Security incident reporting: deadline, regulatory enforcement, and the competence of the National Data Protection Authority*

Comunicação de incidentes de segurança: prazo, regulatory enforcement e a competência da Autoridade Nacional de Proteção de Dados

*Sthéfano Bruno Santos Divino***

ABSTRACT

The General Data Protection Regulation determines reporting the security incidents to the National Data Protection Authority. However, it does not establish a deadline and form for this. The research problem is: how and what is the most appropriate way to regulate the deadline and sanctions for non-compliance with the reporting of security incidents? The objective

* Article received on January 11 2023 and approved on 23 February 2023. DOI: 10.12660/rda.v282.2023.90158.

** PHd and Master's in Private Law at Pontifícia Universidade Católica de Minas Gerais (PUCMG). Bachelor's in Law at Centro Universitário de Lavras. Full Professor on Cursos de Direito, Administração e Ciências Contábeis do Centro Universitário de Lavras. Acting Professor of Private Law at Universidade Federal de Lavras (Ufla) (3/2019-3/2021). Attorney. E-mail: sthefanoadv@hotmail.com.

is to analyze the regulatory competence under the Agencies Law, the Economic Freedom Law, as well as Bill n. 10,411/2020. Subsequently, the nature of the regulatory problem is identified and contributions to the preparation of the Regulatory Impact Assessment (RIA) are presented. Finally, the legal consequences for non-compliance are demonstrated, as well as criticisms about art. 21 of Bill n 10,411/2020. The conclusion is that there is no validly established deadline for reporting security incidents (since the necessary regulatory impact analysis was not verified), and art. 21 of Decree n. 10,411/2020 is unconstitutional. The research adopts the integrated method and the bibliographical research technique.

KEYWORDS

General Data Protection Regulation — security incident — communication — National Data Protection Authority — regulation

RESUMO

A Lei Geral de Proteção de Dados determina a comunicação de incidentes de segurança à Autoridade Nacional de Proteção de Dados (ANDP), contudo, não estabelece prazo e forma para tanto. O problema de pesquisa é: como e qual a forma mais adequada de regulamentar o prazo e as sanções pelo descumprimento da comunicação de incidentes de segurança? Objetiva-se analisar a competência regulamentar sob a ótica das Leis das Agências, da Lei da Liberdade Econômica, bem como do Decreto nº 10.411/2020. Posteriormente, identifica-se a natureza do problema regulatório e apresentam-se contribuições para elaboração da Análise de Impacto Regulatório (AIR). Por fim, demonstram-se as consequências jurídicas pelo seu descumprimento, bem como críticas sobre o art. 21 do Decreto nº 10.411/2020. A pesquisa adota o método integrado e a técnica de pesquisa bibliográfica.

PALAVRAS-CHAVE

Lei Geral de Proteção de Dados — prazo para comunicação de incidentes de segurança —comunicação de incidentes de segurança — Autoridade Nacional de Proteção de Dados — regulação

Introduction

The Brazilian General Data Protection Law (LGPD) proposes an experimental regime, filling a gap between experience and dogma, to filter previously defined operational practices with respect to a technological project built on a panopticon model. On the one hand, there is a digital interface experienced by individual subjects. On the other, datafication, digitization or e-personification exist in a systematized and rendered environment, designed to enrich the Big Techs.

Besides this preparatory critical observation, there is a level of strategy and considerable confidence in the possibility of controlling untrammelled capitalism. In this ambit, coercive measures are established to correct distortions that may be found in relentless marketing and behavioural practices. Legislation tries to soften the fixation on products and functional services, legitimizing the control of data by the owner through the exercise of informative self-determination.

However, a systemic assessment of the accumulation of surveillance and capital that occurred in the Cambridge Analytica case suffices to show there is a surplus for Big Techs in relation to behavioural exchanges, data and sanctions for non-compliance. In an ambitious aim to develop modules and legal regimes to monitor and diagnose data leakage incidents, the Brazilian company LGPD established a charter for safety and good practices, in which the imperative of unpredictability is considered intolerable and the limits and borders for data protection reside in correct management, implementation and adequacy of the aforementioned regulation, and for its maintenance through acts of corporate governance.

In this most elementary sense, art. 48 of the LGPD establishes that the "controller[1] must report to the national authority any occurrence of a security incident that may cause significant risk or damage to the holders". § 1 of art. 48 states that communication must be carried out in a timely manner and must contain minimal structural requirements.[2] Yet, how may we define what is

---

1 According to art. 5, VI, of the LGPD, the controller is the "natural or legal person, under public or private law, responsible for decisions regarding the processing of personal data". BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). Lei n. 13.709 de 14 de agosto de 2018. *Diário Oficial [da] República Federativa do Brasil*, Poder Executivo, Brasília, DF, 14 ago. 2018.

2 "I) description of the nature of the affected personal data; II) information about the holders; III) indication of which technical and security measures were adopted to protect data, provided commercial and industrial secrets are protected; IV) the risks arising from the incident; V) possible reasons and justifications for the delay, if communication is not undertaken within the established deadline; and VI) what measures were or will be adopted to remedy or mitigate the effects arising from the incident". Brasil, Lei Geral de Proteção de Dados, op. cit.

timely and adequate? In a report of a security incident involving personal data to the National Security Authority Data Protection (ANPD)[3] made available by the authority at the start of 2021, a period of two working days is indicated, from the date of cognizance, for respective communication. According to this description, there is no legal and normative imperative which imposes a duty of conduct on a controller to act in such a way. The ANDP recommendation only mentions (the considerable) flaw in the legislation in taking big steps without requisite self-construction. In other terms, what are the consequences in case of failure to observe the deadline recommended[4] by the authority? This is the first objective discussed here.

In presenting a hypothesis consistent with the legal architecture, there is a possibility of the ANPD exercising its regulatory power according to its competence established in art. 55-J, XIII and XVIII of the LGPD, recently updated in Law no. 13,853/2019.[5] However, such power is limited and must be preceded by consultations and public hearings, as well as a Regulatory Impact Analysis (RIA), according to art. 55-J, § 2 of LGPD.[6] In the latter case, its preparation must be in line with the precepts of art. 6 of Law No. 13,848, June

---

3 BRASIL. Comunicação de incidentes de segurança. ANPD. 2022. Available at: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Accessed on: 16 Feb. 2023.

"While regulation is pending, it is recommended that after becoming aware of the adverse event and if there is a relevant risk, the ANPD is informed as soon as possible, a notification within 2 working days, counting from the date of knowledge of the incident." "If the initial communication of the incident was not within the suggested period of 2 working days, after becoming aware of the incident, justify the reasons." BRASIL. *Formulário de comunicação de incidente de segurança com dados pessoais à Autoridade Nacional de Proteção de Dados* (ANPD). ANPD. 2021.

4 This deadline, as established in art. 33(1) of the General Data Protection Regulation (GDPR), must be cogent and not allow interpretative margins for its avoidance, unless duly justified, under the terms of art. 48, V, of the LGPD.

5 "Art. 55-J. The ANPD is responsible for: […] XIII — establishing regulations and procedures for protection of personal data, as well as impact reports on the protection of data for cases in which the processing poses a high risk to the guarantee of the general principles of protection of personal data provided for in this Law; […] XVIII — establish simplified and differentiated standards, guidelines and procedures, including deadlines, so that micro and small businesses, as well as business initiatives of an incremental or disruptive nature that declare themselves startups or innovation companies, can adapt to this Law." Brasil, Lei Geral de Proteção de Dados, op. cit.

6 "§ 2 The regulations and standards established by the ANPD must be preceded by public consultation and hearing, as well as regulatory impact analyses." Brasil, Lei Geral de Proteção de Dados, op. cit.

25th (Agency Law),[7] of art. 5th of the Freedom Law Economic,[8] in accordance with the prescriptions of Decree No. 10,411, June 30, 2020, which regulates the prior instrument. In other words, the preparation of the AIR permeates a procedure defining a regulatory problem, the assessment of which must be prior to the issuance of a normative act and contain information on the likely effects in the economic and social sphere in establishing reasonable parameters and conduct to support decision making.

Furthermore, for the problem to be identified properly, it must be recognize that the existing unwanted situation has diverse aspects, such as failures of market conditions, regulatory failures, informational asymmetry, acceptable or objective risks to social groups that want a solution or an appropriate regulatory intervention. Where technology can have destructive effects, such as unwanted and inappropriate interference in the market, points to the second objective of this article: to analyze and identify the legal nature of regulatory failure provided for in art. 48 of the LGPD, offering contributions to the preparation of the AIR.

