by Supplementary Law no. 73/93 (BRASIL, 2020). The provision's imprecise wording generated controversy among scholars and politicians [9], including mention to a potential "threat to the Authority's autonomy".

Another point that gave rise to discussions has to do with the composition of the ANPD's Administrative Board. According to Order no. 10,474/20, that body has ample powers to, e.g., request from government agencies specific information about the ambit and nature of personal data processed by them (Art. 4, item I, b). It is also tasked with regulating the communication or shared use of *sensitive personal data* among controllers (Art. 4, item II, a). Thus, the appointment of three military [10] to most of the five seats led to a critical response by organized civil society. A survey conducted by the *Associação Data Privacy Brasil de Pesquisa* points out that, among the countries considered economically advanced, only Russia and China have military in the composition of their respective Personal Data Protection Authorities [36, p. 4].

As can be inferred from this discussion, there is a multiplicity of elements necessary for the triggering of a responsive, independent, inclusive and non-verticalized action by ANPD. Only based on this view will this entity be capable of responding to the *poly-contextuality* present in that which [30, pp. 2–28] calls *global villages*, i.e., a context of legal pluralism formed by different public and private actors that is marked by self-regulation mechanisms but does not prescind from the state's action to guarantee values of democracy and social stability [29, p. 63]. Incidentally, even in Europe criticisms are already being levelled at the responsiveness and sufficiency of the model of regulated self-regulation [28], since it has proved to be significantly soft, v.g. the standardization of the recent Codes of Conduct published to regulate the activity of providers of cloud computing (CISPE Code of Conduct and EU Cloud Code).

In fact, in order to move away from the naïve view that a mere formal decentralization of that entity will suffice to protect its important mission or that the formal creation of a consultative body will guarantee democratic representativeness, it is

imperative to keep *windows to the world* open [3, p. 292], paying attention to recent studies that investigate the relation between *actual* political independence of the regulatory authorities and the legal independence ensured to them.

At any rate, the recent critique presented by Hoffmann-Riem [17, p. 112] deserves to be highlighted. In his view, the public institutions created so far are not sufficient for the protection of personal data for a series of reasons—comprehending technological unpreparedness and a shortening of the oversight realm established by legislation, which occasions even a discussion about the creation of a special "digital agency" with even broader powers.

4 International parameters

Besides the possible critique resulting from a marked *regulatory eurocentrism* pervading Brazil's strategy [29, p. 131], it is clear in light of the above discussion that the ANPD's definitive institutional design is directly connected to its ability to regulate the data processing promoted not only by the private sector but also by the government, a topic that is particularly sensitive in several countries, mainly those that have a recurrent authoritarian experience/trend. Some of the already structured regulatory initiatives in Latin America are submitted to critique concerning this point, as there are doubts about the actual oversight performed by them.

In a research project conducted by Brazilian Consumer Protection Institute it was found that since the creation of the Argentine Authority in 2001 until May 2019 there is no record of the enforcement of sanctions by the government due to the misuse of personal data processing by entities of public nature, which is evidence of a significant regulatory asymmetry in comparison to the oversight and control exercised by the private sector [26, p. 22].

In Colombia's regulatory experience, as far as the Superintendence of Industry and Commerce is concerned—which later became the *Delegatura* of Data Protection—does not have the power to directly sanction the state, so that in such a case the preliminary investigation must be referred to the Nation's Office of the General Counsel. In Uruguay, finally, although the government is subject to investigations just like private organizations, the interviewed representatives of civil society question the application of "political filters" in this activity, given the proximity of the *Unidad Reguladora y de Control de Datos Personales*, a deconcentrated agency of the *Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento*, which is an integral part of the Presidency of the Republic [26, p. 29].

The examples presented here are intimately related to the entity's supervisory autonomy vis-à-vis the government itself. And, transferring the debate to Brazil, as reminded by [18, p. 275], in our legal system there are innumerable examples of institutions whose regulatory functions were frustrated by the absence of independence. Consequently, it is salutary to consider a more modern notion of regulation, based on a greater balance between public and economic interests for the good of civil society.

