Personal Data Protection in the Financial Sector: accountability as a bridge between innovation, competition, and consumer protection

DOI: 10.58766/rpgbcb.v19i1.1250

Lorenzzo Antonini Itabaiana*
Eduardo Goulart Pimenta**

Received: 29/10/2025
Approved: 11/12/2025

Abstract

The paper examines the centrality of the accountability principle in Brazil's General Data Protection Law (LGPD) and its role in safeguarding human dignity. A deductive method is adopted, based on national and international literature review, relating the four standards proposed by Daniel Sarmento – intrinsic value, autonomy, existential minimum, and recognition – to the LGPD's material and procedural requirements. The study identifies accountability as an operational governance axis that reduces information asymmetries, disciplines economic incentives, and structures transparency, particularly in the financial sector. It demonstrates that instruments such as records of processing, DPIA, legitimate-interest tests, and the data protection officer's role make the technical and commercial choices of data controllers and processors auditable. The study concludes that accountability is the central governance axis of the LGPD, acting as a balancer that reduces information asymmetries, structures transparency, and disciplines economic incentives, especially in the financial sector. It is therefore argued that the fundamental right to data protection is not absolute and allows flexibility when a proper legal basis, proportionality, and accessible data-subject controls are ensured. Finally, it sustains that regulatory convergence among the National Data Protection Authority (ANPD), the Banco Central do Brasil (BCB), *and the Administrative Council for Economic Defense (CADE) reinforces predictability and legal certainty, converting dignity into an operational benchmark for a data-driven economy.*

Keywords: *LGPD. Accountability. Human dignity. Competition. Consumer. Brazilian National Financial System.*

---

* *Lawyer. Master's degree in Law and Technology at the Federal University of Minas Gerais (UFMG). Specialist in Digital Law, Innovation Management and Intellectual Property from the Pontifical Catholic University of Minas Gerais (PUC/MG). https://orcid.org/0009-0008-2966-9644*

** *Associate Professor of Business Law at the Federal University of Minas Gerais (UFMG). Adjunct Professor IV of Business Law at the Pontifical Catholic University of Minas Gerais (PUC/MG). Member of the faculty of the Postgraduate Program in Law at UFMG and PUC/MG. PhD and Master's degree in Business Law from the Faculty of Law of UFMG. Attorney for the State of Minas Gerais. Corporate consultant and arbitrator. https://orcid.org/0009-0001-2425-5062*

Introduction

In 2024, 14,654[1] cyber risks were reported, including information security incidents and vulnerabilities. According to data from CTIR Gov "In Numbers[2]," most of these risks were related to data breaches. These threats, however, are not limited to breaches of personal data confidentiality. Irregular processing, in violation of legislation and often in a discriminatory manner, poses a risk to fundamental rights and guarantees, particularly in the financial sector. Such risks must be managed by data processing agents, especially organizations subject to authorization by the BCB). In this context, consumer rights related to the services offered by these organizations – especially the fundamental right to personal data protection and to human dignity – are under threat. The protection of these rights, however, must be balanced against other interests involved in the processing of personal data.

Using a predominantly deductive method, based on national and international[3] literature, this paper seeks to answer the following question: how does the accountability principle under the LGPD operate to reconcile human dignity with innovation, competition, and consumer protection, particularly in the financial sector?

*To this end, the **first section** addresses the inclusion of personal data protection among fundamental rights by Constitutional Amendment No. 115/2022 and the impact of this change on the subjective and objective dimensions of this right. It also discusses the obligations imposed on data processing agents by the LGPD, including the duty of accountability.*

*The **second section** examines personal data processing in the financial sector from the standpoint of competition law and consumer protection. It first analyzes data processing within the Brazilian National Financial System (SFN), and then explores the correlation between the risks arising from such processing and the core elements of human dignity, drawing on the four standards proposed by Professor Daniel Sarmento: intrinsic value, autonomy, existential minimum, and recognition.*

Finally, the paper argues that although human dignity must be preserved, the discipline of personal data protection requires balancing legitimate economic interests, which must equally be respected. In this scenario, the accountability principle plays a key role in reconciling these interests, ensuring social benefits such as economic development and innovation in the financial sector, without violating fundamental rights and guarantees such as informational self-determination and the protection of human dignity.

1 Personal data protection as a fundamental right and the accountability principle

Personal data protection is a fundamental right. Since the judgment of Direct Actions of Unconstitutionality Nos. 6388, 6389, 6390, and 6391 by the Brazilian Supreme Federal Court (STF), and the enactment of Constitutional Amendment No. 115/2022, this right has been included among the fundamental rights set forth in Article 5 of the Constitution of the Federative Republic of Brazil of 1988 (CR/1988).

Like all fundamental rights, personal data protection has acquired both subjective and objective dimensions[4]. In its subjective dimension, there has been an expansion of the claims held by data subjects,

1 *Available at https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros access in 6th jan. 2025.*

2 *CTIR Gov "Em Números" is a brazilian initiative created with the aim of providing general statistics of public interest related to government cyber incidents, in an environment that simplifies access to and understanding of data by means of interactive reports and a more user-friendly visual interface. Available at https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros, accessed on January 6, 2025.*

3 *Here, priority is given to European literature, especially the work of Professor Stefano Rodotà. Although the discipline of data protection is not discussed exclusively in Europe, the most significant debates originated there, culminating in the General Data Protection Regulation (GDPR), the European General Data Protection Law, which inspired the creation of Brazilian legislation. It is therefore prudent to seek concepts and perspectives developed on the European continent.*

4 *MENDES, Gilmar; GONET, Paulo. Curso de direito constitucional. 15. ed. São Paulo: Saraiva Educação, 2020, p. 218-219.*

requiring the adoption of specific behaviors regarding their data and imposing on data processing agents (controllers and processors) the duty to protect personal data and data subjects.