This approach encourages normative development in the legislative function vis-a-vis interrelationships, addressing the social pressure for change. However, from an experimental view, the ANPD can apply the respective sanctions responsibly in the event of failure to comply with the *recommended* deadline. In other words, the nature of the issue regulated starts is based on justification of the ends by the means and denies the peculiarities of the guiding situations of the norm itself to the point of damaging the procedure required by the public administration itself. Here, it is worth highlighting the special autonomous nature of the ANPD according to MP no. 1,124, June 13, 2022. The instrumentalization of form and its non-compliance, then, should bring results that conflict with the normative system itself. What are these results? This is the final objective of this

---

7 "Art. 6. The adoption and proposals for changes to normative acts of general interest to economic agents, consumers or users of the services provided will, in accordance with the regulations, be preceded by Regulatory Impact Analysis (AIR), which will contain information and data on the possible effects of the normative act." BRASIL. Lei das Agências. Lei n. 13.848 de 25 de junho de 2019. *Diário Oficial [da] República Federativa do Brasil*, Poder Executivo, Brasília, DF, 25 jun. 2019.

8 "Art. 5. Proposals for establishing and amending normative acts of general interest to economic agents or of users of the services provided, implemented by a federal public administration body or entity, including government controlled autonomous entities and public foundations, will be preceded by regulatory impact analysis, which will contain information and data on the possible effects of the normative act to verify the reasonableness of its economic impact." BRASIL. Lei da Liberdade Econômica. Lei n. 13.874 de 20 de setembro de 2019. *Diário Oficial [da] República Federativa do Brasil*, Poder Executivo, Brasília, DF, 20 set. 2019.

work: to demonstrate the limitations of ANPD actions without the preparation of the AIR and the legal consequences of its acts in the study of the administrative acts.

Nevertheless, the present work has limitations, including the impossibility of establishing definitive and static identification standards for AIR, in relation to the problems presented here, as well as possible criticisms of the instrumentalization of society as a body without collaboration, harmony or integration. Still, the main contributions reside in the propositions: 1) In terms of communication of violation of personal data by the offender, the protection authority is an indispensable mechanism to administrative sanctioning and to implement the general precepts of governance of thematic legislation; 2) ANPD's recommendation regarding deadlines for reporting security incidents does not have binding or normative force; 3) the application of sanctions for non-compliance with art. 48 of the LGPD without the respective elaboration of regulations based on AIR is illegal; 4) illegality occurs due to non-compliance with the essential formality of the procedural rite due to the absence and lack of fulfilment of the duty of the public official responsible for requesting and preparing it; and 5) art. 21 of Decree no. 10,411/2020 is unconstitutional for violating the legal reserve provided for in art. 84, IV of the Federal Constitution.

In short, these objectives converge vis-à-vis a single research focus: how and what is the most appropriate way for the ANPD to regulate the deadline and sanctions for failure to report security incidents? In addressing the issue and complying with the proposals, we have used an integrated technique.

1. Deadline for reporting security incidents and ANPD enforcement: definition and description of the regulatory problem

The internet as structured and culturally produced shapes behavioural beliefs and values and creates patterns repeated by business institutions. A selection and integration process permeates the symbolism and dogma, spreading economic practices through social domains such as financial acquisition. The cornerstone for this process is collaboration network between users/data holders and large technological conglomerates that provide seemingly free services.

The essence of electronic business relationships is interactive, based on the internet, between producers, consumers and service providers.[9] All network architecture has considerable capacity for organic development through innovation practices and production systems and market demands, at the same time, which keeps its focus on the main objective: profit. The problem lies in the very transformation of capital markets into internet firms. The internet, importantly, is not merely technology, but a form of material communication and organizational production, as factories were. This is why the internet itself does not simply include originally digital companies, as there are no peripheries in the network, but, indeed, all in a single capitalist productive center.

All this economic and social integration, resulting from the functioning of a digital, concentrated market, has created a vast flow of personal data, and, with this development, come new challenges in terms of data protection in terms of collection, treatment and exclusion of information. Offering, in a solid and coherent way, predictions, specifications or restrictions, is the responsibility of the state, in the form of data protection legislation and regulations. In Brazil, the strengthening of legal security, was enshrined in Law No. 13,709, August 14, 2018, called the General Data Protection Law (LGPD).

LGPD ontology is the adoption of a diffuse control criterion that enables interested parties to operate directly, not just formally, in terms of a legal position regarding data. In other words, when control is prescribed, semantic and hermeneutic meaning surpasses the simple access to personal information, since the discipline tends to determine which information can be subject to protection, in public and private hands.

In this way, we see a dynamic movement toward informational self-determination capable of strengthening administrative democracy.[10] There is, then, a legislative approach based on direct intervention in the economy and the market with the purpose of regulating and outlining normative parameters of conduct, to prevent marketing logic taking precedence over the legal discipline of data protection. In fact, the insertion of the digital subject as the central issue was addressed by Constitutional Amendment no. 115/2022, which stipulated in art. 5, LXXIX, of the Constitution of the Federative Republic of Brazil data protection as a fundamental right.

---

[9] CASTELLS, Manuel. *A galáxia da internet*: reflexões sobre os negócios, a internet e a sociedade. Rio de Janeiro: Zahar, 2003. p. 65.

[10] RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. São Paulo: Renovar, 2008. p. 73.

The concern, therefore, is not just with simple data protection, but the future of an online social network segmented into digital models and structures at risk of fractionalizing its own identity and democracy. To try to escape or at least deal minimally with these risks, the LGPD established the National Authority for Data Protection (ANPD) as the competent authority to enforce its normative content. Initially, democratic production could be harmed by the dependence of ANPD on the Executive Branch. E-government could take advantage of its administrative structure and create relationships and economic and political dynamics appealing to normative application by the state entity itself. In other words, dependence of a national data protection authority directly to the Executive Branch poses a threat to the democratic environment, given the possibility of restriction, reduction or even cancellation of public policies based on the control and treatment of data obtained from the population.

Not to close our eyes to this risky asymmetry, considering legal subordination of data protection must be given both to the private sector and public authorities, the ANPD should be seen as an government controlled autonomous entity of a special nature, vis-à-vis conversion of Provisional Measure no. 1,124/2022 into Law 14,460/2022. This is not an option, but a need for independence so that the action is not specifically affected by political issues to the point of interfering with democracy. However, ANPD aims to create an environment capable of preventing the public and private spheres being dominated by data totalitarianism, absorbed by the productive sphere and economic exchanges. Therefore, data protection regulation and the enforcement of supervisory authority must be equally applicable to public and private activities within its regulatory scope and disciplinary competence.

A number of questions can be raised in relation to the LGPD, including security concerns. A security incident can be defined as an event, action or omission that allows or may allow unauthorized access, interruption or change in operations (including taking control), destruction, damage, deletion or adulteration of protected data, removal or limitation of use of protected information, or incorrect appropriation, dissemination and publication of data from a critical asset or activity over a period of time shorter than the objective recovery time.[11]

Note that the definition of security incident is broad, defined generically as data leak. The provisions of the ANPD are an indicative list as it is often not

[11] BRASIL. *Guia de resposta a incidentes de segurança*: Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: ANPD, 2021. p. 9.

possible to identify in entirety, for the purposes of investigation, all characteristic situations. Ethical standards and morals relating to data protection can also be violated and, in ultima ratio, be classed as security incidents, such as algorithmic discrimination and the sale of products at different prices through geolocation.

Faced with this situation, valuing the legality of the operation, the LGPD dedicated a section to good practices, in the processing of information. Among the conditions is the obligation to communicate to the ANPD security incidents where they occur. In an analysis of art. 48[12] of the LGPD we can identify some problems.

The first of these relates to the agent responsible for communication. The LGPD expressly states that it is the responsibility of the controller.[13] There are no provisions relating to this obligation vis-à-vis the data operator.[14] From a hermeneutic point of view, the normative interpretation must be restricted, under penalty of expanding the restriction of rights, presume solidarity, creating obligations not provided for by law. In this respect, despite the operator being directly involved in the collection and treatment of data, the obligation, responsibility and legal duty regarding the communication of Security incidents must be restricted to the controller.

