Responsive regulation in the enforcement framework of the Brazilian DPA (ANPD) within a data security breach proceeding

Sayuri Pacheco Hamaoka
Bachelor of Law at the University of Brasília
sayuriphamaoka@gmail.com

BioGraphY

Postgraduate student in Digital Law and Data Protection at PUCRS. Bachelor of Law at UnB (Brazil), with a study exchange period at USAL (Spain). Currently working at the Brazilian National Data Protection Authority (ANPD), focused on the fields of data protection and regulation. Ex-member of the group of studies “Observatório da LGPD” (UnB), purposed to encourage data protection discussions.

Abstract

The Brazilian National Data Protection Authority’s direction towards the adoption of a regulatory design based on Responsive Regulation allows a better dialogue flow between regulator and regulated. Therefore, the present study aims to understand the relationship between Responsive Regulation principles and the application of the ANPD's competencies, especially in a case initiated as a security incident communication proceeding and concluded as a sanctioning proceeding. It was observed a responsive alignment in the Authority's approach, as noted: in the responsive principles contained in the Supervision and Sanctioning Proceedings Regulation, approved by the Resolution CD/ANPD n. 1/2021, and in the application of responsive principles during the proceeding, despite the potential for improvement from a responsive perspective to achieve more collaborative results.

Keywords

National Data Protection Authority. Responsive Regulation. Supervision and Sanctioning Proceedings Regulation. Security incident communication. Digital services.

structured ABSTRACT

[Purpose] The purpose of this study is to identify characteristics of Responsive Regulation in the Supervision and Sanctioning Proceedings Regulation of the Brazilian National Data Protection Authority (ANPD), as well as its role within the incident response process at SES/SC, serving as a "prototype" for cases involving data breaches of entities that provide digital services.

[Methodology/approach/design] The methodology applied is based on conducting a literature review on Responsive Regulation Theory and identifying its characteristics i) in the Supervision and Sanctioning Proceedings Regulation and ii) in a security incident communication proceeding that progressed into an administrative sanctioning proceeding.

[Findings] It was concluded that both the ANPD's Supervision and Sanctioning Proceedings Regulation, as well as its actions throughout the administrative proceedings against SES/SC, exhibited various responsive characteristics. However, it has also identified premises that can be improved by ANPD to ensure proper adherence to Responsive Regulation Theory in their regulations and actions in cases of data breach.

[Practical implications] Some practical implications for the ANPD's actions are related to i) the perspective of improving the Authority's supervision and sanction rules, with the addition of responsive principle articles, as well as ii) the possibility of the ANPD to introduce more responsive alternatives, grounded on the base of the enforcement pyramid from Responsive Regulation Theory. Additionally, it should be noted that ANPD's activities can have socio-economic impacts such as regulatory gaps regarding non-automatically applicable matters, which can cause legal uncertainty for those regulated and data subjects.

[Originality/value] The originality of this work can be seen in the scarcity of discussions on the concrete use of enforcement tools available to the ANPD in the light of Responsive Regulation, especially in cases of security incident communications that have progressed to sanctioning proceedings, given the recent publication of such cases through active transparency from the Authority. In addition to the academic community gaining further empirical evidence of responsive regulation, which is renewed with each practical application carried out, the Authority itself can draw on the reflections presented here to improve how it conducts its relationship with the regulated.

INTRODUCTION

The regulation of digital service provision within the public sector has been the subject of various normative initiatives in Brazil[1][2], both at the state and federal levels, due to the increasing role of technology and the use of personal data in the implementation of such projects. Considering this scenario, in the context of regulating the protection of personal data, the Brazilian National Data Protection Authority (ANPD) becomes one of the central axes as a watchdog and promoter of the input that nourishes the service provision: personal data.

To this end, responsive regulation is a conceivable theory for dealing with the dynamics and challenges of personal data regulation and the need to involve all the actors in the regulated environment to understand the importance of protecting this asset.

In this sense, the very dynamics of the Brazilian General Data Protection Law (LGPD) call for a responsive design, with measures that involve i) engagement of a regulatory authority; ii) self-regulation by data processing agents[3] (controllers and processors); and iii) participation from civil society both a) relating to those being regulated (exercising their rights against controllers, as mainly provided in Article 18 of LGPD), and b) collaborating with the regulator (exercising their rights to social participation in public consultations and hearings).

The Authority plays an essential role in promoting a *culture of data protection* towards data processing agents and data subjects, especially when communication between them both is impossible or unattainable, opportunity in which the DPA can promote dialogues with the regulated parties to understand the processing agent's reality and the need for intervention.

In accordance with this, the controller must be accountable to the Authority to demonstrate compliance with personal data protection rules. In particular, one of the duties to which they must pay attention when providing digital services is to notify both the Authority and the data subject of the occurrence of a security incident[4] that may entail a relevant risk or damage to data subjects, under the terms of Art. 48 of LGPD.

As one of the ANPD's Directors, Miriam Wimmer, has already explained, a security incident is an event to which everyone is susceptible; it is not a matter of "if" but "when" it will happen[5]. This is precisely why processing agents must adopt a proactive posture to mitigate the occurrence of such adverse events, enabling to both combat and report them, when necessary, to data subjects and ANPD.

From a regulatory perspective, gradual regulatory techniques in line with the enforcement pyramid proposed by John Braithwaite and Ian Ayres are also reflected in the Supervision and Sanctioning Proceedings Regulation (henceforth "Supervisory Regulation"), with the provision, for example, of the ANPD's monitoring, guidance, prevention and repression activities. In the case of a security incident, used as an example in this paper, it is up to the Authority to adapt the regulatory instruments placed

[1] In this regard: Law n. 10.129/2021 - Addresses principles, rules, and instruments for Digital Government to increase public efficiency;
Decree n. 10.609/2021 - Establishes the State Modernization Policy and the National State Modernization Forum; Decree n. 12.069/2024 - Establishes the Digital Government Strategy (2024 to 2027); Decree n. 10.046/2019 - Addresses governance in data sharing within the federal public administration and establishes the Citizen Base Register and the Central Data Governance Committee.

[2] The name and content of Brazilian legislations, regulations, decrees, ordinances, and any kind of national norms written in this article were freely translated by the author.

[3] In Brazil, when referring to both controller and processor, they are called "processing agents", as stipulated by Article 5, IX, of LGPD.

[4] For the purposes of this paper, it is assumed that every "security incident" and "security breach" mentioned is related to a personal data breach.

[5] Presentation by the Director of ANPD Miriam Wimmer, in 12/04/2023. Available on: <https://www.camara.leg.br/evento-legislativo/67461?a=560242&t=1681308484647&trechosOrador=> 2min. Accessed on 23 June 2024.

at its disposal to the extent of the relevance of the data security incident and the cooperation of the regulated party in the face of the ANPD's determinations.

Aligned with this sense of choosing the right regulatory techniques for each case, the Responsive Inaugural Article proposed by Márcio Aranha (2023) stands out, in parallel to the principle premises of Article 17 of the ANPD Supervisory Regulation. This arises due the fact that both Articles explain the need to use measures and actions that are proportional to the risks, evidence, behaviours of the regulated parties, etc., as well as prioritizing action based on these elements, with a focus on results.

DIGITAL SERVICES IN THE PUBLIC SECTOR

The processing of data by public authorities to provide digital services has been increasingly promoted by the government and sought after by citizens. In this sense, making government services available on digital platforms offers easier access to information and its monitoring in a constantly digitalizing society, as well as enabling “collaborations with and between societal stakeholders” (OECD, p. 1, 2018).

One of the digital services that can be carried out - and which was presented in the proceeding that will be mentioned in this paper - is the monitoring of waiting lists of patients who "are waiting for appointments (categorized by specialty), exams and surgical interventions and other procedures in the establishments of the public health network of the State of Santa Catarina", under the terms of State Law n. 17.066/2017 (also regulated by State Decree n. 1.168/2017).

The initiative strengthens the implementation of more transparent and efficient public policies, as well as allowing the data subject to easily monitor the progress of service provision.

It is in this same vein that, at the federal level, Brazil has published the Federal Law n. 13.460/2017, which emphasizes the right of public service users to receive adequate service provision, having as a guideline the "application of technological solutions aimed at simplifying user service processes and procedures and providing better conditions for sharing information"[6], as well as the "adoption of measures aimed at protecting the health and security of users"[7]. In addition, Federal Law n. 13.460/2017 also provides that public services and user assistance must comply with the principle of security.

In this context, the expansion of the state's database in pursuit of the development of democracy, with the inclusion of citizens in public policies, has given impetus to the debate on data protection in the public sector, given the duality of surveillance and social participation/concretization of citizenship (Wimmer, 2023).

In the case to be analysed in this paper, it will be seen that the pursuit to materialize the offer of a public digital service failed to guarantee the protection of the personal data of citizens using the service, caused by a security incident.

Given the facts and circumstances of the case, it was up to the Authority, after the regulated party notified the incident, to investigate the case, applying the principles of responsive regulation in its actions.

Brazilian National Data Protection Authority (ANPD)

Establishment and relevance

The Brazilian DPA was initially established by the Provisional Measure n. 869/2018, later converted into Law n. 13.853/2019, framed within the legal nature of a federal public administrative body under the Presidency of the Republic. In June 2022, it was transformed into a special autonomous body (special autarchy) by Provisional Measure n. 1.124/2022, which was converted into Law n. 14.460/2022 in October 2022, and is currently attached to the Ministry of Justice and Public Security, as determined by Decree n. 11.401/2023.

The ANPD is essential for ensuring data protection and informational self-determination for individuals on both subjective and objective levels. From a subjective dimension, this entails a negative freedom against [both] public [and private] entities, demanding justification for any interference in this fundamental right; from an objective perspective, this right requires an obligation from the state to protect it, guaranteeing its exercise and fulfilment (Mendes; Rodrigues Jr.; Fonseca, 2023).

To effectively achieve data protection objectives, the ANPD possesses preventive, regulatory, supervisory, and sanctioning competencies. The Authority has a crucial role as the main entity responsible for enforcing data protection legislation and serving as a point of intersection between data controllers and data subjects. The authority's significance also stems from its expertise in handling specialized technical matters related to data protection. Delegating these responsibilities to other entities would result in legal uncertainty and inefficiency (Doneda, 2020).

[6] Author's translation.
[7] Author's translation.

Furthermore, the ANPD is mandated to oversee not only private entities but also public bodies, as the LGPD applies to both. Therefore, the ANPD must maintain equidistant positions that balances the interests of regulated entities, beneficiaries of regulation, and political power; positions whose best way to achieve is through institutional autonomy.