Data subjects have thus gained the right to demand the adoption of concrete measures to safeguard their private life, either directly through administrative channels – via mechanisms provided by the National Data Protection Authority (ANPD) that allow both complaints and petitions[5] – or through judicial means. Such rights already existed, for example, with respect to claims against public authorities to obtain information of personal, collective, or general interest, to be provided within the timeframe established by Federal Law No. 12,527/2011 (Freedom of Information Act). The innovation lies in the fact that these rights now derive from the recognition of the individual as a personal data subject deserving of protection, pursuant to Article 5, LXXIX, of the Federal Constitution, and are equally enforceable against private entities.

In its objective dimension, personal data protection has produced practical consequences that radiate throughout the legal system as a guiding vector for both public authorities and private actors.[6] As a result of this dimension, Federal Law No. 13,709/2018 (General Data Protection Law – LGPD)[7] began to require data processing agents to adopt specific behaviors, assuming responsibility and becoming more accountable[8] by demonstrating the adoption of effective measures capable of proving compliance with data protection rules. This principle was incorporated from the General Data Protection Regulation (GDPR)[9], the legislation that inspired the LGPD,[10] which defines it simply as accountability in Article 5(2). In the LGPD, this principle is expressly set forth in Article 6, X.

Although it is not possible to assert the existence of a hierarchy among statutory principles, the principle of accountability appears to occupy a central position. Accountability is understood as "an active process of knowledge creation whose objective is to scrutinize a given agent in order to make evaluation more feasible".[11] Due to the complex and technological nature of contemporary society, there is a profound need for data processing agents to render accounts and make their activities subject to scrutiny.[12] Ultimately, this need reflects the obligation of data processing agents to provide sufficient information to data subjects in order to ensure the exercise of their individual powers to limit or determine data processing operations[13].

To support such governance, Article 50, §2, I, "d" of the LGPD provides that controllers may implement a Privacy and Data Protection Governance Program which, at a minimum, establishes appropriate policies and safeguards based on a systematic process of assessing impacts and risks to privacy. This provision appears to encourage data processing agents[14] to define, based on risk assessment, systems of control and monitoring that allow them to assume risks in a controlled manner.

5 https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/denuncia-peticao-de-titular. Access in 28 oct. 2025.

6 GONÇALVES, Bernardo. Curso de Direito Constitucional, 13ª ed. Salvador: Ed. JusPodivm, 2021, p. 366.

7 Although the LGPD was enacted in August 2018, the provisions related to accountability only entered into force in August 2020, pursuant to Article 65, II of the LGPD, and therefore after the judgment of the Direct Actions of Unconstitutionality by the Supreme Federal Court.

8 BRASIL. Lei 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Brasília, DF: Diário Oficial da União, 2018. Art. 6º, X.

9 Our translation: "Accountability is therefore one of the pillars of the current European Community system for the protection of personal data, clearly provided for in Article 5(2) and Article 24(1) of the GDPR, as well as in the legal frameworks of several countries outside the European bloc. This includes Brazil, where the LGPD incorporated this principle – and the entire structural reasoning that derives from it – under Article 6, X, under the designation 'responsibility and accountability." In: PARENTONI, Leonardo. Compartilhamento de Dados Pessoais e a Figura do Controlador (Personal Data Sharing and the Role of the Data Controller. 2021, p. 5.

10 DE LUCCA, Newton; MACIEL, Renata Mota. A Lei 13.709, de 14 de agosto de 2018: A disciplina normativa que faltava. In: DE LUCCA et al. Direito e Internet IV. Sistema de Proteção de Dados Pessoais. São Paulo: Quartier Latin, 2019, p. 38

11 DE HERT, Paul; LAZCOZ, Guillermo. When GDPR-Principles Blind Each Other: Accountability, Not Transparency, at the Heart of Algorithmic Governance. European Data Protection Law Review. Berlin: Lexxion. v. 08, n. 01, p. 31-40, Apr. 2022, p. 4.

12 DE HERT, Paul; LAZCOZ, Guillermo. When GDPR-Principles Blind Each Other: Accountability, Not Transparency, at the Heart of Algorithmic Governance. European Data Protection Law Review. Berlin: Lexxion. v. 08, n. 01, p. 31-40, Apr. 2022, p. 5.

13 MONTEIRO, Renato Leite. Desafios para a efetivação do direito à explicação na Lei Geral de Proteção de Dados do Brasil. 2021. 383 f. Tese (Doutorado em Direito Comercial) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021, p. 86.

14 Although the legal obligation formally rests with the controller, it is understood that it is advisable for processors also to maintain a data protection governance program, especially because, at some point in their activities, they will process personal data in the capacity of controllers. This is the case, for example, when processing employee data. In such situations, an agent that acts as a processor in its core activities will act as a controller in its ancillary activities.

The term "risk" appears more than eleven times in the LGPD, allowing one to infer –together with Article 50, §2, I, "d" – that risk assessment is a relevant element of the statute. Moreover, systematic risk assessment enables institutions to organize measures according to priority, aiming to reduce impacts both on organizational activities and on the privacy and personal data protection of data subjects. Therefore, in the context of data protection, risk should not be viewed as an ethical or moral obstacle, but rather as an inescapable reality that guides the proper allocation of resources.

But what kind of risk are we referring to?

It is certainly not the risk of mere access to personal information. The notion of privacy, taken in isolation, dates back – since the seminal work by Samuel D. Warren and Louis D. Brandeis, The Right to Privacy[15]— to the idea of denying access, linking the use of information to the data subject's consent. If someone, without authorization, takes a photograph of the reader's bedroom, their privacy is violated. Such a photograph may contain private information about the reader's taste in decoration, the size of their bed, or the style of their wardrobe, among other details that, although seemingly irrelevant at first glance, may reveal intimate aspects of their life. These intimate aspects, without the reader's consent, should not be disclosed to the world and could cause surprise if revealed under such circumstances. For this reason, access to such information must be denied to unauthorized third parties and disclosure allowed only with the reader's consent.