In addition to issues involving the modality of responsibility adopted by the LGPD, there is a fundamental point regarding communication of incidents to the ANPD. Art. 48 of the LGPD only establishes the legal duty and the way in which communication must be carried out.[15] The only relevant provision states that it must be forwarded within a timely manner. However, how to define this deadline? LGPD does not expressly establish this. The ANPD, in *Formulário*

---

[12] "Art. 48. The controller must communicate to the national authority and the holder the occurrence of a security incident that may entail significant risk or damage to the holders." Brasil, Lei Geral de Proteção de Dados, op. cit.

[13] According to art. 5, VI: "the controller: a natural or legal person, under public or private law, responsible for decisions regarding the processing of personal data." Brasil, Lei Geral de Proteção de Dados, op. cit.

[14] According to art. 5, VII: "the operator: natural or legal person, under public or private law, who carries out the processing of personal data on behalf of the controller". Brasil, Lei Geral de Proteção de Dados, op. cit.

[15] It must be carried out in a timely manner and mention at least: "I) description of the nature of the data affected; II) information about those involved; III) indication of which technical measures and security measures were adopted to protect data, commercial and industrial; IV) the risks arising from the incident; V) possible reasons and justifications for the delay, if the communication is not made by the established deadline; and VI) what measures have been or will be adopted to remedy or mitigate the effects arising from the incident". Brasil, Lei Geral de Proteção de Dados, op. cit.

de Comunicação de Incidente de Segurança com Dados states two business days, from the date of cognizance of the incident, for the respective communication.[16]

Both the LGPD and the ANPD, in this respect, were at fault. There is no instrument rigid enough to break with the assumption of private autonomy and the beliefs about everything that is not prohibited by legislation. The great irony is that in these conditions, the deadline stipulated by the data protection authority is only indicative and carries not weight in relation to individuals and the State itself. It is ironic, as this particular failure may accompany the erosion of power over the sanctioning power itself.

The appropriate and inescapable response is to edit regulations and norms, whether resolutions or ordinances, according to the competence established in art. 55-J, XIII and XVIII of the LGPD, recently updated by Law no. 13,853/2019.

> Art. 55-J. The ANPD is responsible for:
> […]
> XIII — *editing regulations and procedures on the protection of personal data and privacy*, as well as impact reports on the protection of personal data for cases in which the processing poses a high risk to the guarantee of general principles of personal data protection provided for in this Law;
> […]
> XVIII — *enact simplified and differentiated standards, guidelines and procedures*, including deadlines, so that micro and small businesses, as well as initiatives of an incremental or disruptive nature that declare themselves startups or innovation companies, can adapt to this Law.[17]

In this regulation, the ANPD must expressly stipulate the deadline indicated as an objective parameter to be met, as, given its non-existence, the ANPD finds limitations for the application of administrative sanctions to controllers and those responsible for processing data for incidents occurring during the exercise of economic activity. Again, this difficulty arises precisely because the administrative procedure must require full and contradictory defence,

---

[16] "While regulation is pending, it is recommended that after becoming aware of the adverse event and if there is a relevant risk, the ANPD is informed as soon as possible, notified within 2 working days, counting from the date of knowledge of the incident." "If the initial communication of the incident was not communicated within the suggested period of 2 working days, after becoming aware of it, justify the reasons."

[17] Brasil, Lei Geral de Proteção de Dados, op. cit.

according to art. 55-J, IV, of the LGPD,[18] and in this procedure, if there is no law (in a formal sense, ranging from ordinances to constitutional amendments) formally establishing and objectively the obligations to be fulfilled, the ANPD may see reduced effectiveness and have its sanctioning power withdrawn in the face of regulatory inertia.

Thus, constitutional guarantees must be re-read and observed in light of technological innovation. It is essential, then, for ANPD to formalize this period through a regulatory norm, characterizing it as cogent and opposable erga omnes, under penalty of inapplicability or illegality of the sanction if applied in its current form (merely indicative). Still, the ANPD may encounter challenges in preparing this standard. Even though art. 55-J, XIII and XVIII authorize the elaboration of regulations aimed at improving LGPD, the regulatory power of the ANPD is limited and must be preceded by consultations and public hearings, as well as regulatory impact analyses, according to art. 55-J, § 2 of the LGPD.[19]

It would be a mistake to extract from these considerations that the ANPD may edit the regulation freely. There is a hermeneutic, semantic and legislative dependence linked to objective parameters and results through Regulatory Impact Analysis (AIR). In other words, considering concrete experience, so that there is no democratic imbalance, the introduction of this new regulatory form is directly linked to RIA both by virtue of 55-J, § 2 of the LGPD and art. 6 of Law no. 13,848, 25 June (Agencies Law),[20] of art. 5 of the Economic Freedom Law,[21] as well as the prescriptions of Decree no. 10.411, of June 30, 2020, which regulates the device retrospectively.

Current legislation confirms that such an ambitious objective cannot be relied upon solely at the unilateral disposal of the ANPD. Quantitative and

---

[18] "IV — Monitor and apply sanctions in case of data processing carried out in breach of legislation, through an administrative process that ensures full and contradictory defense and the right to appeal." Brasil, Lei Geral de Proteção de Dados, op. cit.

[19] "§ 2 The regulations and standards published by the ANPD must be preceded by consultation and a public hearing, as well as regulatory impact analyses." Brasil, Lei Geral de Proteção de Dados, op. cit.

[20] "Art. 6. The adoption and proposals for changes to normative acts of general interest to economic agents, consumers or users of the services provided will, in accordance with the regulations, be preceded by Regulatory Impact Analysis (AIR), which will contain information and data on the possible effects of the normative act." Brasil, Lei das Agências, op. cit.

[21] "Art. 5. Proposals for enacting and amending normative acts of general interest to economic agents or of users of the services provided, established by a federal public administration body or entity, including government controlled autonomous entities and public foundations, will be preceded by a regulatory impact analysis, which will contain information and data on the possible effects of the normative act, to verify the reasonableness of its economic impact." Brasil, Lei da Liberdade Econômica, op. cit.

qualitative data processing must respect the social environment and consider progressive economic and technological development, under penalty of inhibiting free enterprise.

Therefore, the regulatory problem posed is precisely the absence of an express deadline, suitable for data controllers and operators to report data incidents to the ANPD. For the AIR to be correctly prepared, the nature of the problem must be known and respective solutions and a prior analysis of the impact proposed. Herein, the aim of this article is to provide an analysis of this issue, without paternalistic or authoritarian exaggerations based on a reflection drawn from a regulatory and economic constitutional perspective.

2. AIR and the legal nature of the problem: analysis and brief contributions on the Kepner and Tregoe Method

The particular intersection between the public and private spheres can support the need for state interference through regulatory procedures. Initially, the study of Regulatory policy was monopolized by economists and occasional contributions from scientists, politicians and administrators were accepted as critical indicators in this area. However, in the current state of maturation and due to the daily practices of the last two decades, there has been considerable growth in interdisciplinarity themes, such as family law, contract law or environmental controls.[22] At the same time, we witness the crystallization of regulatory paradoxes where the main criticism and concern is intrusive regulation or the bureaucratization of the economy and social life.[23] In fact, understanding regulation as control exercised by a public authority over the economic activities of a community[24] appears problematic. The conceptualization of public authority in levels of governance and in relation to the private sector may vary, and how to exercise this control is controversial, as the definition

[22] EEKELAAR, J. M. Regulating divorce. Clarendon Press: Oxford, 1991; HANDLER, T. *Regulating the European environment*. Nova York: Chancery Law Publishing, 1997; STOLOFF, N. *Regulating the environment*. Dobbs Ferry, NY: Oceana Publications, 1991

[23] BALDWIN, R.; CAVE, M.; LODGE, M. Introduction: Regulation—the field and the developing agenda. In: BALDWIN, R.; CAVE, M.; LODGE, M. (Org.). *The Oxford handbook of regulation*. Oxford: Oxford University Press, 2010. p. 3.

[24] SELZNICK, Philip. Focusing organizational research on regulation. *Regulatory Policy and the Social Sciences*, v. 1, n. 1, p. 363-367, 1985.

of a community is a general clause, with a constantly ambiguous margin to define and identify economic problems concretely.[25]

In addition to these issues, there are common provisions within the regulatory framework, especially linked to the economic analysis of law, which appear as patterns or indications of sound regulation. State non-intervention from the perspective of the Social Welfare theory, for example, postulates the free action of the market through efficient allocation of economic resources, but from a very restricted point of view, since this condition, in practice, becomes almost impossible to achieve. This impossibility occurs precisely due to the considerable social, economic and legal variables that are capable of creating points of intersection between failure and success and consequently reducing efficiency. In other words, efficiency as a pretension and greater objective, from the perspective of Pareto[26] is paradoxically limited by its own inability to deal with its failures, including market failures. In this spectrum we can find anti-competitive situations in the development of monopolies or oligopolies or even externalities that impose losses or benefits on third parties that the market cannot deal with. At the same time, there are public goods that cannot be appropriated by a private entity and cannot be consumed due to their indivisibility and non-fungibility. Finally, in this same sense, there are informational asymmetries, in which imperfect or unbalanced data can cause or generate inefficiency in the market vis-à-vis the power of choice.