This is also proposed by the idea of "responsive regulation" [4], suggesting the abandonment of old paradigms associating the state's regulatory function primarily

with the enforcement of sanctions and, in contrast, welcoming a *rewarding* role. An illustration of this consists in the fostering of good practices or ratifying sectoral self-regulatory initiatives. According to Carloni, Doneda and Mendes [9], only based on a dialogical and tripartite action involving data subjects, the state and private organizations will the ANPD be able to work out a regulatory policy adequate to its competences.

Strictly speaking, this logic can be extracted from Article 55-J, item XIV of the LGPD, which establishes as one of its duties precisely "to listen to processing agents and to society in matters of relevant interest and to report on their activities and planning". This openness to deliberation will certainly protect the entity from potential political influences in the process of strategic decision-making.

Such a concern is not unreasonable. In a study that analyzed more than 100 regulatory agencies in 16 European countries, v.g., Ensser-Jedenastik [12, p. 507] attempted to discover whether there is, in fact, a positive relation between the recognition of formal independence of the decentralized entities and an actual reduction in the partisan political interference in the appointments to the directive offices and, consequently, in the regulatory activities promoted by the state. Upon analyzing several aspects—such as the volume of resources directed to the agencies, the profile of appointed officers and the period of their existence in the legal system—the study concluded that the granting of greater independence at the legislative level ultimately fosters and *even greater* political effort to influence the entities' leadership.

Thus, the adoption of normative formulas designed to give technical credibility to the various sectors of civil society also occasions a migratory and pervasive migratory effect by the central Executive Power. In the author's view, this phenomenon does not necessarily prove to be something negative but demonstrates a clear adaptation of political parties to organizational transformations in the public sector, which is present, as shown by the study, in several democratic governments [12, p. 516].

In light of this, the Brazilian challenge is not an isolated case but also does not make a transposition impossible. It is, at any rate, a matter of overcoming a potential political asphyxiation of an eminently technical agency which cannot, therefore, neglect a crucial factor in the phase of its structuring, viz. the state's modernization vis-à-vis technological transformations.

A recent report published by the Brave browser with the suggestive title "Europe's governments are failing the GDPR: Brave's 2020 report on the enforcement capacity of data protection authorities" shows a clear causal relationship between the degree of investment in information technology experts and the investigative capacity of European authorities to ensure the enforcement of the GDPR. In comparative terms, entities such as the British Information Commissioner's Office and the 17 German authorities (including the regional entities) stand out not only due to the budget volume allocated to the sector but also to the allocation of resources for technical staff.

Of course, it should not be expected that the ANPD will achieve in the short term the same degree of maturation of agencies whose tradition and know-how stand out at the international level. There are, however, some lessons that can and must be considered by the Brazilian state in its decision-making towards the entity's definitive structuring. And this entails the need to introject the present debate starting from the

academic milieu, enabling agents to make *choices of an intertemporal quality* [15, p. 237], so that they may persist beyond transitory government policies.

5 State and technology: a step towards the reinvention of the state

The unique position that the NPDA will hold in our legal system can be seen in the list of its tasks, which denotes an extremely multifaceted and inaugural profile in Brazil's government. This is so because the LGPD positions itself as an *activator* of duties in the public and private sector, as it is allowed to establish a minimum standardization of technical and administrative measures to be adopted by the processing agents for the preservation of the security of their information systems (Art. 44, § 1); as a *guarantor* of fundamental rights tasked with 'ensuring the protection of personal data' (Art. 55-J, item I), which includes the role of *educating* the population about the norms and public policies related to the topic (item VI), and as an *overseer*, since it must oversee and enforce sanctions in cases in which data processing is not in compliance with the legislation (item IV), a point that usually raises major controversies, particularly concerning the autonomy of the other government agencies and the federated entities themselves [35, p. 384].