The discipline of personal data protection does not necessarily produce the same effects. In the capitalist and informational[16] era, technological advances and the massive use of personal data for economic purposes have made it unthinkable to seek consent for every use. If the reader photographs their bedroom and voluntarily posts it on a social network such as Instagram, the platform will certainly use their preferences to feed its advertising auction systems ("ads").[17] Under the LGPD, it may even do so without consent, based on legitimate interest (Article 7, IX of the LGPD), provided there is a legitimate expectation and the other legal requirements are met. Nevertheless, it is incumbent upon the social network to provide sufficient information so that the reader may freely decide whether to continue posting such photos on Instagram and understand the consequences of doing so.

This paradigm shift was described by Stefano Rodotà as a "transition from a negative and passive formulation of data protection to a positive and dynamic one".[18] Thus, it is no longer necessary to verify abuse or violation for the data subject to be guaranteed the right to interfere in the stages of processing of their personal data.[19] If data may now be processed without consent, the data subject is also granted the power to intervene in such processing.

For this shift to be possible, it was also necessary to expand the participation of the data subject in the processing process. This expansion is encapsulated in the concept of informational self-determination, a foundational element of data protection law that grants individuals control over their information.[20] The term was coined in 1983 by the German Federal Constitutional Court (Bundesverfassungsgericht) in the landmark Volkszählungsurteil (Census Act decision), which recognized informational self-determination as a fundamental right.[21] The decision arose in response to the 1983 German census, which provided for extensive collection of personal data. The Court acknowledged that technological advancement –particularly automated data processing – posed a significant risk of creating detailed personal profiles without individuals'

15

16 *PELT, Eder van. Sujeito de direito digital: a nova governamentalidade do sujeito na era digital. Rio de Janeiro: Telha, 2024, p. 29.*

17 *As can be inferred from the Instagram Business website. https://business.instagram.com/advertising?locale=pt_BR. Access in 30 Dec. 2024.*

18 *RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Org. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 60.*

19 *RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Org. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 60.*

20 *DONEDA, Danilo. Da privacidade à proteção de dados pessoais. 3. ed. São Paulo: Thomson Reuters. 2021, p. 173; RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Org. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 46.*

21 *Available at https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html Access in 25 Dec. 2024.*

knowledge or consent, potentially leading to excessive surveillance and negatively influencing behavior due to psychological pressure stemming from possible public exposure.

By providing data subjects with sufficient tools to manage their data, the LGPD also grants data processing agents a presumption of good faith,[22] provided they render accounts of their activities by complying with the principles set forth in items I to VIII and, where they cause damage to third parties (item IX), are held liable. In other words, all principles guide the agents' duty to render accounts and their consequent liability, serving as an essential counterbalance for the equilibrium of forces. Accountability thus becomes the force that balances the dynamic between the natural person – whom the law designates as the data subject, surpassing the notion of ownership – and the private entity, defined by law as the data processing agent, which processes personal data.

The clash between these two forces is inevitable, as the relationship of interests among the various stakeholders constitutes an agency relationship. In such relationships, one party (the agent) undertakes to perform on behalf of another (the principal).[23] When conflicts arise, agency conflicts emerge, potentially generating additional costs (agency costs). Consequently, to mediate such conflicts and manage the associated costs, accountability toward stakeholders became necessary – for example, among shareholders, managers, and employees in private companies, and toward society in matters involving diffuse rights, such as environmental protection.

In the field of privacy and data protection, conflicts of interest materialize in the need to reconcile, simultaneously, the fundamental right to data protection and privacy – along with other aspects of personality – with economic, technological, scientific, and social development. This concern was not overlooked by the legislator, who included such objectives among the foundations of the LGPD, requiring their coexistence. A proper interpretation of the LGPD thus presupposes the reconciliation of data subject rights with economic and technological development and innovation, ensuring legal certainty for stakeholders.[24]

The challenge, therefore, is to allow institutions to develop their activities without violating basic rights of data subjects, or, where there is potential for violation, to ensure that risks are effectively managed. Noncompliance with the principles and the potential violation of data subject rights thus constitute the primary risks incurred by data processing agents[25] in a surveillance society or surveillance capitalism.[26] As seen, this is not merely a risk to privacy in the sense that data should never have been processed, but rather a lack of effective and necessary control over data while it is used for economic purposes, preventing data subjects from consciously exercising control over their information. The risk is exacerbated when processing in violation of the principles leads to infringements of fundamental rights and guarantees.

We therefore have a fundamental right to personal data protection which, through the principle of accountability, aims to protect other fundamental rights, such as non-discrimination, honor, and private life (Article 5, I and X of the Federal Constitution). All are essential to a dignified life. Violating them thus amounts to violating human dignity itself. The principle of human dignity is enshrined in Article 1, III of the

22 *PARENTONI, Leonardo. Compartilhamento de Dados Pessoais e a Figura do Controlador (Personal Data Sharing and the Role of the Data Controller). 2021. Disponível em https://www.researchgate.net/publication/351073596_Compartilhamento_de_Dados_Pessoais_e_a_Figura_do_Controlador_Personal_Data_Sharing_and_the_Role_of_the_Data_Controller, p. 5. Access in 30 Dec. 2024.*

23 *ARMOUR, John; HANSMANN, Henry; KRAAKMAN, Reiner. Agency Problems and Legal Strategies. In: The Anatomy of Corporate Law. A comparative and Functional Approach. KRAAKMAN, Reiner et al.Oxford: Oxford, 2017, p. 29.*