Hence the importance of strengthening the Authority for the effective application, interpretation and vigilance of the law in an independent manner, which is widely supported at an international level, both by European Union countries and international organizations (Gutierrez, 2020).

The Organization for Economic Co-operation and Development (OECD), for instance, made a few recommendations in 2020 for Brazil to adapt to the organization's expectations regarding increasing trust in the digital environment, including ensuring the independence of the ANPD, which at the time was not yet a special autarchy. This perspective was also emphasized in 2021 by the Organization of American States (OAS), which advised member states, in the document "Updated Principles on Privacy and Personal Data Protection", to guarantee the existence of independent supervisory bodies, with sufficient resources, as a principle for strengthening the matter at the inter-American level.

In this perspective of the Authority's international projection, the promotion of networked governance between regulators from different countries forms a transgovernmental order, which makes the mode of international governance more effective (Slaughter, 1997). Alongside this, the domestic economy has also been strengthened by the creation of the LGPD and the ANPD (Lima, 2020), as it encourages the domestic market to be recognized and to interact with the foreign market.

Bearing in mind that the complexity of social relations and the organization of the state require entities capable of ensuring dynamism and objectivity for the promotion of citizens' rights, as well as bringing the spheres of the market and the public sector closer to the citizens (Doneda, 2020), the significance of the Brazilian National Data Protection Authority becomes evident.

Competencies

The ANPD's competencies are set out mainly in Article 55-J, of the LGPD but are also dispersed in other Articles of the LGPD (e.g. Art. 5, XIX; Art. 19, §3; Art. 46; among others); in various Articles of Decree n. 10.474/2020; as well as in Ordinance n. 1/2021, which provides for the ANPD's Internal Regulations (IR). Its powers can be divided into four main areas: preventive, regulatory, supervisory, and sanctioning.

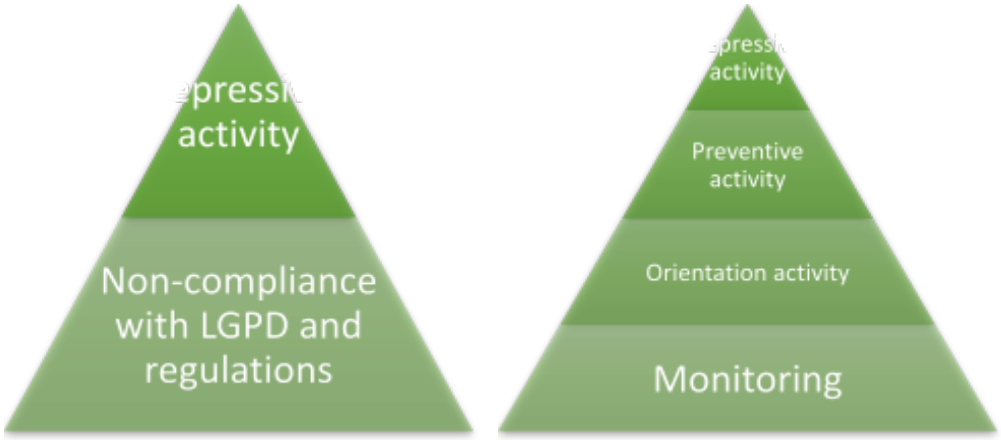
Preventive

Firstly, it is up to the ANPD to take preventive measures, which can also be seen as education and dissemination of data protection, including those contained in Art. 55-J of the LGPD.

Article 2 of the Supervisory Regulation states that "supervision includes monitoring, guidance and preventive action", being the preventive competence also included in supervisory competence. This demonstrates a hierarchical approach to interventions when compared to the regulatory pyramid models proposed by Ayres and Braithwaite (1992) in the Responsive Regulation Theory. The figures below demonstrate a comparison between the command-and-control pyramid and the responsive pyramid of supervisory and sanction measures by ANPD.

Figure 1. Command-and-control approach

Figure 2. Responsive supervisory approach



Source: Regulatory impact assessment (AIR) from the Supervisory Regulation – ANPD (author's translation)

Regulatory

Secondly, it is worth highlighting the ANPD's competence to issue "regulations and procedures on the protection of personal data and privacy", according to Art. 55-J, XIII, of the LGPD, a competence that encompasses a wide spectrum of functions to guarantee the protection of data subjects and to establish guidelines for processing agents.

In line with the objective of standardization by the National Authority when it issues rules on data protection, it also has a terminating role in interpreting the LGPD[8]. Then, it is the competent body to maintain standards for the application of the law (Doneda, 2020) and standardize understandings, with the aim of guaranteeing greater legal certainty for all those who are subject to the legislation.

Its consequence is that it is essential for the Authority to regulate the various parameters of the law, which, on the other hand, does not dispense the involvement of the regulated actors and other stakeholders who are affected by such normative impositions, in line with the notion of nodes of governance between public and private power being connected in a network, so that neither can dominate the other (Braithwaite, 2006).

In addition, the ANPD has drawn up strategic plans to guide it in prioritizing the activities to be carried out, with references to objectives, indicators and calculation formulas. This initiative demonstrates a commendable detachment from a totally discretionary performance from the regulator; however, it is necessary to reflect on a continuous prioritization on the part of the Authority, as will be shown below, particularly since the expectation is that the sectors prioritized in the inspection plans will affect the decision to choose the regulated agents to be inspected.

Supervisory

Thirdly, the Authority's supervisory competences are far-reaching. Among the actions, it must be highlighted those provided for in Art. 55-J of the LGPD: to ensure the protection of personal data; to ensure compliance with commercial and industrial secrets; to supervise; to request specific information from the public authorities on the respective data processing operations; to carry out audits or order them to be carried out; and to ensure that the processing of elderly people's data is carried out in a way that is simple, clear, accessible and suitable for their understanding.

Furthermore, Article 17 of the Internal Regulations (RI) of ANPD has also delegated various competencies in LGPD to the General Supervisory Coordination (CGF). These include responsibilities related to supervision, such as: proposing preventive measures[9]; receiving notifications regarding security incidents; requesting data processing agents to submit Personal Data Protection Impact Assessment (RIPD); conducting inquiries and gathering relevant evidence in administrative proceedings; promoting educational initiatives in coordination with the General Coordination of Standardization; receiving and considering petitions from data subjects submitted to ANPD against controllers, as established by regulations.

[8] LGPD. Art. 55-K. (...) Sole Paragraph. The ANPD will coordinate its work with other bodies and entities with sanctioning and regulatory powers related to the issue of personal data protection and will be the central body for interpreting this Law and establishing standards and guidelines for its implementation. (Included by Law n. 13.853/2019) (author's translation).

[9] According to Art. 17, V and Art. 55 of the Internal Regulations (RI) of ANPD, these preventive measures can be proposed by both the General Supervisory Coordination (CGF) and the Directors of the Board of Directors (CD).

Sanctioning

Lastly, and the one that should be listed as the last resort for trying to get compliance from a regulated party, is the ANPD's sanctioning competencies. This attribution is provided for in Art. 55-J of the LGPD, as well as in the Supervisory Regulation and in the Regulation of Dosimetry and Application of Administrative Sanctions, approved by the Resolution CD/ANPD n. 4/2023.

Its function is, objectively, to apply sanctions in the event of non-compliance with the law, ensuring the principles of adversarial proceedings, full defence, and the right to appeal. However, it is also worth mentioning that there are other ways to avoid or mitigate the sanction itself, such as signing a Conduct Adjustment Agreement (TAC)[10] - even though it's not in practice yet - and implementing a policy of good practices and governance.

According to Art. 37 of Supervisory Regulation, the repressive process, which includes the administrative sanctioning process, can be initiated i) ex officio by the General Supervisory Coordination; ii) as a result of the monitoring process; or iii) in the event of a request in which the General Supervisory Coordination, after carrying out an admissibility analysis, decides to immediately open a sanctioning process, which allows for a wide possibility of opening sanctioning processes, based on premises of evidence, risk, proportionality, planning, among others, provided by the Supervisory Regulation.

INTRODUCTION TO RESPONSIVE REGULATION THEORY

The legal theory of Responsive Regulation has as its core the proposition of alternatives between regulation and deregulation, the stimulation of a policy that combines public and private regulation in a creative way and the creation of incentives for compliance with the law (Ayres and Braithwaite, 1992; Aranha, 2023).

To build the regulator-regulated relationship, Ayres and Braithwaite (1992) argue that the way forward is through dialog and cooperation. Through them, the regulator understands the regulated party to persuade them to return to compliance, to help them improve, and to discover perspectives that are inaccessible without cooperation and dialog.

It is argued that dialog is always the first step in resolving an issue, no matter how serious it is (Braithwaite, 2006); while cooperation is conceived as the ideal approach to be adopted by the parties to achieve mutually beneficial returns (Ayres and Braithwaite, 1992). Both elements serve as a background to the construction of the responsive assumptions that will be discussed below.

Regulatory Pyramids – Escalation of Interventions

The pyramids elaborated by Ayres and Braithwaite (1992), expanded by various other authors, are the best-known representations of the theory. The ones portrayed here give rise to an escalation of government interventions and support, with the central focus being on strengthening the cooperative moment between the regulated and the regulator (Aranha, 2023).

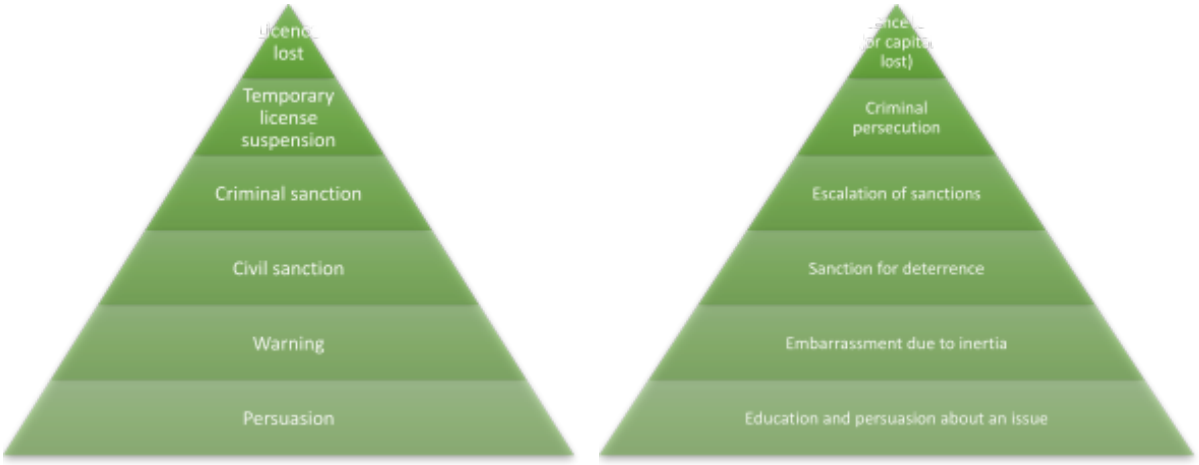
For those who are familiar with a command-and-control model, sanctions are the instrument that is expected to be used. For responsive regulation, however, the focus of regulation is not sanctions, even though their existence is necessary. It is from this perspective that the regulator must demonstrate that punishments can be escalated and will be used if necessary.