According to [11, p. 463], the consequent distinction between "regulatory authorities"—which are customarily linked to a particular public service or exploration of economic activity—and "guaranteeing authorities", a group to which the ANPD belongs and whose main task will be the protection of *subjects*, a duty from which all its regulatory, supervisory, educational and sanctioning duties are derived.

Thus, it will exercise the state presence required for the protection of the projections of the human, embodying the global challenge of modernizing the government in view of the rapid technological evolution. Such a central position in the legal system, which will function as a kind of *civilizational anchor*, must be particularly sensed in the process of *platformization* of the Brazilian state, as inferred from the newly enacted Digital Governance Act (no. 14,129/2021) that assigns to it the duty of issuing complementary norms regarding the compliance with the rights contained in the LGPD in the processing of personal data by the government.

Fortunately, as seen above, Brazil does not face this challenge in an isolated manner. The latter imposes itself on a global level and fosters innumerable investigations of which the Brazilian state can—and must—avail itself. In a study published in the *Computer Law & Security Review*, Raab and Szekely [23, pp. 421–433] examined in which way several regulatory data protection authorities have faced the advance of the employment of new technologies and, as a consequence, the repercussions on the entities' structuring. For this purpose, the researchers sent questionnaires to 79 entities, including regional authorities and European organizations. In order to get responses faithful to the questions, the participating agencies were kept anonymous. Finally, it should be stressed that not all authorities answered all questions.

In one of the questions, the researchers "wanted to know the number of people on the staff of the DPAs ... who have expertise in, or significant familiarity with, ICT"

(Q. 4 and 5)[4]. The responses showed, regardless of the size of the authority's staff, a unanimous dissatisfaction when the proportion of expertise is below 10%. At the opposite end of the spectrum there is a prevalence of satisfaction when the number of professionals is above 50%. Between these two points there is a significant scattering of responses.

Raab and Szekely also attempted to identify the impact of the technicians' professional profile on the conduction of investigations in the European scenario. For this purpose, the following questions (Q. 8 and Q. 9)[5] were asked: "What percentage of your organization's investigations involve information and communications technology (ICT)-related aspects (e.g., the use of computerized databases) and what percentage of investigations require specific ICT expertise?"

In this respect the study showed a large prevalence of investigations requiring only general knowledge of ICTs—only a few entities had a symmetry between both (general and specific) levels of knowledge. The result discloses a possible "deliberate blindness" insofar as the entities, aware of their insufficient technical knowledge, would choose to carry out more investigations requiring less knowledge in the field of technology.

Their research also showed a clear preference for in-house know-how development by the agencies, i.e., a rejection of the importing of external expertise to the public service.[6] The reasons adduced for this choice are of an intuitive nature: besides the cost and daily availability to meet the demands, there is a concern with the entity's independence.

In August 2021, corroborating the conclusions of that study, the report drafted by the European Data Protection Board (EDPB) showed that the challenges for an adequate structuring of data protection authorities are still felt in most European states: only 14% of them claimed that human resources available for the fulfillment of their regulatory duties are sufficient [13, p. 6].

The conclusions of these studies seem to be relevant to Brazil's legal scenario, particularly when considering the relative temporal space between the Brazilian entity's present profile and its future structuring as an autonomous agency.

[4] "Q 4. What proportion of these members of your staff have expertise in, or significant familiarity with, ICT? Q 5. Are you satisfied that this proportion is sufficient for the work of your DPA?".

[5] "Q 8. What percentage of your organization's investigations (responding to data subjects' complaints or initiated by the DPA itself) involve ICT-related aspects (e.g. the use of computerized databases or the Internet)? Q 9. What percentage of your organization's investigations (responding to data subjects' complaints or initiated by the DPA itself) require specific ICT expertise?".