24 *"This analysis seeks only to provide an overview of the topic, followed by the author's legal position, in a clear, reasoned, and practical manner, based on the premise of reconciling respect for the rights of personal data subjects with economic development, innovation, and the functioning of the "data market," in order to ensure legal certainty for all parties involved." In: PARENTONI, Leonardo. Compartilhamento de Dados Pessoais e a Figura do Controlador (Personal Data Sharing and the Role of the Data Controller). 2021, p. 3.*

25 *It is acknowledged that there are other risks not directly related to the data subject, such as collective risks or risks of harm to the corporate entity itself. However, these do not fall within the scope of this article, which aims to investigate the impact of personal data processing on human dignity.*

26 *The terms used here correspond, respectively, to those adopted by Stefano Rodotà and Shoshana Zuboff. In: RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Org. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008; ZUBOFF, Shoshana. A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder. Nova York: Perseus Books, 2019.*

1988 Federal Constitution as one of the foundations of the Federative Republic of Brazil. This constitutional model, inspired by post–World War II European constitutions, prioritizes fundamental rights and guarantees, which in Brazil have been elevated to the status of unamendable clauses (Article 60, §4).

In this sense, the Brazilian Constitution places the human person at the center of the legal order, not from an individualistic perspective, but within a social and collective context.[27] Human dignity is therefore a value that permeates all legal norms, guiding their interpretation and application, and serves as a criterion for the creation or recognition of new fundamental rights[28], even when not expressly provided for in the Constitution. An example of this is the very judgment that recognized personal data protection as a fundamental right through Constitutional Amendment No. 115/2022.

To avoid open-ended and empty interpretations of the content of human dignity, it is necessary to establish benchmarks for its meaning in the context of this study. However, defining human dignity is not the purpose of this work, nor would it be feasible within such limited space. The proposal is merely to adopt a standard in order to avoid a malleable and amorphous use of human dignity.[29]

To this end, the approach adopted is that of Professor Daniel Sarmento[30], who, in his work Human Dignity: Content, Trajectories, and Methodology, breaks human dignity down into four basic elements:

- *intrinsic value of the person;*
- *autonomy;*
- *existential minimum; and*
- *recognition.*

Breaking down human dignity into objective standards allows the debate to move beyond mere rhetoric toward verifiable legal parameters. By adopting these criteria as an interpretative framework, the principle of accountability ceases to be merely an abstract command of the LGPD and becomes an instrument for concretizing dignity in its various dimensions: safeguarding the intrinsic value of the person, ensuring decisional autonomy, protecting an informational existential minimum, and promoting social recognition in digital contexts.

This perspective is particularly relevant when analyzing data-intensive sectors such as the Brazilian national financial system. In this context, the intersection of personal data protection, competition law, and consumer protection demonstrates that accountability is not merely a technical compliance duty, but a structural element of economic and social justice. It is within this framework that the following analysis is situated, examining how these principles interact within the regulatory environment of financial institutions, credit cooperatives, fintechs, and other actors operating in a market deeply driven by information.

2 Data processing in the financial sector: competition law and consumer protection

The financial system has historically been one of the most sensitive environments with respect to the processing of personal data. Banks, credit cooperatives, fintechs, insurance companies, and payment institutions rely heavily on the collection and analysis of customer information in order to offer products and services. Registration, transactional, biometric, and consumer behavior data become central assets for business strategies, generating innovation but also legal and ethical risks.

27 *SARMENTO, Daniel. Dignidade da pessoa humana: conteúdo, trajetórias e metodologia. Belo Horizonte: Fórum, 2016.*
28 *SARMENTO, Daniel. Dignidade da pessoa humana: conteúdo, trajetórias e metodologia. Belo Horizonte: Fórum, 2016, p. 77.*
29 *SARMENTO, Daniel. Dignidade da pessoa humana: conteúdo, trajetórias e metodologia. Belo Horizonte: Fórum, 2016, p. 16.*
30 *SARMENTO, Daniel. Dignidade da pessoa humana: conteúdo, trajetórias e metodologia. Belo Horizonte: Fórum, 2016.*

In this context, personal data protection cannot be analyzed in isolation. The massive flow of information circulating among financial institutions, consumers, and technological platforms has direct effects on competition among economic agents and on consumer protection. The Federal Constitution itself, while ensuring free enterprise and free competition (Article 170, caput and IV), also protects consumer rights as a principle of the economic order (Article 170, V). Accordingly, the debate on data protection finds in the financial sector a privileged field for observing tensions between economic efficiency, fair competition, and fundamental rights, materializing the agency conflict discussed in the previous chapter.

2.1 Processing of personal data in the Brazilian National Financial System (SFN)

Information is one of the main factors of competitiveness in the financial sector. Although the application of mathematical techniques to business is not a phenomenon exclusive to the twenty-first century, the volume of personal data (big data) processed at scale through innovative tools such as machine learning – enabled by high computational processing capacity – has opened new avenues for innovation across various sectors of society, uncovering hidden patterns previously inaccessible to human reasoning. In this sense, there is a clear trend toward data-driven institutions in the twenty-first century, aimed at maximizing productivity[31] while maintaining competitiveness.

The advantages of data exploitation were already evident in experiments conducted in the banking sector during the 1990s, which is regarded as an early adopter[32] due to the early implementation of data science principles. American entrepreneurs Richard Fairbanks and Nigel Morris realized that information technology had the potential to generate more sophisticated predictive models that could be applied to banking services, such as credit granting, payment behavior analysis, and even customer churn analysis.[33] To achieve this, however, it was necessary to obtain high-quality, minimally structured data. With this in mind, Fairbanks and Morris proposed offering various services randomly to customers of Signet Bank in Virginia, United States. Although the initiative initially resulted in losses for the bank, the eventual discovery of financial consumption patterns and data-driven decision-making rendered the operation so profitable that it led to a corporate spin-off,[34] resulting in the creation of Capital One, a major U.S. bank.