This classic analysis scenario demonstrates that, to be more effective, regulations need to weigh potential risks and trade-offs from a holistic perspective, in terms of the social impact produced by its implementation.

---

[25] R. Baldwin, M. Cave e M. Lodge. Introduction, op. cit., p. 4. For methodological satisfaction, some definitions are presented. According to Giambiagi and Além, "the regulation instruments are tariffs, quantities, entry and exit restrictions, and performance standards." GIAMBIAGI, F.; ALÉM, A. C. D. *Finanças públicas*: teoria e prática no Brasil. Rio de Janeiro: Campus, 1999. P. 337. For Aragão, it is the "set of legislative, administrative and conventional measures, abstract or concrete, by which the State, in a restrictive manner of private freedom or merely inductively, determines, controls, or influences the behavior of economic agents, preventing them from harming social interests defined in the framework of the Constitution and guiding them in socially desirable directions". ARAGÃO, A. S. *Agências reguladoras e a evolução do direito administrativo econômico*. 2. ed. Rio de Janeiro: Forense, 2003. p. 37.

[26] "*A Pareto efficient outcome is where the welfare of one individual cannot be improved without reducing the welfare of others. Thus, Pareto efficiency is a situation where all parties benefit, or none are harmed, by a reallocation of resources, goods, assets, or a change in the law. The 'no-one-is-harmed' constraint avoids the economist making interpersonal comparisons of utility, i.e., evaluating whether the loss to one individual is counterbalanced by the gain to others. This Pareto criterion, named after the Swiss-Italian economist Vilfredo Pareto, is based on two additional value judgements: (1) that the individual is the best judge of his or her own welfare; (2) the welfare of society depends on the welfare of the individuals that comprise it.*" R. Baldwin, M. Cave e M. Lodge. Introduction, op. cit., p. 5.

This need is even more critical when new technologies are highlighted, which in a certain way can be a critical indicator of promotion or imbalance of social justice, increase or decrease in inequalities or even the adoption of authoritarian or totalitarian policies in favor of regulators. The necessary engagement and the intended efficiency can be achieved from the moment the State assumes the duty to spend more time preparing and practically checking the impact of the rules drawn up, and not just through theoretical presumption at the time of their proposal. After all, this is one of the *ex post* gaps in normative and regulatory assessments in relation to understanding the real impact on economic and social resources and investments.

It is for this reason that the Regulatory Impact Assessment — RIA, in English must be a tool developed through a constant and systemic process of analysis based on evidence that aims to evaluate, based on the definition of a regulatory framework problem, the possible impact of the action alternatives available to achieve the intended objectives.[27] The main purpose of AIR is to guide and support public decision-making and, ultimately, contribute to regulatory actions that can be effective and efficient.

The AIR process involves the Kepner and Tregoe Method,[28] analysed as follows. Five techniques are developed by the authors: 1) problem definition 2) description of the problem in four dimensions: identity; location; temporality and magnitude; 3) extraction of fundamental information in these dimensions to understand the possible causes of the problem; 4) testing the likely cause; 5) ascertaining the true cause.[29]

In our study, the main issue is identified as absence[30] of a suitable deadline to report security incidents to the ANPD. The problem, in fact, is not only lack of a deadline, but also its adequacy. What is the correct period, for communication

---

[27] BRASIL. *Diretrizes gerais e guia orientativo para elaboração de Análise de Impacto Regulatório* — AIR / Subchefia de Análise e Acompanhamento de Políticas Governamentais [et al.]. Brasília: Presidência da República, 2018a.

[28] KEPNER, Charles H.; TREGOE, B. J. *The new rational manager*. Princeton: New Jersey: Princeton Research Press, 1981.

[29] Charles H. Kepner e B. J. Tregoe, *The new rational manager*, op. cit., p. 38.

[30] Castro and Renda highlight that it is essential that those responsible for defining the problem avoid describing it as "lack of public intervention", as such intervention may, in fact, be one of the possible solutions to the problem, but is not "the problem itself". However, in this case the real problem is the lack of redress, as the exercise of administrative sanctions or the imposition of a duty on an individual, be it an individual tax payer or legal entity, only occurs through legal provision and normative stipulation. CASTRO, R. J.; RENDA, A. *Guía al Estudio de Impacto Regulatoria en la República de Ecuador*. Documento preparado para la Secretaría Nacional de Planificacíon y el Desarrollo (Senplades) del Gobierno de Ecuador. 2015

to be effective? This precise definition is important, as all undertakings, analysis and explanation occur based on the problem posed.

It is at this point that those responsible for AIR must assess the problem and consider the need for intervention. Preferably, the process should begin before the legislative planning phase, as interference in the economic domain will only have the necessary and anticipated effect when the problem is correctly identified and the regulator acts in the relevant regulatory zone.[31] The practices of regulatory authorities should only be exempt from prior preparation of the RIA in case of genuine emergencies or unforeseen events, when a significant delay could objectively risk the well-being of citizens. Supervisory bodies must be critical of managers who excessively use such exemptions. Managers should also be required to conduct an *ex post* evaluation to ensure that the regulation was effective vis-a-vis the period defined.[32]

The second phase is the description of the problem in its four dimensions. When Kepner and Tregoe refer to identity, they postulate what they want or try to explain. In other words, what is the problem itself? Here, the issue is identified as lack of adequate regulation. Further, what is the physical location and where can this problem be encountered? As the LGPD is ordinary legislation (Law no. 13,709/2018) prepared by the national legislative body and issued by the federal Executive Branch, its operation covers the whole of Brazilian territory, generating an *erga omnes* effect on all society, as it is a legal abstraction. Furthermore, the problem may be in art. 48 of the LGPD, which does not establish an appropriate deadline for the respective communication.

At this point we may address the following question: whom are affected by the regulatory problem? Data subjects, faced with a possible security breach, as well as controllers and operators, since an adequate timeframe is not previously established to the point of creating a legal obligation. In addition, the ANPD is also a direct actor in relation to the problem. The problem tends to directly and indirectly affect each of these actors. It directly affects data subjects, as their personal information can be targets due to a lack of digital security, and as a result of normative trivialization through non-adoption of digital governance practices. Indirectly, for those responsible for data protection, a reduction in transaction costs is generated.

At the moment, the ANPD is contributing to the persistence of the problem, as no actions or practices are implemented to remedy it. Although aggravation

---

31 OECD. *OECD regulatory policy outlook 2021*. Paris: OECD Publishing, 2021. p. 77.
32 Ibid., p. 78.

cannot be claimed, at the same time, behavioural change is wanting, in order to avoid, minimize or solve the regulatory problem. Inertia is a preponderant factor.

Furthermore, and in the same sense, the timeframe must be defined, indicating when the problem was initially observed, how much it has been observed since then, and identifying when the solution cycle for this problem began. The observation of the problem may have occurred on February 22, 2021, when the ANPD released a guidance note on its website.[33] The proposed solution was not a solution, but only a recommendation, And the solution cycle was paused on July 21, 2021, exactly at the moment of the latest update, according to information on the website.

Finally, the magnitude of the problem is considerably difficulty to define, since there is no quantitative data at hand. Still, the number of people and affected units can be easily defined: in general terms, all subjects who collect and process data and fall under the spectrum of LGPD regulations will be affected by the regulatory problem, as they have a legal obligation to report the incident. But there is no previously stipulated deadline for doing so.

This information must be taken into consideration for the proper operation of AIR, which is also part of a cyclical and dynamic implementation process that begins with identification of the problem in the regulatory arrangement of objectives. However, the legal nature of the aspect of the problem under analysis must appear as a factor that is not only classificatory, but hermeneutical, capable of placing it correctly and consequently identifying its roots and respective impact.

a) Market failures,[34] which encompass externalities, public commodities, informational asymmetry and excessive use of marketing/economic power;
b) Regulatory failures,[35] where there are failures in implementation or regulatory oversight or harmful rules created and imposed by the

---

[33] Brasil, *Guia de resposta a incidentes de segurança*, op. cit.