The regulatory pyramid of constraint (enforcement pyramid) is the pyramid that portrays the gradation of regulatory strategies to be scaled from the bottom, with persuasive and educational measures; to the top, with dissuasive measures. Along the same lines as the enforcement pyramid, John Braithwaite, Makkai and Valerie Braithwaite (2007) proposed the pyramid of sanctions - adapted by Braithwaite in 2011 - which resulted in the same number of levels and almost the same interventions as the first (the enforcement pyramid):

Figure 3: Enforcement pyramid proposed in Responsive Regulation: Transcending the Deregulation Debate, by Ayres and Braithwaite (1992, p. 35) (adapted)

Figure 4: Pyramid of sanctions proposed in Essence of Responsive Regulation, Braithwaite (2011, p. 482) (adapted)

[10]Supervisory Regulation. Art. 43 - The interested party may submit a proposal to the General Inspection Coordination to enter into a conduct adjustment agreement.



Starting from the ground level, persuasive measures involve soft tools, such as guidelines, protocols and educational strategies, which can be generically summarized as dialogue and persuasion (Drahos, 2004). In this way, persuasion refers to negotiation and the shift from the uncompromising application of punishments to valuing the cooperative behaviour of the regulated agent (Aranha, 2023).

Therefore, it should be assumed that intervention always starts at the lowest level of the pyramid - the most restorative approach, based on dialog - reluctantly escalating to punitive approaches, and only when dialog fails (Braithwaite, 2002, 2006, 2011).

Thus, the pyramid must be built up with a hierarchy of sanctions and regulatory strategies of varying degrees of interventionism (Aranha, 2023). The background to this escalation is the attempt to offer a range of possibilities to make cooperation more attractive, so that a regulator with more than one deterrence option can act against the regulated party on different scales, depending on the level of severity and collaboration (Ayres and Braithwaite, 1992).

It should also be mentioned that the aforementioned pyramidal structures were presented by the authors as examples of the shape of regulatory pyramids, not with the aim of replicating them indiscriminately, since data from practical experiences of responsive regulation show that the regulated sectors call for different types of sanctions (Ayres and Braithwaite, 1992).

As an illustrative example, pecuniary sanctions provided for in the LGPD are not applicable to public authorities, due to the interpretation of the law's omission in this regard, according to Art. 52, §3º, of the LGPD.

It should be noted that the theory is not restricted to the mere construction of regulatory pyramids but involves a whole repertoire of relationships between the regulator, the regulated and third parties. Among these, this study will highlight the heuristics of i) consideration of the context; ii) active listening and dialogue; and iii) resistance from the regulated as an opportunity to improve the regulatory system, presented by Braithwaite in "The Essence of Responsive Regulation" (2011), which summarize various guidelines to be followed by those applying Responsive Regulation, be they regulators, companies or NGOs.

Considering the context when acting on each case

This premise presents the idea that regulators should pay attention to the context and historical period in which they are situated (Braithwaite, 2011). Considering the regulated environment is relevant to understanding that not all measures should be applied at the same time, in the same way, in the same place and with the same justification.

In other words, the regulator, in charge of state regulation, must be sensitive to the behavioural profile of the regulated. Also, it must be understood that not all actions should be adopted equally for everyone, as companies have different designs, different personalities, and different punishments (Braithwaite, 1985).

Additionally, responsiveness must also project itself onto changing regulatory environments and therefore be sensitive to the context of the regulated (Braithwaite, 2014). With this in mind, “the response that issues is therefore flexible, multidimensional, and layered into trying one strategy after another” (Braithwaite, p. 22, 2014). The responsive regulator's approach, therefore, is based on mistakes and successes, depending on the regulatory situation (NDSR, 2021), without universal solutions, but paying attention to the recommendations of responsive theory.

This is why the regulator is expected to come up with innovative responses that mirror the dynamics of the regulated party's attitude, motivation, behaviour, and structure. Because of this non-absolute approach, it is essential that the state demonstrates its intention to comply with the regulatory design model it communicates to society (Aranha, 2023).

Active listening and establishing a dialog with the regulated

Listening is an essential element for promoting change and for understanding the regulated sector and the regulatory environment to which the regulated must be responsive (Braithwaite, 2011).

The regulator's dialogue should be structured in such a way as to give a voice to stakeholders; establish agreed outcomes and how to monitor them; build commitment to helping actors find their own motivation to improve; and communicate a firm determination to persist in solving the problem until it is resolved.

The cooperation of the regulated with the regulator also leads to an increase in the identification of hidden irregularities and therefore early warnings of more serious structural problems (Braithwaite, 2011).

Listening and dialog must be receptive to the numerous attempts at different approaches. The ideal posture of the responsive regulator is to be an active listener, who also dialogues. Dialogue emphasizes that the regulator and the regulated will persist in confronting a problem, escalating through increasingly interventionist strategies, until the adversity is no longer qualifies as such.

It is also important for regulation to be collaborative, in which the regulator and the regulated work together and agree on desired outcomes, self-monitoring and/or external monitoring of progress (Braithwaite, 2011). The regulator must also be guided by the regulated party's values, motivations, skills, resources and statements to strengthen the regulated party's motivation for change.

Besides, the regulated party must express its arguments and plans in favour of change, deciding what is necessary, when and how to proceed, while the regulator must strengthen the debate, deal with resistance from the regulated party and offer cautious advice when requested by the regulated party. These steps are also applicable in the field of data protection, where problem-solving must be based on dialogued and agreed solutions (Wimmer and Pieranti, 2021).

It can be concluded that the responsive regulator is capable of observe, through listening, the commitment to achieving results based on the motivations chosen by those being regulated.

Resistance from the regulated as an opportunity to improve

Resistance from the regulated should be seen as a good thing in a regulatory regime, as it creates the opportunity to improve. Adaptation through the ability to deal with resistance is also emphasized to achieve a quality and resilient regulatory system.

It should be noted that regulated parties who do not get involved in the regulatory dynamic are more difficult to deal with than those who persist in the game to resist the regulator (Braithwaite, 2011). This is why it is necessary to focus on the regulated party's strengths in order to expand them by means of an ascent of rewards/supports - which goes, for example, through education and persuasion about a strength, to informal praise, prizes or subsidies, all the way to the top, by means of an academic award.

Responsive regulation as the guiding principle for ANPD's actions

Principles' Article for a Responsive Design in the National Data Protection Authority (ANPD)

Responsive regulation can be found in some aspects of the LGPD, primarily focusing on self-regulation, co-regulation and accountability. Some notable mechanisms include negotiation processes and consultations, as the opportunity regulated entities have to develop best practices and governance frameworks, which can be used as criteria for assessing compliance levels, also with the possibility of recognition and disclosure by ANPD (Wimmer, 2023b). However, although compatible, the mentioned law lacks principles that determine a responsive framework's construction; this responsibility is instead delegated to the Supervisory Regulation as further discussed below.

According to Márcio Aranha (2023), the responsive model presupposes premises or guidelines that guide the regulator's posture and the strategies to be implemented. In this way, the author suggests the adoption of a principle-based Article that allows the rules of regulated sectors to be adapted to a responsive approach and its derivations (intelligent regulation, governance nodes, risk-based or results-based regulation, among others):

DRAFT OF AN INAUGURAL PRINCIPLE ARTICLE OF A RESPONSIVE DESIGN[11]

Art...The regulation of ... shall observe the following premises:
I - adoption, alone or jointly, of regulatory strategies proportionate:
a) to the Administered Party's behavioral profile of compliance, coordination and cooperation;
b) to the results;
c) to continuous monitoring; or
d) to the systemic or individual risks inherent to the activity, decision-making processes, business management and the economic condition of the regulated parties.
II - respect for the instrumentality of forms and encouragement of continuous improvement in the provision of services about…;
III - functional autonomy between follow-up, monitoring, convincing, management, cooperation, prevention, repair and control measures;
IV - valuing planning for the prioritization, selection, frequency, timing, duration and intensity of supervisions;
V - use of regulatory action instruments that are consistent with the minimum degree of intervention required;
VI - ensuring that information voluntarily shared with the regulator by regulated parties is used exclusively to inform planning, convincing, prevention, cooperation, and voluntary redress measures.