In Brazil, the processing of personal data within the Brazilian National Financial System (SFN) is subject to dense sub-legal regulation, compliance with which is essential for the effectiveness of the accountability principle. The coordinated action of the BCB and the National Monetary Council (CMN) structures a regulatory regime aimed at reconciling innovation, security, and data protection.

From a normative perspective, CMN Resolution No. 4,893/2021 – which addresses cybersecurity policy – and BCB Resolution No. 85/2021 – which establishes requirements for contracting cloud data processing and storage services – stand out. These regulations complement the LGPD framework by imposing governance duties and internal controls, requiring financial institutions to implement protection policies and continuous monitoring of operational and information security risks.

Open finance, regulated by Joint Resolution No. 1/2020 (BCB, CMN, and CNSP), constitutes a paradigmatic example of the application of the principle of proactive responsibility. The standardized model for data and

31 *PROVOST, Foster; FAWCETT, Tom. Data Science for Business: What You Need to Know About Data Mining and Data-Analytic Thinking. Sebastopol: O'Reilly, 2013, p. 10.*

32 *PROVOST, Foster; FAWCETT, Tom. Data Science for Business: What You Need to Know About Data Mining and Data-Analytic Thinking. Sebastopol: O'Reilly, 2013, p. 7.*

33 *PROVOST, Foster; FAWCETT, Tom. Data Science for Business: What You Need to Know About Data Mining and Data-Analytic Thinking. Sebastopol: O'Reilly, 2013, p. 10.*

34 *Under Brazilian law, and pursuant to Article 229 of Law No. 6,404/1976, a spin-off is defined as a corporate transaction by which a company transfers portions of its assets to one or more other companies.*

service sharing, based on customer consent, strengthens transparency and informational self-determination, while simultaneously requiring participating institutions to adopt auditable mechanisms for recordkeeping, authentication, and traceability – typical instruments of accountability.

Furthermore, the BCB Supervision Manual and the Cybersecurity Best Practices Guide demonstrate that accountability is not merely documentary in nature: it materializes through continuous risk monitoring and the ability of institutions to demonstrate the adoption of effective technical and organizational measures. The absence of such mechanisms may result in supervisory actions or administrative sanctions, pursuant to Article 44 of the LGPD. The principle of accountability thus connects directly to the Central Bank's supervisory function, which, by requiring verifiable evidence of compliance, internalizes the mandate of Article 6, X of the LGPD within the prudential regime of the SFN.

Despite the importance of personal data processing for financial institutions, it must not be overlooked that large-scale data exploitation may simultaneously generate risks to consumer privacy and data protection, as well as risks of market concentration. Below, based on the four standards proposed by Professor Daniel Sarmento, we examine how these risks to human dignity may materialize in the data processing activities of agents within the Brazilian National Financial System.

2.2 Four standards of human dignity: ethical data processing in the brazilian national financial system

2.2.1 Intrinsic value of the person

The first element, the intrinsic value of the person, seeks to determine whether there exists a natural quality inherent to human beings. To this end, dignity must be tested through hypothetical situations involving "collisions between the individual's fundamental rights and the interests of the majority or of an abstract entity, such as the State, the Nation, the people, or race".[35] Torture is often cited as a paradigmatic example in this discussion: is it justifiable to torture an individual to obtain a confession that could save many lives? If there is no certainty regarding how many or which lives would be saved, does torture remain justifiable? Or, conversely, is there a "moral foundation that transcends any utility"[36] and must be respected in all circumstances?

In the field of personal data protection, this raises the question of whether there exists an absolute right to personal data protection, or whether, in certain cases, interests such as privacy may give way to technological development and innovation. While this question would require a separate in-depth analysis, the structure of the LGPD itself reveals that, in several instances, the law allows economic development to prevail. For example, by permitting the use of personal data to train social media algorithms based on legitimate interest (Article 7, IX of the LGPD),[37] the legislation allows, in the name of economic interests, the rights to intimacy, privacy, and image use to be placed in a secondary position. Nevertheless, this does not amount, strictly speaking, to a violation of such rights, since the platform does not intend – nor should it – to use the image to the detriment of the data subject, but rather solely to train its artificial intelligence algorithms.

It may be argued that such use entails risks of discrimination against the data subject, which is indeed true. As previously noted, risk is a natural consequence of data processing, but it must be carefully managed.

35 *SARMENTO, Daniel. Dignidade da pessoa humana: conteúdo, trajetórias e metodologia. Belo Horizonte: Fórum, 2016, p. 102.*

36 *SANDEL, Michael J. Justiça: o que é fazer a coisa certa. Tradução de Heloísa Matias e Maria Alice Máximo. 40. ed. Rio de Janeiro: Civilização Brasileira, 2024, p. 53.*

37 *Here, no defense of this legal basis is being made; it is used solely in a hypothetical manner in order to test the autonomy standard from the perspective of personal data protection.*

Should the feared discrimination materialize, there would be a violation of human dignity due to a lack of respect for the intrinsic value of the person. Economic utility, therefore, is only justifiable insofar as fundamental rights and freedoms do not prevail, since, according to the Kantian formula,[38] the human being is an end in itself. This limitation is explicitly set forth in the LGPD provision defining legitimate interest,[39] and it also appears in other contexts, such as restrictions on the legal basis of fraud prevention (Article 11, II, "g" of the LGPD) and the mandatory preparation of a Data Protection Impact Assessment (DPIA) (Article 38) when processing poses risks to civil liberties and fundamental rights (Article 5, XVII of the LGPD).