[34] "It occurs when the market alone is not capable of achieving efficient economic results, causing suboptimal resource allocations and preventing the achievement of maximum well-being from a social point of view. The most common market conditions are market power (monopoly, natural monopoly, imperfect competition), positive or negative externalities, information asymmetry and the existence of public or meritorious goods. Examples: • Information asymmetry between agents in the health market; and • Barriers to market entry of oil exploration, due to the high initial investments required." (Brasil, *Diretrizes gerais e guia orientativo para elaboração de Análise de Impacto Regulatório* — AIR, op. cit., p. 37).

[35] "It occurs when an action taken to resolve a regulatory problem is not effective or is inconsistent, creating new problems or worsening an existing problem. This can occur for a number of reasons, such as problem of poorly defined objectives, failure to implement or monitor regulation, consequences of unforeseen events, inconsistency between competing or complementary regulations, disruptive innovations, etc." Ibid., p. 37.

governmental official;

c) Institutional failures,[36] vis-a-vis public or private institutions that act in an inefficient or ineffective way, hindering the desired objectives;
d) Unacceptable risks,[37] to human health, safety, environment etc.;
e) Contribution to guaranteeing fundamental rights; that is
f) Social objectives,[38] understanding the need to guarantee fundamental rights or objectives in operationalizing public policies.[39]

When the problem is analysed from these perspectives there is a clear framing in terms of regulatory failure. The lack of formal regulations can mean that actors in this area lack mutual recognition or are not included in this standardization. In other words, there are doubts, uncertainties and insecurities in their business model, as there is an absence of objective criteria for analysis and verification to present responses to the application of administrative sanctions. In other words, the absence of an adequate deadline may mean the incident report is not carried out due to the impossibility of applying administrative sanctions vis-à-vis the lack of legal obligation in this regard. The regulatory asymmetry between public and private entities is symptomatic of the absence of regulatory clarity.

As the problem can present itself as multifaceted and have different causes and origins, it can also be framed as a dogmatic problem affecting human rights and constitutional issues, such as the privacy of the data subject or the free initiative of controllers and operators, as well as social objectives. Fostering adoption and LGPD implementation should not just be a legal enforcement

---

[36] "It occurs when institutions act in a dysfunctional way or have an unsatisfactory performance, damaging the efficiency and/or effectiveness of processes or preventing the achievement of the desired objectives. Lack of clarity, duplication or overlapping of competences between institutions, rigidity in changing standards or structures to adapt to new realities, and capture of institutions, are examples of factors that can cause institutional failures." Ibid., p. 18.

[37] "Occurs when there are risks that are considered intolerable or that can only be justified in circumstances exceptional. This type of risk may vary depending on local culture, the country's income level, etc. Example: Risk of bankruptcy of the financial system: may lead to the adoption of prudential regulatory rules." BRASIL. *Manual de Análise de Impacto Regulatório (AIR) e de Avaliação de Resultado Regulatório* (ARR). 3. ed. Brasília, Agência Nacional de Transportes Terrestres, 2020.

[38] "It occurs when there is a need for intervention to guarantee public policy objectives, such as: equity, housing, health, protection of national industry. Example: Regulation that seeks massification of broadband, aiming to contribute to the achievement of public policy objectives such as digital inclusion and improved productivity, with consequences for economic development, in addition to educational and health policies" Brasil, *Diretrizes gerais e guia orientativo para elaboração de Análise de Impacto Regulatório* — AIR, op. cit., p. 18.

[39] Brasil, *Manual de Análise de Impacto Regulatório* (AIR) e de Avaliação de Resultado Regulatório (ARR), op. cit.

factor, but a policy inserted in the public and private spheres to guarantee informative self-determination.[40]

Thus, as a supplementary suggestion with regard to consultations and public hearings, it is recommended the ANPD objectively analyse the appropriate time for companies to register notification, according to efficiency in the corporate governance sector. But this practice should not be preponderant or override the data protection of the holder, as the adequacy obligation is in force and there is no excuse for any legal entity to fail to comply. Only administrative sanctions cannot be implicated. Hence, the intermediate or a middle ground between a sanctioning regulatory aspect and cultural adequacy and understanding, which is indispensable for its constitution and effectiveness in case the privacy of third parties is infringed.

Among the possible actions to be taken in a regulatory environment are normative and non-normative. These include self-regulation, co-regulation, economic incentives and information and education. Even with the need for constant consideration, non-normative alternatives are not altogether effective. The discussion of dissuasive or persuasive actions[41] is pertinent, but in this case the regulations responsible appear more appropriate to encompass different behaviours and apply the necessary and punitive restriction on those who refuse to cooperate and effectively comply with legislation. It should be noted sanctions already have their respective place in the LGPD. Therefore, the challenge in this case is not identification and implementation of effective measures, but of mechanisms that bridge the gap between the imposition of a legal duty and sanctions in case of non-compliance. In other terms, it is not a question of creating elaborate prescriptive actions, which develop or create barriers or costs unnecessary to those regulated, but of rational and objective standards for applying the law itself.

If the proposal is analysed from the perspective of the four cost categories of Ehrlich and Posner,[42] it appears at least three assume an insignificant position. First, the cost of developing and implementing rules (rule-making costs) may be considerable, from the moment the LGPD demands public consultation and a hearing as a formal requirement for preparation. This demand is not just

---

[40] "Art. 7. The processing of personal data may only be carried out in the following cases: […] Art. 26. The shared use of personal data by the Public Authorities meets specific purposes for the execution of public policies and legal attribution by public bodies and entities, respecting the principles of personal data protection listed in art. 6 of this Law." Brasil, *Lei Geral de Proteção de Dados*, op. cit.

[41] B. Ballantine e B. Devonald, *Modern regulatory impact analysis*, op. cit.

[42] EHRLICH, Isaac; POSNER, Richard A. An economic analysis of legal rulemaking. *The Journal of Legal Studies*, v. 3, n. 1, p. 257-286, 1974.

illustrative, as it needs to take into account the economic and social reality to create appropriate regulations. Furthermore, the enforcement costs will be almost zero, since the sanctions are previously defined in law and may reach the ANPD upon complaint from the holder of the data or by an oversight. Even in the latter case, the costs of enforcement are already foreseen in the regulations. Thus, it is believed that there are no additional provisions in simply regulating the case. The same happens when analyzing the costs of this regulation for the industry and the market (compliance costs). As already mentioned, the adoption and implementation of the LGPD according to its Regulatory scope is not an option, but an obligation. In theory, businesses and activities in their ambit should have already implemented it effectively and deduct compliance costs from their accounts. What may cause an increase in costs are the deadline and the form of communication. In fact, it is believed that the ANPD statement of two working days should be maintained or at least increased to meet the demands of micro and small companies that do not have adequate knowledge to act effectively in the protection of the data collected and processed. Finally, social costs (harm costs) apparently do not occur, as there is no effective or apparent decrease in social wealth due to the regulatory act.

Note that AIR must be prepared through qualitative and quantitative means in Brazil, since identical regulatory responses or similar policies may be more effective in one country than in another. A possible answer is linked to the transaction costs of implementing this regulatory policy. However, that is not the issue addressed in this work.[43]

The in-depth analysis of possible alternatives that present themselves as causes, consequences and responses must be mapped and can be costly. However, the brief considerations developed here serve as indications of those that appear viable and with potential effectiveness to the point of being detailed and developed in the AIR.

---

[43] For more, see: LEVY, Brian; SPILLER, Pablo T. The institutional foundations of regulatory commitment: a comparative analysis of telecommunications regulation. The Journal of Law, Economics, and Organization, v. 10, n. 2, p. 201-246, 1994. "Levy and Spiller see regulatory design as consisting of two components: regulatory governance and regulatory incentives. The governance structure of a regulatory system consists of the mechanisms that societies use to constrain regulatory discretion, and to resolve conflicts that arise in relation to these constraints. On the other hand, the regulatory incentive structure consists of the rules governing utility pricing, cross- or direct-subsidies, entry, access, interconnection, etc. While regulatory incentives may affect performance, Levy and Spiller argue that regulatory incentives (whether positive or negative) only become important if effective regulatory governance has been established" (VELJANOVSKI, C. Economic approaches to regulation. In: BALDWIN, R.; CAVE, M.; LODGE, M. *The Oxford handbook of regulation*. Oxford: Oxford University Press, 2010. p. 9).