Regarding ANPD regulation and responsive principles, the Supervisory Regulation sets out "supervisory premises" (Art. 17)[12], which are intended to guide the ANPD's actions. In view of the above-mentioned inaugural article proposed by Aranha (2023), it will be exposed a comparative analysis between the principles presented by the ANPD and those proposed by Aranha (2023), to better understand these responsive principles in the Authority's inspection rule:

Table 1. Comparison between the Inaugural Principle Article proposed by Márcio Aranha and the principles of the Article 17 of the ANPD' Supervisory Regulation

Draft of the Inaugural Principle Article of a Responsive Design	**Article 17 of the ANPD' Supervisory Regulation – Subsections that resemble the central ideas of the Inaugural Principle Article**
Art...The regulation of ... shall observe the following premises:	Art. 17: The ANPD's supervisory process will observe the following premises:
I - adoption, alone or jointly, of regulatory strategies proportionate: a) to the Administered Party's behavioral profile of compliance, coordination and cooperation;	IV - act in a responsive manner, adopting measures proportional to the risk identified and the stance of the regulated agents;
I - adoption, alone or jointly, of regulatory strategies proportionate:	II - prioritization of action based on evidence and regulatory risks, with a focus and orientation towards results;

[11]The translation of this draft article was carried out by the author of the present paper.
[12]Supervisory Resolution. Art. 17: The ANPD's supervisory process will observe the following premises:
I - alignment with strategic planning, with the instruments for monitoring data processing activities and with the National Policy for the Protection of Personal Data and Privacy;
II - prioritization of action based on evidence and regulatory risks, with a focus and orientation towards results;
III - integrated and coordinated action with public administration bodies and entities;
IV - act in a responsive manner, adopting measures proportional to the risk identified and the stance of the regulated agents;
V - encouragement to promote a culture of personal data protection;
VI - provision for transparency, input/output loop and self-regulation mechanisms;
VII - encouragement of responsibility and accountability by processing agents;
VIII - encouragement of direct conciliation between the parties and prioritization of the resolution of the problem and reparation of damages by the controller, observing the principles and rights of the data subject provided for in the LGPD;
IX - requirement of minimal intervention in imposing administrative conditions on the processing of personal data; and
X - carry out the supervisory activities that best suit the ANPD's competencies. (Author's translation)

b) to the results;	
I - adoption, alone or jointly, of regulatory strategies proportionate: c) to continuous monitoring; or	I - alignment with strategic planning, with the instruments for monitoring data processing activities and with the National Policy for the Protection of Personal Data and Privacy;
I - adoption, alone or jointly, of regulatory strategies proportionate: d) to the systemic or individual risks inherent to the activity, decision-making processes, business management and the economic condition of the regulated parties.	II - prioritization of action based on evidence and regulatory risks, with a focus and orientation towards results; IV - act in a responsive manner, adopting measures proportional to the risk identified and the stance of the regulated agents;
II - respect for the instrumentality of forms and encouragement of continuous improvement in the provision of services about…;	
III - functional autonomy between follow-up, monitoring, convincing, management, cooperation, prevention, repair and control measures;	
IV - valuing planning for the prioritization, selection, frequency, timing, duration and intensity of supervisions;	I - alignment with strategic planning, with the instruments for monitoring data processing activities and with the National Policy for the Protection of Personal Data and Privacy; II - prioritization of action based on evidence and regulatory risks, with a focus and orientation towards results;
V - use of regulatory action instruments that are consistent with the minimum degree of intervention required;	IX - requirement of minimal intervention in imposing administrative conditions on the processing of personal data; and (in the same direction, Art. 5 of the same Resolution: Art. 5. Regulated agents are subject to supervision by the ANPD and have the following duties, among others: (...) § Paragraph 1. The documents, data and information requested, received, obtained and accessed by the ANPD under the terms of these Regulations are those necessary for the effective exercise of its attributions, as well as those subject to the rules of access and classification of secrecy provided for in specific regulations).
VI - ensuring that information voluntarily shared with the regulator by regulated parties is used exclusively to inform planning, convincing, prevention, cooperation, and voluntary redress measures.	

Source: Elaborated by the author

From the table, it can be observed that the ANPD presents various perspectives of the article proposed by Aranha (2023), particularly the premises of the Supervisory Resolution which depict an idea of collaboration with external and regulated agents, as well as encouragement for conciliation between parties. These initiatives aim to prevent an accumulation of functions already assigned to ANPD.

On the other hand, some inaugural principles are not mentioned in the ANPD's Supervisory Resolution, namely: i) item II, regarding the instrumentality of forms and the continuous improvement of service provision; ii) item III, regarding the functional autonomy between follow-up, monitoring, convincing, management, cooperation, prevention, reparation and control measures; and iii) item VI, which provides for restrictions on the use of information voluntarily shared with the regulator by the regulated party.

It is also worth mentioning that, although the premise of encouraging the promotion of a culture of personal data protection "fits" in some way with the principle of encouraging continuous improvement in the provision of (inspection) services, a principle specifically indicating the improvement of the provision of the inspection service would be necessary, to encourage, for example, the constant improvement of communication channels between the regulator, the regulated party and interested third parties or services for monitoring citizens in relation to inspection processes. Although there are several responsive principles in the Resolution, it will be seen that some of them are not in total harmony with what is applied in practice.

In this context, ANPD has chosen Responsive Regulation as the best way to carry out its supervisory function, which is also seen in various statements by the Authority's Directors and Coordinators, as well as in official documents[13].

Supervision and Sanctioning Proceedings Regulation in the light of Responsive Regulation

The Supervisory Regulation of the ANPD aims to "establish the procedures inherent to the supervision proceeding and the rules to be observed within the scope of the administrative sanctioning proceeding" by the ANPD. It is therefore essential to understand how these provisions relate to the premises of responsive regulation.

From the analysis of the documents made public by the ANPD, the Regulatory Impact Assessment Report on what would become the Supervisory Regulation, published in May 2021, clarifies that meetings were held with the Anatel, Aneel and Antaq agencies, in which the negative sides of a command-control adoption were highlighted, whose centrality of action would be in the application of sanctions.

Thus, the model of responsive regulation was considered the most appropriate for the Authority, with emphasis on the points: i) "inducing behaviour without necessarily using punishments", ii) "adopting positive and negative incentives" iii) "gradation between transgressions of the legislation and their treatment according to their seriousness" and iv) establishing concurrent responsibilities of the ANPD and the regulated, "in the creation of a normative system of compliance in relation to the protection of personal data, based on a less interventionist approach on the part of the ANPD" (BRASIL, p. 22, 2021).

In Supervisory Regulation, there are other provisions that correlate with responsive characteristics (Frazão, Carvalho and Milanez, 2022), including expressly mentioning that the activities to be adopted are "the object of responsive action", which are: i) monitoring, ii) guidance, iii) preventive activity and iv) repressive activity. According to Article 15 of the Regulation:

i) monitoring is aimed at "gathering relevant information and data to support decision-making by the ANPD" (§1);

ii) guidance aims to promote orientation, awareness and education of processing agents and personal data subjects (§2);

iii) preventive activity, "preferably based on the joint and dialogical construction of solutions and measures", is intended to "bring processing agents back into full compliance" or "to avoid or remedy situations that may entail risk or damage" to data subjects and other processing agents (§3);

iv) repressive activity, which refers to coercive action, "aimed at interrupting situations of damage or risk, bringing them back into full compliance and punishing those responsible by applying the sanctions provided for in Article 52 of the LGPD" (§4).

The first of these, the monitoring activity, is made up of two instruments: the Monitoring Cycle Report (RCM) and the Priority Themes Map (MTP). The former has the function of (i) evaluating the inspection activities carried out, (ii) directing future actions and (iii) consolidating information obtained from requests and incident reports (Art. 20); while the latter acts as a parameter for the ANPD to define priority issues for the purposes of studying and planning supervisory activities (Arts. 21 and 22).

[13] E.g.: Presentation by the Director of ANPD Miriam Wimmer, in 12/04/2023. Available on: <https://www.camara.leg.br/evento-legislativo/67461?a=560242&t=1681308484647&trechosOrador=> 0min42seg. Accessed on 23 June 2024; <https://www.youtube.com/watch?v=oKYWZimEXnY> 25min08seg – 27min. Accessed on 23 June 2024.
Presentation by the Director President of ANPD Waldemar Gonçalves, in 22/08/2023. Available on: < https://www.youtube.com/watch?v=aIxbVWgoXQg> 2h12min. Accessed on 23 June 2024.
Presentation by the General-Coordinator of CGF Fabrício Lopes, in 25/07/2023. Available on: < https://www.youtube.com/watch?v=wmiZODsNzQA&list=WL> 15min25seg – 16min. Accessed on 23 June 2024.

The Monitoring Cycle for 2022 was only published in August 2023, which deserves attention, since the regulated agents and society were unaware for much of the year of the direction the ANPD might take. The Priority Themes Map, on the other hand, had not been implemented until December 2023, which was acknowledged by the ANPD itself in the content of the Monitoring Cycle Report.[14]

The failure to draw up the Priority Themes Map for 2023, even after drawing up the Monitoring Cycle for 2022, illustrates that the Authority, probably due to its recency and its staff shortages, has distanced itself from the principle of valuing oversight planning, which should be considered an element of its responsive regulatory strategy.[15]

The fact is that the existence of Priority Theme Maps is essential for establishing responsive regulatory guidelines, since this enables the regulator to understand the intended objectives, allowing it to choose the most appropriate instruments for achieving them (Gunningham; Grabosky, 1998).

It is not argued, however, that the ANPD should act in a rigid manner by strictly following its plans. This perspective is even dismissed by the Regulation itself, which provides that the General Supervisory Coordination or Directors from the Board of Directors (CD)[16] can reasonably propose changes to the Map of Priority Themes in case of new and urgent facts (Article 23). Considering this, there is no reason not to develop it, albeit approximately, which would demonstrate this proactive action from the Authority.

However, in 2024, the ANPD published its MTP for the 2024-2025 biennium, in line with the issues raised in the 2023 RCM. The parameters for prioritizing the cases to be analysed by the General Supervisory Coordination (CGF) that dealt with security incidents in the RCM for the first half of 2023 were defined. The criteria designated as the basis for prioritization were aligned with the sanctioning processes initiated by the CGF, essentially due to the parameter of failure to communicate the security incident to the data subjects, as will be seen below.

To the guidance activity, some examples of measures to be adopted have been designated[17], which do not prevent the adoption of other actions (Art. 29) that are compatible with the general bias of guidance, awareness and education of regulated agents (processing agents, other members or interested parties in the processing of personal data) and the subjects of personal data.

The preventive activity also contains exemplary measures, which may be extended to other interventions, as long as they are compatible with its main objective: bringing the treatment agent back into full compliance or preventing or remedying situations that entail risk or damage to the holder. The measures include: i) disclosure of information, ii) warning, iii) request for regularization or reporting and iv) compliance plan (art. 32).

Finally, the repressive activity corresponds to the administrative sanctioning proceeding (PAS) and its possible phases, which are: i) the preparatory procedure, set up before the infraction notice is drawn up, to carry out preliminary investigations; ii) the possibility of proposing a conduct adjustment agreement (TAC); iii) the phases of Initiation, Instruction and other procedures covered by the PAS itself.

Although the ANPD does not have all the instruments to adopt Responsive Regulation in its supervisory competence, since its supervisory premises still require improvement (compared to the draft of the inaugural principle article on responsive design), the Authority is constantly at work, opening ways to materialize them. It is therefore very important to analyse this issue to

---

[14]"It is worth noting that, although Article 20, Paragraph 1, I, of the Supervisory Regulation states that the Monitoring Cycle Report will also evaluate the inspection activities of the priority themes, this activity should take place from the next reports, as the Priority Themes Map will be drawn up for the first time this year". Available on: https://www.gov.br/anpd/pt-br/assuntos/noticias/2023-08-17-relatorio-do-ciclo-de-monitoramento-2022.pdf. Accessed on 3 Out 2023. (Author's translation)

[15] DRAFT OF AN INAUGURAL PRINCIPLE ARTICLE OF A RESPONSIVE DESIGN

Art…The regulation of ... shall observe the following premises: […] IV - valuing planning for the prioritization, selection, frequency, timing, duration and intensity of supervisions;

[16] The Board of Directors (also known as "CD") is the ANPD's highest governing body.