[6] "The second most popular method was 'bringing in expertise from outside when necessary': more than twenty DPAs preferred this option. This seems to be somewhat contradictory to the opinions expressed in the issue of developing expertise in-house v. importing expertise from external sources, when only five responding authorities were in favor of the latter alternative. The results lead us to conclude that DPAs clearly distinguished the two situations: the importing of external expertise in investigations, and the importing of external expertise for educational purposes" [23, p. 428].

6 ANPD's structuring in its provisional profile and alternatives for its continued openness to technological transformations

The movements made by ANPD in the first year of its existence indicate that it is attentive to the need to structure itself so that it is up to the magnitude of its challenge, viz. becoming agile and sufficiently appropriate to guaranteeing the implementation of the fundamental right to data protection, which, in turn, is anchored in the guarantee of the state's informational division, the due informational process and the protection of informational self-determination.

Thus, in November 2021 the ANPD published an edict for selection, seeking to attract several profiles of professionals within the federal public administration itself, particularly those with training in ICTs, preferably with "experience in the planning and oversight of ICT contracts" and "knowledge about Digital Governance Strategy". The request for proposals also attempted to attract designers skilled in UX (user experience), i.e., with knowledge about user experience in digital environments [1].[7]

Later, in February 2022, Presidential Order no. 10,975/2022 altered the norms that structured the ANPD in its provisional profile and created the *General Coordination of Information Technology*, a new body to directly assist the Administrative Board (Art. 3, item III, subitem d of Presidential Order no. 10,975/2022) that will have three executive appointed positions: one of General Coordinator, one of Coordinator and one of Division Head [22].[8]

In parallel, the agency has also shown interest in the capacity-building of already allocated employees by offering them training opportunities such as specific courses on data protection and ways of dealing with security incidents. It should be added that the courses and topics can be chosen by the employees themselves and their immediate superiors, provided the choice is adequately justified and ruled by specific criteria [1].

These initiatives aiming at the improvement of the agency's structural rules and capacity-building of civil servants precisely in the area of information technology are aligned with a concern of all sectors of society: according to a survey conducted by the *Associação das Empresas de Tecnologia da Informação e Comunicação* (TIC) *e de Tecnologias Digitais* (BRASCOM), the expected demand for technology professionals in the next five years went up from 420,000 in 2019 to almost 800,000, which constitutes a collective challenge to train agents to act in the public and private sector [8].

However, although the measures related to structuring and capacity-building adopted by the authority's leadership are salutary, they do not seem to be sufficient to enable the government's staff to keep up with digital society's dynamic transformations as they are part of a highly centralizing culture. For this reason, several public entities have been searching for new paths.

Just to give an idea of the problem, the Federal Accounting Court, for example, announced in February 2022 the execution of an unprecedented contract, viz.

[7] Available at https://www.gov.br/anpd/pt-br/canais_atendimento/Editalfinal.pdf.

[8] Available at http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D10975.htm.

a "technological order" for artificial intelligence solutions to support the evidentiary stage of accusations and petitions [7]. It can be inferred from the invitation for bids that its purpose is precisely to counter the shortage of IT professionals, since it aims at the development of an "artificial intelligence-assisted training module" that should become part of the Court's assisted fact-finding, including an openness to "future public acquisitions"—which denotes the necessary continuity of this service. Thus, the macro-goal of the contract execution for the contracting entity itself is "to change work process and to promote a digital transformation" in the Accounting Court [7]. The bid notice allowed the participation of private law companies of any size, non-profit private law entities, science and technology institutions and their associated foundations and businesses.

Analyzing the paths sought by the Brazilian Audit Courts is justified both by the independence such entities should have and by their common duty to perform audits in the fulfillment of their supervisory function—which, in the case of the ANPD, is determined by Article 55-J. item XVI of the LGPD. Thus, in order to find out whether a personal data controller carries out a processing that, for instance, has discriminatory consequences for data subjects, the national authority must have the technical capability to verify the unlawfulness without, however, violating the commercial or industrial secret of regulated subjects. It should be noted that the similarity of these competences to those of the Accounting Courts is such that, in the past, several German states gave their regional data protection authorities the status of Regional Accounting Courts as an attempt to render them more independent [16, p. 425].