Another point of contribution to AIR are *ex post* actions. Monitoring the relevant conduct[44] and the adoption of collegiate bodies in decision-making[45] are part of the process developed and instrumentalized to elaborate a quality regulatory system.[46] This, then, is regulatory improvement through rational practice, an indicative factor of transparency and inclusion.[47]-[48]

Finally, another useful starting point for exploring reasons for regulation are the categories offered by Prosser, namely (1) regulation for economic and market efficiency, (2) regulation to protect rights, (3) regulation for social solidarity,

---

[44] DAL BÓ, E. Regulatory capture: a review. *Oxford Review of Economic Policy*, v. 22, n. 2, p. 203-225, 2006.

[45] LAFFONT, J.-J.; MARTIMORT, D. Separation of regulators against collusive behavior. *The Rand Journal of Economics*, v. 30, n. 2, p. 232-262, 1999; SNYDER, J. M. On Buying Legislatures. *Economics & Politics*, v. 3, n. 2, p. 93-109, 1991.

[46] BALLANTINE, B.; DEVONALD, B. Modern regulatory impact analysis: the experience of the European Union. *Regulatory Toxicology and Pharmacology*, v. 44, n. 1, p. 57-68, 2006.

[47] HUGÉ, J.; WAAS, T. Converging impact assessment discourses for sustainable development: the case of Flanders, Belgium. *Environment, Development and Sustainability*, v. 13, n. 3, p. 607-626, 2011; STARONOVA, K. *Regulatory impact assessment in Slovakia*: performance and procedural reform. Impact Assessment and Project Appraisal, v. 34, n. 3, p. 214-227, 2016.

[48] Art. 6 of Decree No. 10.411/2021 provides that: "AIR will be concluded through a report that contains: I — an objective and concise executive summary, which must use simple language that is accessible to the public in general; II — identification of the regulatory problem to be resolved, with presentation of its causes and its extension; III — identification of economic agents, users of services provided and others affected by the identified regulatory problem; IV — identification of the legal basis that supports the action of the body or entity regarding the identified regulatory problem; V — definition of the objectives to be achieved; VI — description of possible alternatives to face the identified regulatory problem, considering the options of non-action, normative solutions and, whenever possible, non-normative solutions; VII — description of the possible impacts of the identified alternatives, including their regulatory costs; VIII — consideration of the information and manifestations received as to possible social participation or other processes for receiving subsidies from interested parties in the matter under analysis; IX — mapping of international experience regarding the measures adopted for resolution and the regulatory problem identified; X — identification and definition of the effects and risks arising from enactment, amendment or revocation of the normative act; XI — comparison of alternatives considered for resolution of the identified regulatory problem, accompanied by a reasoned analysis that contains the methodology chosen for the specific case and the suggested alternative or combination of alternatives, considered more suitable for resolving the regulatory problem and achieving the intended objectives; and XII — description of the strategy for implementing the suggested alternative, accompanied by forms of monitoring and assessment to be adopted and, when applicable, assessment of the need for amendment or revocation of current standards. Sole paragraph. The content of the RIA report should, whenever possible, be detailed and complemented with additional elements specific to the specific case, according to its degree of complexity, scope and repercussion of the matter under analysis".

and (4) regulation as deliberation.[49] This is not the only categorization,[50] but the different groups are usually transversal to each other.[51]

Thus, technology itself is in fact a locus of market failure. There is no specifical link to technology or technological industries, but, particularly in this sector, it is desirable for regulations to formulate technical standards to enable interoperability between parties.

Thus far, we have seen the inapplicability of administrative sanctions due to non-compliance, without going into detail. The normative characteristics and justifications provided will be presented here.

3. The nullity of the Sanctioning Administrative Act in the absence of AIR: notes to art. 21 of Decree No. 10,411/2020

So far, we have determined that the freedom granted to economic agents by the legal system for the respective performance in the market is limited by a set of standards. This relationship is more accentuated when analysed from the perspective of the digital and shared economy, where the concept of consumption is replaced by idea of using goods, for which possession or ownership is not necessary.[52] This limitation cannot be given in a broad and unrestricted way, as it can subsequently have a negative impact on innovation, job creation, productivity, competitiveness, and national development, among others. Thus, *prima facie* social well-being is valued together with economic growth, efficiency and effectiveness.

One of the ways to achieve these ends was the creation of AIR. Its constitution presupposes the organizational unit of the public official responsible for elaboration of regulation inserted in the economic, legal and social sphere. The function of this unitary body, as demonstrated, is to address problems and make decisions in a cooperative way that takes all parties into consideration. It should be noted that, in this case, the parties are not restricted public administration, but include, as seen, those affected by the regulation.

---

[49] PROSSER, Tony. *The regulatory enterprise*: government, regulation, and legitimacy. Oxford University Press, 2010. p. 18.

[50] SUNSTEIN C. *After the rights revolution*: reconceiving the regulatory State. Cambridge: Harvard University Press, 1990. p. 47-73

[51] MOSES, L. B. Regulating in the face of sociotechnical change. In: BROWNSWORD, R.; SCOTFORD, E.; YEUNG, K. *The Oxford handbook of law, regulation and technology*. Oxford: Oxford University Press, 2016. p. 604-627.

[52] RAGAZZO, Carlos. *O direito e a economia do compartilhamento*. In: PINHEIRO, A. C.; PORTO, A. J. M.; SAMPAIO, P. R. P. *Direito e economia: diálogos.* Rio de Janeiro: FGV Editora, 2019. p. 573.

During the brief analysis given, we saw that AIR is a bureaucratic and onerous procedure, but a valuable tool in the implementation of regulatory policies. Non-compliance, however, must be checked with greater caution to identify premises or consequential results. As already mentioned, there are at least three regulations that require the preparation of AIR: 55-J, § 2 of LGPD[53], art 6 of Law no. 13,848, June 25th (Agency Law)[54], Article 5 of the Law of Economic Freedom,[55] and in accordance with the prescriptions of Decree no. 10,411, 30 June 2020.

However, art. 21 of Decree no. 10,411/2020 provides that: "Non-compliance with the provisions of this Decree does not constitute a valid excuse for non-compliance with the standard nor result in its invalidity".

Note, two observations, in this connection. First, as stated, the fact that sanctions are not applied immediately, given legislative silence on the deadline for notifying the competent authority, is no excuse for implementing the law in the business and economic sphere. Thus, as an imperative and cogent norm, all companies must structure themselves to meet the management purposes of data provided for in the legislation itself. This is the legitimizing instrument for data protection that goes beyond the matter of consent to collect and process, including the option of control over ownership.

The second observation is that the norm eliminates the possibility of invalidity of the norm established even in the absence of AIR. Thus, even if sparse legislation determines its prior elaboration as a normative condition of validity, there is no need to consider nullity of the regulatory act. At this point, the legislator offers considerable innovation. Hermeneutics, at this point, is essential with regard to the constitutionality of the instrument.

In the first place, there is a differentiation between law and regulation that is not limited or restricted to the origin of one or the other. The substantial distinction,

---

[53] "§ 2 The regulations and standards published by the ANPD must be preceded by consultation and a public hearing, as well as regulatory impact analyses". Brasil, *Lei Geral de Proteção de Dados*, op. cit.

[54] "Art. 6. The adoption and proposals for changes to normative acts of general interest to economic agents, consumers or users of the services provided will, in accordance with the regulations, be preceded by Regulatory Impact Analysis (AIR), which will contain information and data on the possible effects of the normative act." Brasil, *Lei das Agências*, op. cit.

[55] "Art. 5. Proposals for enacting and amending normative acts of general interest to economic agents or of users of the services provided, established by a federal public administration body or entity, including government controlled autonomous entities and public foundations, will be preceded by regulatory impact analysis, which will contain information and data on the possible effects of the normative act to verify the reasonableness of its economic impact." (Regulation)

according to Mendes and Branco,[56] "lies in the fact that the law can originally innovate in the legal system". On the other hand, the regulation, according to Bandeira de Mello,[57] only establishes the "organic procedures designed to implement the institutional principles established by law, or to develop the precepts contained in the law, expressed or implicit, within the orbit circumscribed." Thus, according to art. 84, IV, of the CRFB,[58] as established by the Federal Supreme Court (STF) in ADI no. 1,075-MC/DF,[59] the power of regulation granted to ministers of State, although constitutional, does not legitimize the establishment of normative acts of a primary nature, with their exercise, content and limits necessarily subordinate to the prescriptions of the laws and Constitution of the republic. Thus, even though it is of a secondary degree, the legal act only gives faithful normative execution to the extent that it forms a supplementary and descriptive part of the normative system, vis-a-vis the head of the Executive Branch of the Union.