[17]Supervisory Regulation. Art. 29. I - drawing up and making available guides to good practices and model documents to be used by processing agents; II - suggesting that regulated agents carry out training and courses; III - drawing up and making available tools for self-assessment of compliance and risk assessment to be used by processing agents; IV - recognizing and publicizing the rules of good practice and governance; and V - recommendations for: a) use of technical standards that facilitate control by the holders of their personal data; b) implementation of a Privacy Governance Program; and c) observance of codes of conduct and good practices established by certification bodies or other responsible entity. § Paragraph 1 Other measures not provided for in this article may be adopted as long as they are compatible with the provisions of articles 27 and 28. § Paragraph 2 Regulated agents, or their representative associations, may suggest the adoption of the guidance measures listed above, subject to evaluation by the ANPD.

contribute to future adjustments and improvements in its activities. It is in this context that this paper will seek to demonstrate the ANPD's behaviour under the responsive bias in the next topic.

SES/SC CASE

Given that the ANPD has incorporated the fundamentals of responsive regulation into its Supervisory Regulation, it will be verified the practical application of these provisions in specific actions taken by the Authority towards the regulated party in the sanctioning proceeding brought against SES/SC, which deals, among other things, with the need to communicate the security incident to the data subject. In addition to the responsive actions taken by the ANPD in this case, measures will be mentioned that could be used in favour of a more optimized regulatory design.

Brief report

This process began with the preliminary communication of a security incident presented by the controller, the Santa Catarina State Health Department (SES/SC), due to a failure in the controller's systems on 21st August 2021, when part of the waiting list database of the Unified Health System (SUS) in Santa Catarina, linked to the hospital regulation service, would have been exfiltrated after it was made available on the website listadeespera.saude.sc.gov.br. This initiative stems from a legal obligation on the part of the SES/SC to provide a digital service to inform citizens of the forecast and their position in the queue for care in the state's public health system, as required by State Law n. 17.066/2017 and State Decree n. 1.168/2017.

In the context of the Security Incident Communication Proceeding n. 00261.001020/2021-60, after several interactions between the regulated party SES/SC and the regulatory body ANPD and the lack of compliance with the ANPD's determinations, the Administrative Sanctioning Proceeding (PAS) n. 00261.001886/2022-51 was initiated. The PAS was opened due to possible violations of Arts. 38[18], 48[19] e 49[20] of Law n. 13.709/2018 (Brazilian General Data Protection Law - LGPD) and Art. 5[21] of Supervisory Regulation, culminating in the application of sanctions and corrective measures to the regulated party.

Chronology of main facts

Subsequently, the most relevant events in the case will be highlighted, which will provide the basis for i) an analysis of the Authority's responsive action towards the regulated party and ii) the facts that relate to the central topic of the obligation to communicate the security incident to the data subject, when this could lead to a relevant risk or damage to data subjects.

- **21/08/2021** – occurrence of the security incident.
- **23/08/2021** - SES/SC becomes aware of the security incident.
- **26/08/2021** – SES/SC submits preliminary Security Incident Communication (CIS) to ANPD.
- **08/11/2021 –** determination by the CGF (2994422) for the controller to notify the data subjects about the incident.
- **24/12/2021 –** analysis of the incident by the General Coordination of Technology and Research (CGTP) (3082118), which considered the seriousness of the security incident to be high because sensitive personal data relating to the health of a significant number of data subjects had been exfiltrated.
- **11/03/2022 –** determination by the CGF (3107909) for the SES/SC to correct a public note on the website, which did not communicate the real content of the security incident, in view of the principle of transparency and the provision of CIS parameters provided for in Paragraph 1 of Art. 48, LGPD. ANPD also determined the controller to attach to the proceeding proof of the CIS sent directly to the data subjects.

[18] Failure to submit Personal Data Protection Impact Assessment (RIPD) before the initiation of the administrative sanctioning proceeding (PAS).
[19] Absence of individualized CIS to the data subject; Absence of CIS within a reasonable timeframe. In accordance with Art. 48 of the LGPD, a Security Incident Communication (CIS) is mandatory both towards the ANPD and the data subjects affected, if there is an occurrence of a security incident that might result in significant risk or damage to data subjects.
[20] Absence of systems for processing personal data that meet security requirements, standards of good practice and governance, the principles of the LGPD and regulatory standards.
[21] Failure to submit a technical report on the incident, with no justification for not submitting the document.

- **18/03/2022 –** date on which the CIS order would have been partially complied with, through the publication of a news item about the incident on SES/SC website.
- **31/03/2022 –** SES/SC i) informs the quantity of data subjects affected (47,483), ii) reports that the general CIS to data subjects was published on its website and made a channel available for data subjects to obtain information about the event, and iii) requests for an extension of time to carry out the **individual** CIS and to conclude its personal data protection impact assessment.
- **11/04/2022 –** in an Order (3300944), the CGF grants more days for SES/SC to present the CIS to the data subjects and reiterates its determination to SES/SC attach information from the CIS to data subjects on SES/SC website about the incident.
- **06/05/2022 –** issuance of Notice 18/2022 (3348561) ordering the SES/SC to submit what was determined in the Order (3300944), after the stipulated period had elapsed, without any manifestation from the SES/SC.
- **16/05/2022 –** SES/SC informed the content and address of the general CIS to data subjects which was published on the website. The controller justified not having communicated data subjects individually because it did not have up-to-date and complete data about them to do so. The SES/SC requested a meeting to be held between representatives of the SES/SC and the ANPD to clarify doubts about the measures to be taken because of the incident.
- **24/05/2022 –** meeting held, as requested, between representatives of the SES/SC and the CGF. At the meeting, the formal and material insufficiency of the general CIS was pointed out, with the consequent need for it to be adapted, as well as for individual communication to be made to those whose data was available.
- **25/05/2022 –** request from the SES/SC for a period of 30 days to comply with the determinations made by the ANPD, including those related to proof of CIS for the data subjects and the presentation of information from the public note on SES/SC website about the incident. The SES/SC also stated that the information note on the incident would be adjusted and republished, for a period of six months, at https://listadeespera.saude.sc.gov.br/#/home.
- **30/05/2022 –** SES/SC sent to CGF, for prior analysis, a new version of the public note published in their website about the incident. The Coordination requested adjustments to its content.

- **10/06/2022 –** CGF (3426634) grants the request for a deadline, giving the controller five days to prove that the general CIS had been published on its website, since it had not been located.
- **20/06/2022** – presentation of proof by SES/SC of the new version of the general CIS on the controller's website. There was no proof in the individual CIS to data subjects, nor any further justification.
  - **14/09/2022** – about three months after the deadline for SES/SC to respond, the CGF issued Notice of Infraction 9 (0050621) in which it revealed the possibility of infractions of Articles 38, 48 and 49 of the LGPD and Article 5 of the Supervisory Regulation, moment in which the Administrative Sanctioning Proceeding was initiated.
  - **03/10/2022 –** attachment of Administrative Defence (3666467). Explanations on the mapping of methods to carry out the individual CIS to the data subjects, as well as an explanation of the inconsistency of information from the data subjects.
  - **07/08/2023** – attachment of Final Allegations (4470740). Clarifications on actions taken to comply with the order to send the individual CIS to data subjects.
  - **11/10/2023** – issuance of the Investigation Report (4478157), in which an unreasonable deadline was found for the general CIS, which would have been carried out on SES/SC's website in March 2022, that is, 7 months after the incident. It was also pointed out that the CIS was not carried out individually.
  - **16/10/2023** – issued Decisional Order (4647004) to apply a sanction of warning cumulated with corrective measures, so that to SES/SC i) maintains the general CIS on the website for another 90 days, and ii) notifies data subjects individually within 20 days.
  - **01/11/2023** – filing of an Appeal at 1st Instance (4700492) to challenge the deadline for compliance with the order to send an individual CIS to each affected data subject. These, in view of the dependence on a third-party service for its execution and the respective administrative process for the acquisition of the service by public entities.
  - **09/11/2023** – issued Decision Order (4716709), on reconsideration, to grant an extension of the deadline for SES/SC to send the CIS to the data subjects individually.

Connection between the procedures of SES/SC data breach's proceeding and the current ANPD' supervision planning

In principle, it is worth remembering that not every security incident must be reported to the ANPD and the data subject, since, under the terms of Art. 48 of the LGPD, the incident must be reported when it may cause significant risk or damage to data subjects.

However, given the large number of data security breaches that occur every day, the increasing number of such reports received by the ANPD and the difficulty in dealing with all of them, it is necessary prioritize those that may have a greater impact on the data subject and that may be sensitive from a broader point of view (categories of sensitive data, vulnerable people, high risk of processing, etc.).

The Security Incident Communication Proceeding of the Santa Catarina State Health Department (SES/SC) began even before the ANPD's supervisory planning was announced - thus, before the first versions of the RCM and MTP were released - as well as the Supervisory Regulation, published in October 2021 and the Security Incident Reporting Regulation (henceforth "CIS Regulation"), published in April 2024.

It is important to point out, however, that the facts and circumstances that led to the SES/SC proceeding being considered relevant both for i) prioritizing its analysis, and ii) recognizing it as a hypothesis in which incident reporting is required, in accordance with Art. 48 of the LGPD, are suitable - and it is likely that they have even been used as a subsidy - for the ANPD's current prioritization of the supervision of security incident cases, as stated in the RCM for the first half of 2023 and in the CIS Regulation.

According to the RCM for the first half of 2023, the prioritization of the choice of incident cases to be analysed was under pressure due to the expectation of an increase in the number of incident cases accumulated, at risk of being time-barred. In view of this, Director Miriam Wimmer issued Vote n. 18/2023/DIR/MW/ANPD[22] to propose to the Board of Directors (CD) criteria for prioritizing the analysis of security incidents. The parameters established by the DC were: incidents without notification to the holders of personal data and those in which at least one of the following conditions would be identified: a) the presence of sensitive data, data on children and adolescents or data that could expose the data subject to fraud; b) recurrence, i.e. those in which the same controller has reported the occurrence of other incidents in the last two years; or c) those whose controller's main activity involves high-risk processing, in accordance with Art. 4 of Regulation of Dosimetry and Application of Administrative Sanctions.