From a competition law perspective, this standard opposes the reduction of individuals to mere economic inputs in digital markets. Data concentration by large financial institutions or payment platforms may be justified by efficiency gains, but it must respect the condition of the human being as an end in itself. From a consumer protection standpoint, the same rationale applies to abusive clauses that impose broad authorizations for data use (Terms of Use and Privacy Policies) or practices that exploit informational vulnerabilities. In line with the cross-sectoral application of the LGPD (Article 45) and its joint application with other legal frameworks, the Consumer Protection Code (CDC) acts as a counterbalance to excessive instrumentalization of individuals by prohibiting abusive practices and recognizing human dignity as a central value (Article 4, caput of the CDC).

Therefore, from the perspective of the intrinsic value of the person, a certain degree of instrumentalization of the data subject's data for economic purposes is permissible, provided that it does not violate other fundamental rights and guarantees.

Although the intrinsic value of the person is a parameter of utmost relevance, it is necessary – within the new paradigm of data protection law outlined above – to understand how data subjects may autonomously influence the processing of their personal data.

2.2.2 Autonomy

The second element of human dignity therefore also coincides with an essential element for the proper processing of personal data: the possibility of freely deciding on aspects related to one's private life. This element seeks to understand the extent to which individuals are, in fact, in control of their own decisions, as well as the limits of this private freedom. Private autonomy "corresponds to the individual's ability to make and implement choices concerning their own life," enabling them to decide what is good or bad for themselves.[40] Human dignity thus requires that individuals be able to decide for themselves, exercising full autonomy.

In this sense, can one speak of consumer autonomy in the context of personal data relations? Does a consumer act autonomously when they relinquish part of their intimacy in exchange for the use of their information by a social network? Is sufficient information provided so that the consumer may freely decide whether to accept the terms of such an arrangement? These questions inevitably lead back to the discussion of informational self-determination. This foundation, previously introduced in this work, requires that sufficient information be provided so that data subjects can define their conduct in relation to institutional data-use policies, thereby correcting informational asymmetries between institutions and consumers.

Such asymmetry generates a competition problem that directly affects consumer autonomy. The absence of autonomy and the concentration of data by financial institutions may also create barriers to entry for new

38 *SARMENTO, Daniel. Dignidade da pessoa humana: conteúdo, trajetórias e metodologia. Belo Horizonte: Fórum, 2016.*

39 *Article 7. The processing of personal data may only be carried out in the following circumstances:*
IX – when necessary to meet the legitimate interests of the controller or of a third party, except where the fundamental rights and freedoms of the data subject prevail and require the protection of personal data.

40 *SARMENTO, Daniel. Dignidade da pessoa humana: conteúdo, trajetórias e metodologia. Belo Horizonte: Fórum, 2016, p. 140.*

competitors, leading data subjects to depend on a small number of dominant institutions. The open finance initiative, led by the the BCB, illustrates an attempt to correct this distortion: by enabling the portability of financial data upon the data subject's consent, it seeks to restore individual control over personal information while simultaneously fostering competition in the sector.

Despite the recognition of the right to autonomy, informational self-determination – like all fundamental rights – is not absolute. In the very judgment of the Volkszählungsurteil, which recognized informational self-determination as a fundamental right,[41] the German Federal Constitutional Court also acknowledged its limitations, holding that other interests may prevail over it:[42]

> *"b) The right to "informational self-determination" is not, however, guaranteed without limitation. It does not afford the individual absolute or unlimited control over "their" personal data; rather, the individual develops their personality within the social community and is dependent on communication with others. Any information, including personal data, mirrors social reality and thus cannot be attributed exclusively to the person concerned. As repeatedly emphasized in the Court's case law, the Basic Law resolves the tension between the individual and the community by endorsing the notion that the individual is connected to and bound by the community. The individual must therefore accept that the right to informational self-determination is, in principle, subject to restrictions serving overriding public interests."*

For the German Constitutional Court, individuality does not prevail over the collective, which is essential to the formation of the individual and constitutes the social context in which they exist. This understanding appears to align with the limitations that the LGPD imposes upon itself. For example, the LGPD does not apply to matters of public security and national defense.[43] An individual who has committed a crime does not autonomously decide how law enforcement authorities will process their data, nor may they exercise the right to erasure of data held in police databases. In such cases, public interests prevail and limit the data subject's self-determination.

Accordingly, providing information to consumers appears to be the rule. Only data processing agents who can demonstrably invoke rights that prevail over the right to information are exempt from this obligation. Intellectual property rights may serve as an example, as their protection – previously discussed – may limit the scope of information disclosed to data subjects, as may other collective rights whose protection outweighs individual interests.

2.2.3 Existential minimum

The concept of the existential minimum is grounded in the understanding that "the State and society must provide the basic material conditions for those in need who are unable to sustain themselves,"[44] an idea embraced by the 1988 Constitution.[45] Only when basic subsistence needs – such as food, education, and

41 *Available at https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html. Access in 25 Dec. de 2024.*

42 *Available at https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html. Access in 25 Dec. de 2024.*

43 *The situations in which the LGPD does not apply are set forth in Article 4 of the LGPD:*
Article 4. This Law does not apply to the processing of personal data: I – carried out by a natural person for exclusively private and non-economic purposes; II – carried out exclusively for: a) journalistic or artistic purposes; or b) academic purposes, in which case Articles 7 and 11 of this Law shall apply; III – carried out exclusively for purposes of: a) public security; b) national defense; c) State security; or d) activities of investigation and prosecution of criminal offenses; or IV – originating outside the national territory and not subject to communication, shared use of data with Brazilian processing agents, or international data transfer to a country other than the country of origin, provided that the country of origin ensures a level of personal data protection equivalent to that provided under this Law.