With this premise, we see that defence of the administrative act creates obligations or restricts rights under penalty of violating private autonomy and the material constitutional domain. The regulatory Decree must be faithful to the content of regulated law. Legal determinations should not be expanded or the legislative scope restricted. The instrument responsible for this action is precisely the law. Decrees should only provide form and ways in which enshrined rights will be exercised.[60] In other words, the legal reserve is a mechanism to guarantee state impositions and respective restrictions in case of unavailability of due legal process guaranteed by the CRFB (art. 5, LIV), avoiding the suppression of rights or arbitrary and abusive exercise of public power.[61]

Thus, as the Economic Freedom Law and the Agencies Law did not delegate power to the Executive to expressly provide for obligation, a defect is found in the legislative act which compromises legislative material competence and makes it unconstitutional due to infringement of art. 84, IV of the CRFB. The Executive Branch does not have an autonomous creative force, nor does it

---

56 MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de direito constitucional*. São Paulo: Saraiva Educação SA, 2016. p. 973. (Série IDP-2020).

57 BANDEIRA DE MELLO, Oswaldo. *Princípios gerais de direito administrativo*. São Paulo: Malheiros, 1969. v. 1, p. 314.

58 "Art. 84. The President of the Republic is exclusively responsible for: […] IV — sanctioning, promulgating and enacting the laws, as well as issuing decrees and regulations for their faithful execution."

59 BRASIL. Supremo Tribunal Federal. ADI 1.075, rapporteur minister Celso de Mello, Full Court, judged on 24 Nov. 2006.

60 SCATOLINO, Gustavo; TRINDADE, João. *Manual de direito administrativo*. 4 ed. Salvador: Jus Podivm, 2016. p. 354.

61 BRASIL. Supremo Tribunal Federal. AC 1.033 AgR-QO, rapporteur minister Celso de Mello, Full Court, judged on June 16th, 2006.

provide conditions for decisive innovation in the legal order which legislative measures have not previously granted it.

The use and abuse of regulation by agencies, ignoring the preparation of the AIR, basing such conduct on art. 21 of Decree no. 10,411, June 30, 2020, in addition to unconstitutionality, results in the invalidity of the normative act through formal non-compliance with the regulatory process, as provided in art. 2 of Law no. 9,784/1999.[62] This is a moderate or mitigated formalism, which indicates that in the administrative process there must exist a reasonable and proportionate measure to meet the public interest and guarantee the rights of those administered.[63] In addition to its provision, it has an appropriate form and is regulated by Decree no. 10,411/2020, falling within the exception provided for in art. 22 of Law No. 9,784/1999.[64] For these reasons the illegality of the act is a mere consequence of non-observance of form and procedure.

It should be noted that AIR is not a mere formality, but an indispensable tool for regulatory organizational discipline, to prevent unfounded restrictive behaviour resulting from strong idealism or even totalitarian or arbitrary conduct typical of reactionary orders. For this same reason, Decree no. 10,411/2020, in art. 4,[65] recognized restricted situations exempt from AIR. In the rest it is an indispensable component of the regulatory administrative process. Economic regulation is an exception and must be treated with full

[62] "Art. 2. The Public Administration will comply with, among others, the principles of legality, purpose, motivation, reasonableness, proportionality, morality, broad and contradictory defence, legal certainty, public interest and efficiency. Sole paragraph. In administrative processes, the following criteria will be observed, among others: […] VIII — compliance with formalities essential to guarantee the rights of those administered;"

[63] NOHARA, Irene Patrícia. *Direito administrativo*. 11. ed. São Paulo: Atlas, 2022. p. 203.

[64] "Art. 22. The acts of the administrative process do not depend on a specific form unless the law expressly requires."

[65] "Art. 4. AIR may be waived, as long as there is a reasoned decision by the competent body or entity, in the cases of: I — urgency; II — a normative act intended to regulate rights or obligations defined in a hierarchically superior standard that does not allow, technically or legally, different regulatory alternatives; III — a normative act considered to have low impact; IV — a normative act aimed at updating or repealing standards considered obsolete, without changing their merits; V — a normative act that aims to preserve liquidity, solvency or health: a) insurance, reinsurance, capitalization and pension markets; b) financial, capital and exchange markets; or c) payment systems; SAW — a normative act that aims to maintain convergence with international standards; VII — a normative act that reduces requirements, obligations, restrictions or specifications with the aim of reducing regulatory costs; and VIII — a normative act that reviews outdated standards to adapt them to development of internationally consolidated technology, in accordance with the provisions of Decree no. 10.229, of February 5, 2020."

responsibility, assuming a possible delay or non-decision in the absence of appropriate instruments.

Finally, during the analysis of art. 48 of the LGPD, there is an omission establishing the deadline and its adequacy to the situations in which it is intended to proceed with sanctions. Given this situation, the material legislative exercise cannot be controlled, as the act is not adjusted to the hypotheses to which it applies. In other terms, there is no maintenance of legality due to non-compliance with the act and the normative requirements for its correct formalization. Thus, in addition to issues involving the formal aspects of the administrative process, there is a motivation defect potentially implying the nullity of the act practiced.

As the entire process must be guided by constitutional guarantees, there is no way to establish objectively measurable standards, especially with regard to deadlines, owing to normative silence. The broad and contradictory defence will possibly be affected and may result in the nullity of the act. As much as regulatory environment discretion is assumed, arbitrariness is not assumed as a reference standard. Restrictions should exist, as regulatory decisions in economic matters must be informed and enable deliberation in the decision-making process with concrete data that clarify the range of options available.[66] Therefore,

> with AIR, regulatory discretion is now seen as an administrative competence (not mere faculty) to evaluate and choose, on a concrete level, solutions based on robust reasons (factual and legal), which must meet requirements with safe, formal evaluations and substantial evidence of the fundamental right to good administration.[67]

Therefore, if the ANPD regulates the term of art. 48 of the LGPD without the respective preparation of AIR, the act carried out by the regulatory body will be riddled with defects vis-à-vis the absence of qualified motivation.[68] This

---

66 ALBUQUERQUE, Kélvia Frota de. *A retomada da reforma/melhora regulatória no Bra*sil: um passo fundamental para o crescimento econômico sustentado. Brasília: Seae/MF, 2013.

67 FREITAS, Juarez. Políticas públicas, avaliação de impactos e o direito fundamental à boa administração. *Sequência*, Florianópolis, n 70, p. 115-133, 2015.

68 TEIXEIRA, R. S. *Ausência da análise de impacto regulatório (AIR) exigível como causa de nulidade do ato regulatório normativo*. Monografia de conclusão de curso. Universidade Federal do Rio Grande do Sul, Porto Alegre, 2021.

is a mechanism designed to limit unfounded actions to the point of causing an impact on the market and the economy.

Conclusion

Our purpose here was to address the research question: how and what is the most appropriate way for the ANPD to regulate the deadline and sanctions for failure to report security incidents? As observed, the most appropriate way to regulate the deadline is by drafting regulations by the body itself. However, the answer, despite its simplicity, exists in the light of a complex regulatory procedure required by arts. 55-J, § 2 of the LGPD, art. 6 of Law no. 13,848, of June 25th (Agency Law), and art. 5 of the Economic Freedom Law, and per the prescriptions of Decree no. 10.411, of June 30, 2020. The entire process must occur through prior preparation of the AIR to determine the impact on the economic sector.

Brief, potential solutions were discussed in the second section, referencing the Kepner and Tregoe method to identify the problem and effective management strategies to resolve regulatory defects. And, in this sense, the legal nature of the regulatory problem appears as a regulatory failure and, incidentally, as a social objective.

One of the limitations of this study lies in the second section, since the considerations presented were necessarily brief. Regulatory impact analysis is extremely complex and it is not possible to exhaust it within the methodological limits of an article. Furthermore, there is a limitation in research knowledge about the economic and social criteria involved. For these reasons the contributions presented were broad in the sense of offering guidance for future studies and regulations in the ANPD.

However, it seems clear that preparation of the AIR is an indispensable formal element for correct regulation and its absence may cause nullity of the regulations prepared, as well as the sanctions applied based on this regulation. In other words, it appears that the imposition of a deadline by the ANPD, waiving the AIR, may contain motivation and formal defects under the terms of art. 2 of Law No. 9,784/1999, giving rise to its inadequate application.