Furthermore, Art. 5 of the CIS Regulation[23] sets out the criteria that define whether a security incident can cause significant risk or damage to the data subject, in order to make CISs equally mandatory for the data subject and the ANPD, in the event that they can cause significant risk or damage to the data subject.

The present case fits the prioritization criteria established in the RCM for the first half of 2023, established according to the Vote of the Director Miriam Wimmer, since it concerns a security incident in the SES/SC systems, which was initially reported only to the ANPD, i) without the data subjects involved having been notified, and ii) having compromised data that possibly involved children, adolescents or the elderly (categories of vulnerable data subjects). Secondly, the hypothesis is in line with the relevance criteria of the items I, II and V of Art. 5 of the CIS Regulation, as it involved i) a large volume of data - 4GB of data

---

[22] Available on: https://www.gov.br/anpd/pt-br/assuntos/deliberacoes-do-conselho-diretor-1/cds-ano-2023/cd-16-2023-votos.pdf. Accessed on 12 Mar 2024.

[23] Security Incident Reporting Regulation:

Art. 5 A security incident may cause relevant risk or damage to holders when it may significantly affect the interests and fundamental rights of data subjects and, cumulatively, involve at least one of the following criteria:

I - sensitive data;

II - data relating to children, adolescents or the elderly;

III - financial data;

IV - system authentication data; or

V - large-scale data.

§ Paragraph 1 Incidents that have the potential to significantly affect the interests and fundamental rights of data subjects will be characterized, among other situations, in those in which the processing activity may inhibit the exercise of rights or the use of a service, as well as cause material or moral damage to data subjects, such as discrimination, violation of physical integrity, the right to image and reputation, financial fraud or identity theft.

§ Paragraph 2 Large-scale data incidents are considered to be those involving a significant number of data subjects, also considering the volume of data involved, as well as the duration, frequency and geographic extent of the data subjects' location.

§ Paragraph 3 The ANPD may publish guidelines with the aim of assisting processing agents in the assessment of the incident that may cause significant risk or damage to data subjects.

would have been exfiltrated (1.2 million records) - and ii) a large volume of data subjects - approximately 48,000 data subjects would have been affected.

The parameters that were implemented throughout and after the actions taken in the case of SES/SC, both in the RCM and in the CIS Regulation, reinforce the importance that the Authority attaches to the communication of the security incident (CIS) to the data subject, as provided for in Art. 48 of the LGPD following some criteria, which were verified in the case under analysis.

All these ongoings demonstrate the importance of the premise of "valuing planning for the prioritization, selection, frequency, timing, duration and intensity of supervisions", provided for in item IV of the Responsive Inaugural Article, which can be related to items I and II of Art. 17, of the Supervisory Regulation[24]. It will be interesting to monitor whether future cases of Security Incident Communication Proceeding that eventually will become Sanctioning Proceedings will also follow these standards.

In the scenario under analysis, the alignment between the prioritization criteria of the ANPD's strategic supervisory planning and the circumstances of the security incident that occurred with the SES/SC stands out. This perspective endorses the indicators of regulatory planning, which, in turn, "binds the regulator's strategy to define the priorities for enforcement action based precisely on a duly motivated decision as to which regulated parties should benefit from less ostentatious enforcement regimes and which should be reinforced by such enforcement"[25] (Aranha, p. 168, 2023).

Escalation of Authority intervention

One of the main objectives of the initial conception of responsive regulation is the escalation of the use of lighter regulatory strategies to more severe ones. The aim of this practice is to avoid conflict and keep the regulated at the bottom of the pyramid, so that the agent achieves compliance without sanctions. The paradox of the pyramid lies in the fact that the possibility of escalating to harsh responses at the top means that most of the regulatory action can be at the bottom of the pyramid (Braithwaite, 2011), as was seen in this case.

In line with this, the item I, “a”, of the Responsive Inaugural Article[26], as well as item IV, Art. 17, of the Supervisory Regulation[27], highlight the direction to be taken by the Authority, since regulation must observe responsive principles, such as prioritizing the use of cooperative means over punitive instruments.

From the subsumption of the case to the aforementioned articles, the ANPD's efforts to achieve scalable and proportional action can be identified, since the process began with the exchange of communications between the regulator and the regulated party; continued as a process of communication of a security incident and was transitioned to a sanctioning process only after repeated non-compliance by the regulated party with the determinations established by the regulator.

In this sense, as reported in the topic "Chronology of main facts", the ANPD ordered the SES/SC to carry out the CIS to the data subjects 3 times, by means of Orders (2994422; 3107909; 3300944), before adopting the preventive measure "Notice" (3348561), under the terms of Art. 32, II, of the Supervisory Regulation[28]. The Authority then granted requests for a meeting and an extension of the deadline for compliance. The "Notice of Infraction 9" (0050621), which opened the sanctioning proceeding, was only issued after the regulated party failed to comply with the measures requested by the ANPD, even three months after the deadline. Only after that and after ensuring the right to defence and contradictory, the sanction was imposed due to the lack of the Security Incident Communication (CIS) to data subjects individually and within a reasonable period, as defined in the specific case.

Figure 5. ANPD’s gradual interventions in the SES/SC case

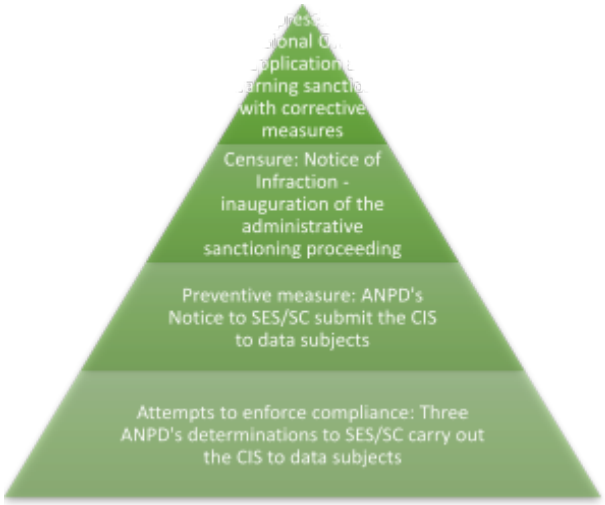
[24] Art. 17: The ANPD's supervisory process will observe the following premises:
I - alignment with strategic planning, with the instruments for monitoring data processing activities and with the National Policy for the Protection of Personal Data and Privacy;
II - prioritization of action based on evidence and regulatory risks, with a focus and orientation towards results;

[25] Author’s translation.

[26] Art... I - adoption, alone or jointly, of regulatory strategies proportionate: (…) d) to the systemic or individual risks inherent to the activity, decision-making processes, business management and the economic condition of the regulated parties.

[27] Art. 17. (...) IV - act in a responsive manner, adopting measures proportional to the risk identified and the stance of the regulated agents;

[28] Art. 32. The following are considered preventive measures: (…) II - notice.



Source: Elaborated by the author

From the above, we can see the practical application of the Authority's proposal contained in Art. 15 of the Supervisory Regulation[29], which provides for responsive action at different levels of intervention, among them, through guiding and preventive activities in the Security Incident Communication Proceeding, culminating in repressive activity in the Administrative Sanctioning Proceeding.

However, as will be better discussed in the last subsection of this paper, the Authority may, at least in these first cases of incidents that are chosen for analysis, for educational purposes, explicitly justify to the processing agent the importance of communicating the incident to the data subject since the beginning. Thus, demonstrating to the regulated party the precautions the data subject can take in the event of an incident, which would encourage the regulated party to obey orders from the ANPD more quickly, would avoid escalation of severe measures.

Of course, scaling will not always be followed to the letter, since this perspective should also be interpreted in conjunction with the principle of using measures that are proportional to the agent's behaviour. In this case, however, there was a significant commitment by the Authority to favour the responsive aspect of concentration in the pre-sanctioning moments of the pyramid (NDSR, 2021), given that the sanctioning process was only initiated almost one year after the ANPD's first imposition regarding the need to communicate the incident to the data subjects and only after several attempts by the Authority to encourage the regulated party to comply with the legal obligation provided for in the LGPD.

Proportional measures to the regulated's behavioural profile

Item I, point "a", of the Responsive Inaugural Article, emphasizes the "I - adoption, alone or jointly, of regulatory strategies proportionate: a) to the Administered Party's behavioural profile of compliance, coordination and cooperation;", which correlates with item IV of Article 17 of the Supervisory Regulation[30].

As explained in the topics "Chronology of main facts" and "Escalation of Authority intervention", the ANPD seemed to reinforce the idea of taking on instruments and measures of persuasion with a view to achieving regulatory compliance, acting in proportion to the efforts of the regulated party.

This can be seen from i) the response to the request for a meeting sent by SES/SC, which shows that the Authority, in assuming its role as a listener, granted space to the regulated party (Braithwaite, 2011); ii) the ANPD's clarification of the Secretariat's non-conformities, reiterating the desired requirements, and iii) the Authority's openness to requests for extension of deadlines, including in the decision of reconsideration.

On this last point, after several attempts to compel SES/SC to notify the data subjects of the security incident, the last move made by the defendant was to recognize, in an administrative appeal, that the sanction imposed due to the absence of an

[29] Article 15. The ANPD will adopt monitoring, guidance, and prevention activities in the inspection proceeding and may initiate repressive actions.

[30] Art. 17. (…) IV - act in a responsive manner, adopting measures proportional to the risk identified and the stance of the regulated agents;

individual CIS for the data subject had been duly applied, challenging only the deadline for compliance with the order to send an individual CIS to each affected data subject.

Then, in a retraction, the ANPD acknowledged the practical difficulties faced by the public body in carrying out the individual CIS, which also identifies the proportional attitude adopted by the regulatory body, in attention to the behaviour of the regulated party and its attempt to cooperate with the regulator, despite all the justifications that caused the momentary impossibility of carrying out the individualized CIS.

From the above, it can be concluded that the ANPD had the gradation of its intervention with the regulated party at its disposal, in an attempt to bring SES/SC into compliance, even though the DPA could have provide further justification for the importance about sending CIS to data subjects. The Authority also signalled its continuity in escalating the pyramid until the determinations were complied with. Therefore, the sanction imposed at the end did not appear to have been used as an end in itself, but as the result of a progressive process of dialog with the regulated party.