The problem related to the technical sufficiency of personal data protection authorities is far from being solved. In his analysis of the European scenario, Ido Sivan-Sevilla [25, p. 8] stresses that, although the GDPR establishes in Article 52 (4) that the member states must ensure that the entities have adequate human, technical and financial resources, the norm does not set guidelines for that sufficiency nor the paths to be covered. It is clear, however, that the staff robustness of DPAs must be not only quantitative but also qualitative, which has to be measured by the professional history and technical expertise of their members. In his view, high levels of expertise would enable an effective supervision of the regulated sectors and support the agencies' sanctioning actions [25, p. 8].

At any rate, since it is convenient for the ANPD to start developing in-house know-how, a possibility to be explored would be to structure a hybrid format in which the agency has public servants with IT training in its staff but does not dispense with instruments of institutional collaboration of this nature, thus remaining updated and in constant dialog with the most recent research conducted in the private sector and the academic sphere.

Thus, the entity must have strong state careers in the area of ICTs, capable of leading technological innovation processes within the agency's end activity and of articulating dynamic partnerships with civil society. Expecting that the Brazilian agency will overcome, in an isolated manner, the challenge that attracting these professionals represents today is not fruitful, so that openness to articulation with research institutions, for example—with due safeguarding of the strategic secrecy necessary for the performance the ANPD regulatory role—is alternative that should

be considered. In fact, what suggests itself is a process in which education becomes the necessary lever for the formation of staff, but short and medium-term alternatives have to be found in light of the risks and the urgency imposed by the demand.

7 Final remarks

Before completing two years of existence, the ANPD, in its provisional format, sought to adopt a dynamic and responsive management style, launching invitations for bids to look for resources in civil society that might be relevant to the data protection regulatory agenda in Brazil. Furthermore, it attempted to prospect federal public employees who may have a training compatible with the agency's duties. However, the studies analyzed here showed both the importance of having professionals with ICT expertise for an independent performance of the work of data protection authorities and a difficulty to attract them at the global level.

The challenge is also felt at other state levels in Brazil, such as at the Federal Accounting Court and the Accounting Court of the State of Pernambuco, whose strategies to overcome this hindrance may serve as parameters for future initiatives, contracts and agreements to be concluded by the ANPD in the field of technology, in parallel with the creation of state careers of its own in the area of ICTs. The period of planting has already begun, and now tasks of profound transformation are underway, which, if they follow the Constitution's parameters, will provide a harvest of trustworthiness and security in the national scenario. In this sense, it must be stressed that the primary task of the ANPD, as well as of all data protection authorities, is to act in a technical, ethical and legal manner for the production of an ecosystem aligned with the human and fundamental rights. This implies an independent positioning that will set limits to unlawful, negligent and harmful actions in the processing of personal data either by the public or the private sector, which refers above all to the exclusion of a shape of the Brazilian state as a monolithic unit, i.e., contrary to the informational separation of powers.

References

1. Autoridade Nacional de Proteção de Dados (2021) Edital de Oportunidades Autoridade Nacional de Proteção de Dados (ANPD) nº 02. https://www.gov.br/anpd/pt-br/canais_atendimento/Editalfinal.pdf (Created 26 Nov 2021). Accessed 12 July 2022
2. Barros A (2021) Internet chega a 88,1% dos estudantes, mas 4,1 milhões da rede pública não tinham acesso em 2019. https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/30522-internet-chega-a-88-1-dos-estudantes-mas-4-1-milhoes-da-rede-publica-nao-tinham-acesso-em-2019 (Created 14 Apr 2021). Accessed 30 June 2021
3. Barroso LR (2009) O direito constitucional e a efetividade de suas normas: limites e possibilidade da Constituição brasileira. Renovar, Rio de Janeiro
4. Ayres I, Braithwaite J (1992) Responsive regulation: transcending the deregulation debate. Oxford University Press, New York
5. Brasil (2018) Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Accessed 10 July 2021
6. Brasil (2022) Medida Próvisória n. 1.124, de 13 de junho de 2022. Altera a Lei nº 13.709, de 14 de agosto de 2018. https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Mpv/mpv1124.htm. Accessed 10 Aug 2022