44 *SARMENTO, Daniel. Dignidade da pessoa humana: conteúdo, trajetórias e metodologia. Belo Horizonte: Fórum, 2016, p. 190.*

45 *SARMENTO, Daniel. Dignidade da pessoa humana: conteúdo, trajetórias e metodologia. Belo Horizonte: Fórum, 2016, p. 193.*

health – are met can individuals fully exercise their autonomy. Although of limited direct application to the purposes of this work, the notion of the existential minimum bears an interesting correlation with the concept of freedom.[46]

Similarly, and with the natural limitations of the comparison, only a sufficiently informed individual can effectively take control of their personal data, including understanding the risks they incur when consenting to data processing or, even without consent, deciding to continue using a given product or service. Thus, in the realm of consumer protection, the existential minimum manifests itself through transparency: without adequate and minimum information, consumers cannot make conscious choices regarding credit, insurance, or the use of biometric data. Information here functions as an essential input for freedom, becoming a true fundamental consumer right.

From a competition law perspective, the existential minimum translates into the obligation to ensure, beyond mere information for informed decision-making, inclusive and non-discriminatory access to digital financial services. The exclusion of certain profiles through opaque algorithmic criteria may undermine economic citizenship itself.

2.2.4 Recognition

Recognition, like the existential minimum, has a limited scope of application within this article. Nevertheless, it offers valuable insights for understanding the scope of human dignity. Recognition consists in the "valuation of the recognized person, through an attitude that expresses due respect," the absence of which "oppresses, establishes hierarchies, frustrates autonomy, and causes suffering".[47] *It thus reflects the need to be accepted by others in one's full humanity. The recognition pillar encompasses issues such as sexual orientation, ethnic or racial origin, religion, among others, whose moral significance is often the subject of intense public debate.*

What these individual characteristics have in common is the potential to cause discrimination if improperly disclosed. Personal data classified as sensitive under the LGPD share this feature and therefore receive heightened legal protection, particularly through restrictions on the legal bases authorizing their processing. This aspect is also closely related to informational self-determination: while individuals must be free to express themselves – and to be recognized and treated with equal consideration – it is up to each person to decide when and how such expression will occur. Thus, an individual who wishes to disclose their sexual orientation to the world must do so within their own context, considering the personal risks involved. For this reason, it is crucial that individuals receive sufficient information from financial institutions that may potentially process such data, so they may decide whether or not to proceed. Irregular processing of such data by financial institutions may therefore deeply affect fundamental rights and guarantees, constituting a risk that data processing agents must assess.

Accordingly, a violation of the principle of human dignity will occur when the processing of personal data infringes the right to recognition – not only the individual's right to reveal personal characteristics without retaliation and with equal consideration, but also the right to control how such disclosure occurs.

46 *SARMENTO, Daniel. Dignidade da pessoa humana: conteúdo, trajetórias e metodologia. Belo Horizonte: Fórum, 2016, p. 197.*
47 *SARMENTO, Daniel. Dignidade da pessoa humana: conteúdo, trajetórias e metodologia. Belo Horizonte: Fórum, 2016, p. 242.*

Conclusion

This study sought to understand how the principle of accountability under the LGPD operates to reconcile human dignity with innovation, competition, and consumer protection, particularly in the financial sector. It proceeded from the hypothesis that accountability plays a particularly relevant role in the context of data processing within the financial system.

The analysis confirms this hypothesis, demonstrating that accountability occupies an axial position in the Brazilian data protection regime, functioning as an operative criterion for reconciling economic innovation with the protection of fundamental rights. By adopting the four standards of human dignity proposed by Daniel Sarmento – intrinsic value, autonomy, existential minimum, and recognition – as normative benchmarks, it becomes evident that the LGPD requires data processing agents not merely formal compliance, but a continuous capacity to justify decisions, measure risks, and demonstrate effective protection outcomes.

In practical terms, the principle of accountability extends into banking regulation as a complementary regime of supervision and governance. Within the context of the BCB, this entails requiring institutions to demonstrate, on a continuous and auditable basis, the effectiveness of their privacy and data protection programs, integrating them into internal control systems and operational risk management in accordance with SFN-specific regulations. Consequently, convergence between the LGPD, CMN/BCB resolutions, and ANPD guidelines establishes an integrated regulatory governance framework in which accountability serves as a link between technological innovation, financial stability, and consumer protection. This integration reinforces the Central Bank's role as a guarantor of a competitive, ethical financial market centered on human dignity.

Human dignity, as understood through these four dimensions, does not impose an absolute veto on data processing but rather establishes substantive and procedural limits: (i) a prohibition on instrumentalizing data subjects when there are significant harms or risks associated with financial data processing; (ii) sufficient information to enable free and reversible choices; (iii) minimum safeguards for the effective exercise of rights; and (iv) barriers against discrimination and stigmatization, enabling access to the banking system for data subjects and consumers. Within this framework, flexibility in data processing is permissible in specific cases, provided it is grounded in an appropriate legal basis, proportionality, verifiable technical and organizational measures, and accessible control mechanisms for data subjects.

In the financial sector, where data processing is particularly intensive, accountability plays an additional structural role. It reduces informational asymmetries by providing data subjects and the market with information about data processing practices, disciplines economic incentives by establishing administrative and judicial sanctions for noncompliance, and enables competition and consumer protection by leveling requirements across different markets.[48]

This new framework entails a shift from a purely prohibitive approach (such as the mere denial of access) to a positive and dynamic governance model based on control, transparency, and risk mitigation, supported by auditable documentation such as Records of Processing Activities (Article 37), Data Protection Impact Assessments (Article 38), and Legitimate Interest Assessments (Article 10). These instruments materialize the risk assessments conducted by data processing agents as a sine qua non condition for the lawful exercise of their activities.