Result orientation

In the case of SES/SC, it is possible to verify the presence of the regulator's regulatory choices with a focus on results, in line with item I, paragraph "a" of the Inaugural Responsive Article and item II of Article 17 of the Supervisory Regulation. This is due to the ANPD's commitment to demonstrating two "results" to the regulated parties: i) the possibility of integrating regulatory instruments in a gradual manner and ii) the importance of reporting security incidents to data subjects.

The regulatory strategy adopted in the SES/SC case through the use of regulatory instruments present in the ANPD's pyramid of constraints (guiding, preventive and sanctioning measures) demonstrated that regulatory techniques[31] available to the ANPD were applied in a staggered manner, i) to the extent that the regulated party did not cooperate and ii) due to the specific context.

This is due to the practical exercise of integrating instruments of regulatory constraint, which was materialized in the process under analysis by: Orders (approaching an orientated bias); Warning (preventive measure); drawing up of the Notice of Infraction (initiation of an administrative sanctioning proceeding); and application of Warnings (sanctioning measures), which signalled to the regulated party the regulator's regulatory objective of implementing gradual interventions that are proportional and reflective of the regulated party's behaviour.

Of course, this does not invalidate the possibility that the institutes made available to the Authority are not applied gradually, since in the event of serious circumstances, the regulator can apply heavier sanctions, even if this results in not following the stages of cooperation with the regulated party from the bottom of the pyramid to the top (Baldwin and Black, 2007).

Regarding the second aspect, it was observed the emphasis given by ANPD to the individualized CIS to data subjects, due to its reiteration in determining the SES/SC to dispatch the communication to data subjects, which underscores the Authority's focus on ensuring that the regulated parties are oriented towards regulatory compliance with this obligation.

This fact corroborates the possible existence of regulatory risks related to the issue, given the fact that the specific CIS regulation had not yet been published in its definitive version at the time of the events described [32], which may therefore had given the regulated party the impression that this obligation was not yet of great value. However, the Authority apparently had tried to fill this gap by dealing with the issue not only in this case, but in most of the sanctioning proceedings published so far[33].

Thus, although the final version of the CIS regulation was still pending for publication at the time that the action were taken, and the fact that the "relevant risk or damage to data subjects" (art. 48, of the LGPD) had not yet been regulated at that time - a characteristic that gives rise to the obligation to communicate - the ANPD reinforced the requirement for the regulated parties to prepare the CIS for the data subject, qualifying the incident as a relevant risk or damage on a case-by-case basis, prioritizing part of its supervisory action for cases that contain evidence of the occurrence of the incident and the respective lack of

[31] In this article, the terms "regulatory instruments" and "regulatory techniques" are used synonymously. In this sense: "Regulatory instruments or techniques are means that the state uses to influence social behaviour to achieve the objectives set out in public policies." (Aranha, p. 70, 2023) (Author's translation).

[32] The CIS Regulation was published only in April 2024.

[33] The communication of security incidents to data subjects was also subject to sanctions in the Proceedings ns. 00261.001192/2022-14; 00261.001969/2022-41; 00261.001888/2023-21 and 00261.001963/2022-73. In addition, the absence of a CIS for the data subject is present in the Proceedings ns. 00261.001882/2022-73 e 00261.000456/2022-12, but they are still pending analysis or at least publication, according to information on the ANPD website. Available on: https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/processos-administrativos-sancionadores. Accessed on 13 June 2024.

communication to the data subjects – key factors applied to prioritize the monitoring of certain security incidents, as mentioned above.

The ANPD's actions in relation to the regulated entity appear to have been balanced. On the one hand, the absence of regulations on specific matters, such as reporting security incidents, makes it difficult for the regulated to know what to do in this respect, causing legal uncertainty. On the other hand, the Authority adopted several gradual measures so that the regulated entity could meet its expectations.

Improvement of regulatory design

As explained throughout this paper, the Authority's planning actions and administrative enforcement measures are directly related to its interactions with the regulated, which are instruments for "testing the quality and suitability of the standard, as well as collecting information that can contribute to the feedback and continuous improvement of the regulatory system" (NDSR, p. 381, 2021).

Consequently, the ANPD sought to compel the controller to comply with the obligation laid down in the rule, which is to notify the data subject of the occurrence of a security incident that may entail a relevant risk or damage to the data subject, under the terms of Art. 48 of the LGPD. To this end, it was necessary to use various instruments to facilitate cooperation between the regulated party and the regulator.

However, with the use of increasingly harsh regulatory techniques, as the regulated party continued to fail to comply with the Authority's determination, the resistance and complexity of carrying out the individual CIS by the public body became apparent.

In view of this, it is interesting to reflect on alternative methods to be adopted by the ANPD in the future, so that this legal obligation can be complied with by the regulated parties without the need for coercion, much less individualized coercion of certain regulated parties by the regulator.

In this context, the use of administrative law institutions must be aligned with the intended regulatory objectives (Aranha, 2023), so that instruments such as sanctions can be replaced by other compliance measures to achieve results (principle of instrumentality of regulatory techniques). In the context of this study, one of the expected results would be recognition by the regulated parties of the importance of reporting security incidents to data subjects.

Hence the significance of regulating security incident communications. A rule that clarifies the importance and parameters of a CIS makes regulation more effective in all its senses - the existence of a cogent rule makes it possible to demand compliance by the Authority and by data subjects, brings greater legal certainty for those regulated, legitimizes the actions of the supervisory authority, stipulates the levels of constraints that infractions can be subjected to, etc. On the other hand, it is recognized that rules on the protection of personal data must go through an intense and lengthy process due to conditions such as public participation in the construction of the rule, as well as the analysis of the regulatory impacts arising from the edition of the rule - following practices recognized by the OECD[34], which leads to the current gap on the "ideal" proportional measure of action by the Authority in cases where the CIS is required of the data subject.

Furthermore, the adoption of other regulatory instruments and measures would be an alternative to achieve the desired result in terms of signalling the importance of the obligation to report security incidents. By way of example, the inclusion of a specific section in the Guide aimed at public authorities - already published by the ANPD - on security incidents and the need to communicate the security incident to the data subject, bearing in mind that guides and guidelines, in theory, do not necessarily need to be submitted to external consultations, so that their preparation becomes more celebrated. In this way, not only would the regulated party have greater legal certainty about their duties, but the regulator would also have less of a burden in overseeing cases like this.

An additional alternative is to make available a self-assessment for security incident related to personal data breaches, as provided for the Information Commissioner's Office (ICO)[35], so that regulated parties can reflect if there is a need to communicate the Authority and data subjects about the data breach.

Another solution is to show processing agents the measures that data subjects can take when they become aware of an incident, which would therefore clarify the real impact and importance of the agent guaranteeing CIS to the data subject. In this sense,

[34] OECD (2020), Regulatory Impact Assessment, OECD Best Practice Principles for Regulatory Policy, OECD Publishing, Paris, https://doi.org/10.1787/7a9638cb-en.

[35] Available in: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/. Accessed on 28 June 2024.

broadening the dissemination to processing agents of the document depicting the precautions to be taken by data subjects[36], would also allow the ANPD to avoid regulatory instruments on a scale of greater coercion, while maintaining the dissemination of the culture of personal data protection to all the actors involved in the regulatory environment.

Conclusion

The guarantee of digital services and the pursuit of transparency towards data subjects requires public authorities to handle personal data intensively, which must always guarantee data protection, in line with respect for individual freedoms and fundamental rights, especially given the current importance of these assets in a data-dependent society.

This reveals the importance of processing agents implementing tools to prevent foreseeable risks and mitigate potential or actual consequences. Even so, as has been shown, any processing agent is likely to be subject to a security incident, which could lead to a breach of the principles and rules guaranteed by the LGPD and related data protection and privacy laws.

However, the mere occurrence of a security incident will not give rise, as a presumption, to the need to comply with the determination to notify the ANPD, nor the data subject, since the incident must be qualified by the potential for "risk or relevant damage to data subjects". In cases in which the Authority is notified, either through a complaint or through a CIS received directly from the processing agent (in addition, of course, to those in which ANPD may act ex officio), the Authority may determine the need to communicate the incident to the data subject, when the controller has not carried it out, as well as prioritizing the analysis of incident cases in which there may be greater impacts, according, for example, to the criteria listed in the RCM of the first half of 2023.

That is why it is so important to adopt a regulatory strategy for the processing and protection of personal data that allows for the best way to conduct the analysis of this type of incident. In this sense, given that responsive regulation was advocated as a guideline in the ANPD Regulation, several aspects were highlighted, both in terms of the compliance of Article 17 of the Supervisory Regulation with the principles proposed in the Responsive Inaugural Article and in terms of the practical application of these principles and heuristics of the Responsive Regulation Theory to guide the ANPD's actions in the context of a case involving a data security incident.

Comparing the principles of the Supervisory Resolution with the principles proposed in the Inaugural Responsive Article, it was observed that there are several provisions that are aligned with Responsive Regulation, so that the ANPD has legal backing to use instruments and strategies paired with responsiveness. In any case, it is important to emphasize that i) the principle of valuing planning should continue to receive more attention, as has been seen over the semesters, and in accordance with criteria and targets that are achievable in practice; and ii) certain aspects provided for in the inaugural article can be incorporated subsequently, such as that of *respect for the instrumentality of forms and encouragement of continuous improvement in the provision of services about…*; *functional autonomy between follow-up, monitoring, convincing, management, cooperation, prevention, repair and control measures*; and the one that provides for restrictions on the use of *information voluntarily shared with the regulator by regulated parties*.

Regarding the subsumption of the SES/SC case to the responsive principles contained in the Supervisory Resolution and in the Responsive Inaugural Article, it was specifically verified the connections between a) the case prioritization criteria contained in the ANPD's most recent public enforcement planning and b) the characteristics of the SES/SC incident case, which matched several of these criteria.

Additionally, the criterion of proportionality of the measures employed in relation to the behaviour of the regulated company was observed, in particular because of: a) the response to a request for a meeting, in order to listen to the concerns of the regulated entity, b) the Authority's repeated determinations in response to the lack of responses from SES/SC; as well as c) the consideration of requests for a deadline extension, including a reconsideration decision, granted after understanding the various difficulties faced by the regulated company in sending CISs to the individual data subjects.

In addition, the use of escalating interventions by the ANPD against the regulated party was also exposed, starting with a CIS proceeding initiated by SES/SC in accordance with Art. 48 of the LGPD, which gradually progressed to more constraining measures, culminating in the application of sanctions, duly recognized by the controller, although it was mentioned that other more peaceful forms could be taken to avoid escalation of interventions, such as forms of improvement of the regulatory design.