7. Brasil (2022) Tribunal de Contas da União. Imprensa: TCU lança edital inédito para contratação por Encomenda Tecnológica (21/02). https://portal.tcu.gov.br/data/pages/8A81881E7DB4DC45017F1DC0EA7D42D5.htm (Created 18 Feb 2022). Accessed 28 Mar 2022
8. Brasscom (2021) Estudo da Brasscom aponta demanda de 797 mil profissionais de tecnologia até 2025. https://brasscom.org.br/estudo-da-brasscom-aponta-demanda-de-797-mil-profissionais-de-tecnologia-ate-2025/. Accessed 28 Mar 2022
9. Carloni G, Doneda D, Mendes LS O papel da ANPD conforme a nova LGPD. https://youtu.be/8HqYzOy9Iu4 (Created 23 Sept 2020). Accessed 20 July 2021
10. Coura K (2020) ANPD: Bolsonaro indica nomes para a diretoria da Autoridade de Dados. Waldemar Gonçalves Ortunho Junior foi indicado para ser o diretor-presidente do Conselho da ANPD. Confira os outros nomes. https://www.jota.info/jotinhas/anpd-bolsonaro-indica-nomes-para-a-diretoria-15102020 (Created 15 Aug 2020). Accessed 15 July 2021
11. Doneda D (2021) A Autoridade Nacional de Proteção de Dados e o Conselho Nacional de Proteção de Dados. In: Doneda D et al. (eds) Tratado de Proteção de Dados Pessoais. Forense, Rio de Janeiro, p. 459–469
12. Ennser-Jedenastik L (2016) The politicization of regulatory agencies: between partisan influence and formal independence. J Public Adm Res Theory 26(3):507–518 (https://doi.org/10.1093/jopart/muv022)
13. European Data Protection Board (2021) Overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Autorities. https://edpb.europa.eu/our-work-tools/our-documents/other/overview-resources-made-available-member-states-data-protection_en (Created 5 Aug 2021). Accessed 22 Aug 2021
14. European Data Protection Supervisor (2021) Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary. https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en (Created 23 Apr 2021). Accessed 23 May 2021
15. Freitas J (2019) Sustentabilidade: direito ao futuro, 4th edn. Fórum, Belo Horizonte
16. Gundermann L (2021) So many Data, so little time—Data Protection Authorities in Germany: status quo and challenges. In: ANPD e LGPD: desafios e perspectivas. Almedina, São Paulo, pp 419–432
17. Hoffmann-Riem W (2021) Teoria do direito digital: transformação digital: desafios para o direito. Forense, Rio de Janeiro
18. de Lima CRP (2020) A Autoridade Nacional de Proteção de Dados e a Efetividade da Lei Geral de Proteção de Dados: de Acordo com a Lei Geral de Proteção de Dados (Lei n. 13.709/2018 e as Alterações da Lei n. 13.853/2019), o Marco Civil da Internet (Lei n. 12.965/2014) e as Sugestões de Alteração do CDC (PL 3.514/2015). Almedina Brasil, São Paulo
19. Micklethwait J, Wooldridge A (2015) A Quarta Revolução e a corrida global para reinventar o Estado. Portfolio Penguin, São Paulo
20. Nova (2020) Nova falha do Ministério da Saúde expõe dados de 243 milhões de brasileiros na internet, diz jornal. https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml (Created 2 Dec 2020). Accessed 10 July 2021
21. OCDE (2020) Revisões da OCDE sobre a transformação digital: a caminho da era digital no Brasil. https://www.oecd-ilibrary.org/docserver/9a112bbe-pt.pdf?expires=1621814810&id=id&accname=ocid54025470&checksum=12966397DECD92399B1AC6C52D8EF99A. Accessed 11 July 2021
22. Presidência da República (2022) Decreto n. 10.975 de 22 de fevereiro de 2022. http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D10975.htm. Accessed 12 July 2022
23. Raab C, Szekely I (2017) Data protection authorities and information technology. Comput Law Secur Rev 3(4):421–433 (https://www.sciencedirect.com/science/article/pii/S0267364917301619)
24. Rodriguez DP (2021) O Direito Fundamental à proteção de dados: vigilância, privacidade e regulação. Lumen Juris, Rio de Janeiro
25. Sevilla-Sivan I (2022) Data Protection Gatekeepets post-GDPR: A fuzzy-set qualitative comparative analysis (fsQCA) across data protection authorities. https://osf.io/preprints/socarxiv/kjf8q/. Accessed 1 Apr 2022 (Journal of European Public Policy (under review—second round))
26. Simão B, Oms J, Torres L (2019) Autoridades de proteção de dados na América Latina: um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai. IDEC, São Paulo (https://idec.org.br/publicacao/autoridade-de-protecao-de-dados-na-america-latina)
27. Sistemas (2021) Sistemas do TJ-RS continuam fora do ar após ataque hacker. https://www.conjur.com.br/2021-mai-04/sistemas-tj-rs-continuam-fora-ar-ataque-hacker (Created 4 May 2021). Accessed 30 June 2021