48 *Considering that the LGPD applies across all sectors of the economy, subject to the statutory exceptions to its applicability and the special application regime for small-scale data processing agents.*

Finally, regulatory convergence among the ANPD, the BCB, and CADE should be understood as an institutional extension of accountability. Coordinated dialogue among authorities enhances legal certainty by establishing clear rules and standards for stakeholders[49]*, raises governance standards, and reduces agency costs.*

The practical path forward, therefore, lies in living governance. To ensure effective accountability, data processing agents within the Brazilian National Financial System must establish Privacy and Data Protection Governance Programs incorporating metrics, periodic audits, third-party management, proportional explainability, and competition and consumer impact assessments where appropriate. It is this practical architecture – rather than abstract documents such as generic privacy policies – that renders human dignity operational and sustainable in a data-driven economy.

References

ALEMANHA. Tribunal Constitucional Federal. ***Volkszählungsurteil – Census Act case – Judgment of 15 December 1983*** *– 1 BvR 209/83.*

ARMOUR, John; HANSMANN, Henry; KRAAKMAN, Reiner. ***Agency Problems and Legal Strategies. In: The Anatomy of Corporate Law. A comparative and Functional Approach****. KRAAKMAN, Reiner et al.Oxford: Oxford, 2017.*

BRASIL. Agência Nacional de Proteção de Dados. ***Resolução CD/ANPD 18, de 16 de julho de 2024.*** *Aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais. Diário Oficial da União: seção 1, Brasília, DF, 17 jul. 2024.*

BRASIL. Constituição (1988). ***Constituição da República Federativa do Brasil de 1988****. Brasília, DF: Senado Federal, 1988. Available at: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Access in: 18 jan. 2025.*

BRASIL. ***Lei 13.709, de 14 de agosto de 2018****. Lei Geral de Proteção de Dados. Brasília, DF: Diário Oficial da União, 2018.*

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. ***CTIR-Gov em números****. Available at: https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros. Access in: 18 jan. 2025.*

COSTA, Rafael Viana de Figueiredo. ***ANPD, BC e CVM:*** *reflexões sobre mecanismos de coordenação regulatória. Revista da Procuradoria-Geral do Banco Central, v. 18, n. 1, p. 93-107, jun. 2024.*

DE HERT, Paul; LAZCOZ, Guillermo. ***When GDPR-Principles Blind Each Other:*** *Accountability, Not Transparency, at the Heart of Algorithmic Governance. European Data Protection Law Review. Berlin: Lexxion. v. 08, n. 01, p. 31-40, Apr. 2022.*

DE LUCCA, Newton; MACIEL, Renata Mota. A Lei 13.709, de 14 de agosto de 2018: A disciplina normativa que faltava. In: DE LUCCA et al. ***Direito e Internet IV. Sistema de Proteção de Dados Pessoais****. São Paulo: Quartier Latin, 2019.*

DONEDA, Danilo. ***Da privacidade à proteção de dados pessoais****. 3. ed. São Paulo: Thomson Reuters. 2021.*

49 *For a deeper analysis of the intersection between the ANPD, the Central Bank (BC), and the Securities and Exchange Commission of Brazil (CVM), see COSTA, Rafael Viana de Figueiredo. ANPD, BC e CVM: reflexões sobre mecanismos de coordenação regulatória. Revista da Procuradoria-Geral do Banco Central, v. 18, n. 1, p. 93–107, June 2024.*

GONÇALVES, Bernardo. ***Curso de Direito Constitucional****. 13. ed. Salvador: JusPodivm, 2021.*

MENDES, Gilmar; GONET, Paulo. ***Curso de Direito Constitucional****. 15. ed. São Paulo: Saraiva Educação, 2020.*

*MONTEIRO, Renato Leite****. Desafios para a efetivação do direito à explicação na Lei Geral de Proteção de Dados do Brasil.*** *2021. 383 f. Tese (Doutorado em Direito Comercial) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021.*

PARENTONI, Leonardo. ***Compartilhamento de Dados Pessoais e a Figura do Controlador (Personal Data Sharing and the Role of the Data Controller)****. 2021. Disponível em https://www.researchgate.net/publication/351073596_Compartilhamento_de_Dados_Pessoais_e_a_Figura_do_Controlador_Personal_Data_Sharing_and_the_Role_of_the_Data_Controller. Access in: 24 dez. 2024.*

PELT, Eder van. ***Sujeito de direito digital:*** *a nova governamentalidade do sujeito na era digital. Rio de Janeiro: Telha, 2024.*

PROVOST, Foster; FAWCETT, Tom. ***Data Science for Business:*** *What You Need to Know About Data Mining and Data-Analytic Thinking. Sebastopol: O'Reilly, 2013.*

RODOTÀ, Stefano. ***A vida na sociedade da vigilância:*** *a privacidade hoje. Org. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.*

SANDEL, Michael. ***Justiça:*** *o que é fazer a coisa certa. Tradução de Heloísa Matias e Maria Alice Máximo. 40. ed. Rio de Janeiro: Civilização Brasileira, 2024.*

SARMENTO, Daniel. ***Dignidade da pessoa humana:*** *conteúdo, trajetórias e metodologia. Belo Horizonte: Fórum, 2016.*

WARREN, Samuel D.; BRANDEIS, Louis D. ***The Right to Privacy****. Harvard Law Review, v. 4, n. 5, p. 193–220, 1890. Available at: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. Access in: 23 dez. 2024.*

ZUBOFF, Shoshana. ***A era do capitalismo de vigilância:*** *a luta por um futuro humano na nova fronteira do poder. Nova York: Perseus Books, 2019.*