Finally, in view of the ANPD's results-oriented approach, two aspects were highlighted that could be assumed as the Authority's desired end results: the demonstration of i) the possibility of integrating regulatory instruments gradually and ii) the importance

[36] "Fascículo Vazamento de Dados". Available on: https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf. Accessed on 13 Mar 2024.

of communicating security incidents to data subjects. As explained throughout the text, both perspectives were identified in the ANPD's work, although other measures could be employed and desired to improve these results.

REFERENCES

Aranha, M. (2023). Manual de Direito Regulatório: Fundamentos de Direito Regulatório. 8. ed, Laccademia Publishing, London.

Ayres, I. and Braithwaite, J. (1992). Responsive Regulation: Transcending the Deregulation Debate. Oxford University Press, Oxford.

Baldwin, R and Black, J. (2007). Really Responsive Regulation. LSE Law, Society and Economy Working Papers. London: LSE, 15, 1-47.

Braithwaite, J. (1985). To Punish or Persuade? Albany, NY: State University of New York Press.

Braithwaite, J. (2006). Responsive Regulation and Developing Economies. In: *World Development*, 34, 5, 884-898.

Braithwaite, J. (2002). Restorative Justice & Responsive Regulation.: Oxford University Press, Oxford.

Braithwaite, J. (2014). SPECIAL ISSUE: Evidence for Restorative Justice. *The Vermont Bar Journal & Law Digest*, Summer, 40, 18-22.

Braithwaite, J. (2011). The Essence of Responsive Regulation. University of British Columbia Law Review, 44, 3, p. 475-520.

Braithwaite, J.; Makkai, T and Braithwaite, V (2007). Regulating aged care: ritualism and the new pyramid. Edward Elgar Publishing, Inc, Cheltenham.

Brasil (1988). Constituição da República Federativa do Brasil de 1988, *Diário Oficial da República Federativa do Brasil*, Brasília, DF.

Brasil (2017). Decreto Estadual n. 1.168, de 29 de maio de 2017, Florianópolis, SC.

Brasil (2017). Lei Estadual n. 17.066, de 11 de janeiro de 2017, Florianópolis, SC.

Brasil (2018). Decreto n. 10.474, de 26 de agosto de 2020. *Diário Oficial da República Federativa do Brasil*, 20, 27 de agosto de 2020, Brasília, DF.

Brasil (2018). Medida Provisória n. 869, de 27 de dezembro de 2018. *Diário Oficial da República Federativa do Brasil*, 28 de dezembro de 2018, Brasília, DF.

Brasil (2018). Lei n. 13.853, de 8 de julho de 2019. *Diário Oficial da República Federativa do Brasil*, 20 de dezembro de 2019, Brasília, DF.

Brasil (2018). Lei n. 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da República Federativa do Brasil*, 15 de agosto de 2018, Brasília, DF.

Brasil (2021). Autoridade Nacional de Proteção de Dados. Coordenação-Geral de Fiscalização, Processo de comunicação de incidente de segurança n. 00261.001020/2021-60, Brasília, DF.

Brasil (2021). Autoridade Nacional de Proteção de Dados. Portaria n. 1, de 8 de março de 2021: Estabelece o Regimento Interno da Autoridade Nacional de Proteção de Dados – ANPD, *Diário Oficial da República Federativa do Brasil*, Brasília, DF.

Brasil (2021). Autoridade Nacional de Proteção de Dados. Relatório de Análise de Impacto Regulatório de Maio de 2021: Construção do modelo de atuação fiscalizatória da ANPD para zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados, Brasília, DF.

Brasil (2021). Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD n. 1, de 28 de outubro de 2021: Aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados, *Diário Oficial da República Federativa do Brasil*, Brasília, DF.

Brasil (2022). Autoridade Nacional de Proteção de Dados. Coordenação-Geral de Fiscalização, Processo Administrativo Sancionador n. 00261.001886/2022-51, Brasília, DF, Available on: https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/sesc-sc-00261001886202251-autos-publicos.pdf. Accessed on 15 Mar 2024.

Brasil (2023). Autoridade Nacional de Proteção de Dados. Relatório do ciclo de monitoramento: Exercício 2022, Brasília, DF.

Brasil (2023). Autoridade Nacional de Proteção de Dados. Relatório do ciclo de monitoramento: Exercício 1º semestre de 2023, Brasília, DF.

Brasil. (2023). Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD n. 10, de 5 de dezembro de 2023: Aprova o Mapa de Temas Prioritários para o biênio 2024-2025 e dispõe sobre a periodicidade do Ciclo de Monitoramento, *Diário Oficial da República Federativa do Brasil*, Brasília, DF.

Brasil (2024). Autoridade Nacional de Proteção de Dados. Vazamento de Dados - Cartilha de Segurança para Internet. Available on: https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf. Accessed on 15 mar 2024.

Doneda, D.C.M. (2020). Da privacidade à proteção de dados pessoais [livro eletrônico]: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. Thomson Reuters Brasil, São Paulo.

Doneda, D.C.M and Mendes, L. S. (2019). A Profile of the new Brazilian General Data Protection Law. In: Belli, Luca; Cavalli, Olga, (editors). Internet governance and regulations *in Latin America: analysis of infrastructure, privacy, cybersecurity and technological developments in honor of the tenth anniversary of the South School on Internet Governance,* FGV Direito Rio, Rio de Janeiro.

Drahos, P. (2004). Intellectual Property and Pharmaceutical Markets: A Nodal Governance Approach. Temple Law Review, 77, 401-424.

Frazão, A; Carvalho, A and Milanez G. (2022). Curso de proteção de dados pessoais: fundamentos da LGPD. 1. ed. Forense, Rio de Janeiro.

Gunningham, N; Grabosky, P. and Sinclair, D. (1998). Smart Regulation: Designing Environmental Policy. Clarendon Press, Oxford.

Gutierrez, A. (2020). Capítulo IX - Da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. In: Maldonado, Viviane Nóbrega; Blum, Renato Opice (coord.). *LGPD: Lei Geral de Proteção de Dados comentada* [livro eletrônico] – 2. Ed, Thomson Reuters Brasil, São Paulo.

Lima, C. R. P. d. (2020). Agentes de Tratamento de Dados Pessoais (Controlador, Operador e Encarregado pelo Tratamento de Dados Pessoais). In: Lima, Cíntia Rosa Pereira de (coord). *Comentários à lei geral de proteção de dados: Lei n. 13.709/2018, com alteração da lei n. 13.853/2019*. Almedina, São Paulo.

Mendes, L. S. and Fonseca, G. C. S. d. (2020). Proteção De Dados Para Além Do Consentimento: Tendências Contemporâneas De Materialização. In: *Revista Estudos Institucionais*, maio/ago, 6, 2, 507-533.

Mendes, L. S.; Rodrigues Jr., O. L. and Fonseca, G. C. S. d. (2023). O Supremo Tribunal Federal e a proteção constitucional dos dados pessoais: rumo a um direito fundamental autônomo. In. Doneda, D.C.M; Mendes, L. S.; Rodrigues Junior, O. L.; Sarlet, I. W. (coord.); BIONI, B. (coord. exec). *Tratado de Proteção de Dados Pessoais*. Forense, Rio de Janeiro, 61-73.

NDSR, Núcleo de Direito Setorial e Regulatório da Faculdade de Direito da UnB (2021). Estudo sobre abordagem comando-e-controle e teorias da regulação apoiadas em incentivos, com ênfase na regulação responsiva e seus fundamentos, inclusive o desenho das pirâmides responsivas, bem como sua aplicação direta no setor aéreo. Brasília.

Slaughter, A-M. (1997). The Real New World Order. Foreign Affairs, NY New York: Council on Foreign Relations, 76, 5, Sep. – Oct, 183-197. Available on: https://www.jstor.org/stable/20048208. Accessed on 1st Mar 2024.

OECD (2018). Relatório Revisão do Governo Digital do Brasil. Rumo à Transformação Digital do Setor Público. Principais conclusões. In: OECD, *Seminário sobre perspectivas para o governo digital no Brasil – Peer Review Governo Digital, May-02*. Available on: https://www.gov.br/casacivil/pt-br/assuntos/centrais-de-conteudo/eventos/ocde/2018/seminario-sobre-perspectivas-para-o-governo-digital-no-brasil/relatorio-revisao-do-governo-digital-no-brasil/revisaogovernodigitalbrasil-portugues.pdf/view. Accessed on 13 Mar 2024.

OAS (2021). *Princípios atualizados sobre a privacidade e a proteção de dados pessoais*. OAS. Documentos oficiais, OEA/Ser.D/XIX.20. Available on: https://www.oas.org/en/sla/iajc/docs/Publicacion_Principios_Atualizados_sobre_a_Privacidade_e_a_Protecao_de_Dados_Pessoais_2021.pdf. Accessed on 13 Mar 2024.

Wimmer, M. (2023). O regime jurídico do tratamento de dados pessoais pelo Poder Público. In: Doneda, D.C.M; Mendes, L. S.; Rodrigues Junior, O. L.; Sarlet, I. W. (coord.); BIONI, B. (coord. exec). *Tratado de Proteção de Dados Pessoais*. Forense, Rio de Janeiro.

Wimmer, M. (2023a). Sanções aplicadas pela Autoridade Nacional de Proteção de Dados. Anexo II, Plenário 08: Câmara dos Deputados, 12 abr. 2023. 1 vídeo (4min). Available on:

https://www.camara.leg.br/evento-legislativo/67461?a=560242&t=1681309481253&trechosOrador=&crawl=no. Accessed on 14 mar 2024.

Wimmer, M. (2023b). Os Desafios do Enforcement Na LGPD: Fiscalização, Aplicação de Sanções Administrativas e Coordenação Intergovernamental. In. Doneda, D.C.M; Mendes, L. S.; Rodrigues Junior, O. L.; Sarlet, I. W. (coord.); BIONI, B. (coord. exec). *Tratado de Proteção de Dados Pessoais*. Forense, Rio de Janeiro, p. 379-392.

Wimmer, M. (2023c). Voto n. 18/2023/DIR/MW/ANPD. Processo n. 00261.001548/2023-09. Available on: https://www.gov.br/anpd/pt-br/assuntos/deliberacoes-do-conselho-diretor-1/cds-ano-2023/cd-16-2023-votos.pdf. Accessed on 13 Mar 2024.