28. Sjoera (2021) New EU Code of Conduct for cloud providers: not a GDPR party. https://www.privacycompany.eu/blogpost-en/new-eucode-of-conduct-for-cloud-providers-not-a-gdpr-party (Created 6 Feb 2021). Accessed 11 July 2021
29. Sombra TLS (2019) Fundamentos da regulação da privacidade e proteção de dados pessoais: pluralismo jurídico e transparências em perspectiva. Thomson Reuters Brasil, São Paulo
30. Teubner G (1996) Global Bukowina: legal pluralism in the world-society. In: Teubner G (ed) Global Law Without a State. Dartsmouth, p. 2–28. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=896478. Accessed 20 Jul 2021
31. Valente F (2020) STJ diz ter backup e garante retomada; advogados consideram que episódio é grave. https://www.conjur.com.br/2020-nov-06/stj-backup-advogados-consideram-episodio-grave (Created 6 Nov 2020). Accessed 30 June 2021
32. Vazamento (2020) Vazamento de senhas do Ministério da Saúde expõe informações de pacientes de Covid-19. https://g1.globo.com/bemestar/coronavirus/noticia/2020/11/26/vazamento-de-senhas-do-ministerio-da-saude-expoe-informacoes-de-pessoas-que-fizeram-testes-de-covid-19-diz-jornal.ghtml (Created 26 Nov 2020). Accessed 10 July 2021
33. Viola M (2019) Transferência de dados entre Europa e Brasil: análise da adequação da legislação brasileira. https://itsrio.org/wp-content/uploads/2019/12/Relatorio_UK_Azul_INTERACTIVE_Justificado.pdf. Accessed 20 Sept 2020
34. Wimmer M (2021) Poder entrevista: Miriam Wimmer, diretora da ANPD. https://www.youtube.com/watch?v=jTTTT76RUPs&t=665s (Created 6 Aug 2021). Accessed 28 Mar 2022
35. Wimmer M (2021) Os desafios do enforcement na LGP: fiscalização, aplicação de sanções administrativas e coordenação intergovernamental. In: Doneda, Danilo et al. (Org). Tratado de proteção de dados pessoais. Forense, Rio de Janeiro, pp 375–387
36. Zanatta R, Santos B, Cunha B, Saliba P, Goulart de Andrade E (2020) Perfil das Autoridades de Proteção de Dados Pessoais: civis ou militares? Associação Data Privacy Brasil de Pesquisa, São Paulo