Thus, it is recommended to guarantee independent functioning of the market, and observance of private autonomy is a way of implementing the fundamental precept of constitutional and democratic non-intervention without the necessary legal reservation. With this assumption, the aim is to avoid a

distortion of the functioning of the market and actions that are clearly illegal because they avoid existing legal and bureaucratic procedures.

Finally, it appears that art. 21 of Decree no. 10.411, June 30, 2020, contains an unconstitutionality defect under art. 84, IV, of the CRFB, as it establishes innovative legislation on regulatory matters, conduct prohibited by the Constitution and already decided in the ADI matter by the STF (ADI nº 1,075).

Thus, despite the limitations acknowledged, it is hoped the contributions made here suggest discursive possibilities in relation to this key topic of social interest, with its constitutional, administrative and regulatory-economic scope.

References

ALBUQUERQUE, Kélvia Frota de. *A retomada da reforma/melhora regulatória no Brasil: um passo fundamental para o crescimento econômico sustentado*. Brasília: Seae/MF, 2013. (Documento de trabalho, nº 35). Available at: http://www.seae.fazenda.gov.br/central-de-documentos/documentos-de-trabalho/documentos-de-trabalho-2006/Dt_35.pdf. Accessed on: 16 Feb. 2023.

ARAGÃO, A. S. *Agências reguladoras e a evolução do direito administrativo econômico*. 2. ed. Rio de Janeiro: Forense, 2003.

BALDWIN, R.; CAVE, M.; LODGE, M. Introduction: Regulation—the field and the developing agenda. In: BALDWIN, R.; CAVE, M.; LODGE, M. (Org.) *The Oxford handbook of regulation*. Oxford: Oxford University Press, 2010. p. 1-10.

BALLANTINE, B.; DEVONALD, B. Modern regulatory impact analysis: the experience of the European Union. *Regulatory Toxicology and Pharmacology,* v. 44, n. 1, p. 57-68, 2006.

BANDEIRA DE MELLO, Oswaldo. *Princípios gerais de direito administrativo*. São Paulo: Malheiros, 1969. v. 1.

BRASIL. Comunicação de incidentes de segurança. *ANPD.* 2022. Available at: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis . Accessed on: 16 Feb. 2023.

BRASIL. *Diretrizes gerais e guia orientativo para elaboração de Análise de Impacto Regulatório — AIR* / Subchefia de Análise e Acompanhamento de Políticas Governamentais [et al.]. Brasília: Presidência da República, 2018a.

BRASIL. Formulário de comunicação de incidente de segurança com dados pessoais à Autoridade Nacional de Proteção de Dados (ANPD). *ANPD*. 2021. Available at: https://www.gov.br/anpd/pt-br/assuntos/atual-formulario-de-comunicacao-de-incidentes-de-seguranca-com-dados-pessoais_01-03-2021-4.docx. Accessed on: 27 Feb. 2022.

BRASIL. *Guia de resposta a incidentes de segurança*: Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: ANPD, 2021. Available at: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca. Accessed on: 23 July 2022.

BRASIL. Lei da Liberdade Econômica. Lei n. 13.874 de 20 de setembro de 2019. *Diário Oficial [da] República Federativa do Brasi*l, Poder Executivo, Brasília, DF, 20 set. 2019.

BRASIL. Lei das Agências. Lei n. 13.848 de 25 de junho de 2019. *Diário Oficial [da] República Federativa do Brasi*l, Poder Executivo, Brasília, DF, 25 jun. 2019.

BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). Lei n. 13.709 de 14 de agosto de 2018. *Diário Oficial [da] República Federativa do Brasil*, Poder Executivo, Brasília, DF, 14 ago. 2018b.

BRASIL. *Manual de Análise de Impacto Regulatório (AIR) e de Avaliação de Resultado Regulatório (ARR)*. 3. ed. Brasília: Agência Nacional de Transportes Terrestres, 2020.

BRASIL. Supremo Tribunal Federal. AC 1.033 AgR-QO, relator ministro Celso de Mello, Tribunal Pleno, julgado em 16 jun. 2006.

BRASIL. Supremo Tribunal Federal. ADI 1.075, relator ministro Celso de Mello, Tribunal Pleno, julgado em 24 nov. 2006.

CASTELLS, Manuel. *A galáxia da internet:* reflexões sobre os negócios, a internet e a sociedade. Rio de Janeiro: Zahar, 2003.

CASTRO, R. J.; RENDA, A. *Guía al Estudio de Impacto Regulatorio en la República de Ecuador*. Documento preparado para la Secretaría Nacional de Planificacíon y el Desarrollo (Senplades) del Gobierno de Ecuador. 2015.

DAL BÓ, E. *Regulatory capture: a review*. Oxford Review of Economic Policy, v. 22, n. 2, p. 203-225, 2006.

EEKELAAR, J. M. *Regulating divorce*. Clarendon Press: Oxford, 1991.

EHRLICH, Isaac; POSNER, Richard A. An economic analysis of legal rulemaking. *The Journal of Legal Studies*, v. 3, n. 1, p. 257-286, 1974.

FREITAS, Juarez. Políticas públicas, avaliação de impactos e o direito fundamental à boa administração. *Sequência*, Florianópolis, n. 70, p. 115-133, 2015.

GIAMBIAGI, F.; ALÉM, A. C. D. *Finanças públicas*: teoria e prática no Brasil. Rio de Janeiro: Campus, 1999.

HANDLER, T. *Regulating the European environment*. Nova York: Chancery Law Publishing, 1997.

HUGÉ, J.; WAAS, T. Converging impact assessment discourses for sustainable development: the case of Flanders, Belgium. *Environment, Development and Sustainability*, v. 13, n. 3, p. 607-626, 2011.

KEPNER, Charles H.; TREGOE, B. J. *The new rational manager*. Princeton, New Jersey: Princeton Research Press, 1981.

LAFFONT, J.-J.; MARTIMORT, D. Separation of regulators against collusive behaviour. *The Rand Journal of Economics*, v. 30, n. 2, p. 232-262, 1999.

LEVY, Brian; SPILLER, Pablo T. The institutional foundations of regulatory commitment: a comparative analysis of telecommunications regulation. *The Journal of Law, Economics, and Organization*, v. 10, n. 2, p. 201-246, 1994.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de direito constitucional*. São Paulo: Saraiva Educação SA, 2016. (Série IDP-2020).

MOSES, L. B. Regulating in the face of sociotechnical change. In: BROWNSWORD, R.; SCOTFORD, E.; YEUNG, K. T*he Oxford handbook of law, regulation and technology*. Oxford: Oxford University Press, 2016. p. 604-627.

NOHARA, Irene Patrícia. *Direito administrativo*. 11. ed. São Paulo: Atlas, 2022.

OECD. *OECD regulatory policy outlook 2021*. Paris: OECD Publishing, 2021.

PROSSER, Tony. *The regulatory enterprise:* government, regulation, and legitimacy. Oxford University Press, 2010.

RAGAZZO, Carlos. O direito e a economia do compartilhamento. In: PINHEIRO, A. C.; PORTO, A. J. M.; SAMPAIO, P. R. P. *Direito e economia:* diálogos. Rio de Janeiro: FGV Editora, 2019. p. 571-598.

RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. São Paulo: Renovar, 2008.

SCATOLINO, Gustavo; TRINDADE, João. *Manual de direito administrativo*. 4 ed. Salvador: Jus Podivm, 2016.

SELZNICK, Philip. *Focusing organizational research on regulation*. Regulatory Policy and the Social Sciences, v. 1, n. 1, p. 363-367, 1985.

SNYDER, J. M. On buying legislatures. *Economics & Politics*, v. 3, n. 2, p. 93-109, 1991.

STARONOVA, K. Regulatory impact assessment in Slovakia: performance and procedural reform. *Impact Assessment and Project Appraisal*, v. 34, n. 3, p. 214-227, 2016.

STOLOFF, N. *Regulating the environment*. Dobbs Ferry, NY: Oceana Publications, 1991.

SUNSTEIN C. *After the rights revolution: reconceiving the regulatory State*. Cambridge: Harvard University Press, 1990.

TEIXEIRA, R. S. *Ausência da análise de impacto regulatório (AIR) exigível como causa de nulidade do ato regulatório normativo*. Monografia de conclusão de curso. Universidade Federal do Rio Grande do Sul, Porto Alegre, 2021.

VELJANOVSKI, C. Economic approaches to regulation. In: BALDWIN, R.; CAVE, M.; LODGE, M. *The Oxford handbook of regulation*. Oxford: Oxford University Press, 2010. p. 1-15.