SPECIAL STRICT CIVIL LIABILITY IN BRAZIL'S GENERAL DATA PROTECTION LAW

Rafael de Freitas Valle Dresch [*]
José Luiz de Moura Faleiros Júnior [**]

Abstract: This research is focused on the interaction between data protection regulation and civil liability in Brazil, focusing on the General Data Protection Law (LGPD). As technology evolves rapidly, the LGPD addresses new risks and vulnerabilities tied to personal data processing. Drawing on the European GDPR and the Brazilian Consumer Protection Code, we argue that the LGPD introduces a special strict civil liability regime for data controllers and operators. Although some scholars argue for a fault-based approach, our hypothesis contends that the Act's strict liability standard, grounded in the defect theory and a reversable burden of proof, ensures stronger protection for data subjects. By using strict liability in tandem with a plethora of safeguarding principles, the law compels courts to focus on the existence of harm and irregular data practices rather than on explicit fault. This approach streamlines litigation while motivating thorough compliance. By emphasizing governance, transparency, and prevention, the LGPD compels organizations to adopt proactive data security and accountability measures. Its principles enshrine fundamental rights, such as privacy and autonomy, while encouraging collaborative risk management. Mandates for compliance programs, technical safeguards, and rapid incident notification nurture a culture of responsible data use so that the shift toward strict liability deters harmful practices by linking financial and reputational risks to suboptimal data handling. Thus, we conclude that the special strict civil liability regime functions as both a deterrent and a means of redress, reinforcing the legal foundation of digital rights which in turn adapts to evolving technologies.

Keywords: Data Protection Law; LGPD; Strict Liability; Personal Data; Privacy.

INTRODUCTION

Throughout the 20th century, remarkable phenomena were observed in the maturation of technological usage across a broad range of human activities. Indeed, one might speak of a society rooted in informational dynamism which, in concert with the process of globalization, gave rise to new archetypes of human relations.

Beginning in the 1960s, rapid advances in computing power and the

[*] Associate Professor at the Federal University of Rio Grande do Sul, Rio Grande do Sul, Brazil. Ph.D, Pontfical Catholic University of Rio Grande do Sul, Rio Grande do Sul, Brazil. Email: rafael.dresch@ufrgs.br /ORCID iD: https://orcid.org/0000-0001-5534-567X

[**] Ph.D, University of São Paulo, Brazil. Email: josefaleirosjr@outlook.com / ORCID iD: https://orcid.org/0000-0002-0192-2336

growing accessibility of new technologies permeated human endeavors, becoming ever more indispensable for performing tasks of all kinds. This led to the collection of a colossal volume of information, eventually giving rise to what is now known as Big Data.

Because technology evolves at a pace that is out of sync with the State's ability to legislate effectively for new contingencies, concerns grew about the volume of data collected and—most notably—about the ways in which large corporations handle such data to operate within this emerging market. Consequently, a global trend soon emerged to regulate data-related operations and oversight mechanisms.

Regulatory frameworks began to be introduced worldwide. In Brazil, the Consumer Protection Code (Law No. 8,078 of September 11, 1990) had already established certain protections for consumer relations, but the first major legislation specifically directed at internet regulation was Law No. 12,965 of April 23, 2014 (known as the *Marco Civil da Internet*, or Internet Civil Framework), followed by Decree No. 8,771/2016, which provided further details to it. In the wake of the European General Data Protection Regulation (GDPR), Brazil enacted Law No. 13,709 of August 14, 2018 (the General Data Protection Law, LGPD), later amended by other laws.

As one might have anticipated so fat, civil liability remains a perennial concern in legislation of this sort, engendering manifold controversies that call for a meticulous examination of the statutory frameworks enacted by lawmakers to illuminate the theoretical foundations of accountability for those subject to the new regulatory regime.

Since the enactment of the LGPD, numerous doctrinal and jurisprudential debates have arisen concerning the legal nature of the civil liability regime set forth in the law. Some authors argue that it is a fault-based regime, while others advocate for strict (objective) civil liability. Still others, examining the statute's guiding principles, maintain that it is actually a specialized model founded on presumed fault. This research aims to demonstrate that, due to the clear influence of the Consumer Protection Code (CDC) on how each provision regarding civil liability is structured in the LGPD, one can indeed speak of a special regime of strict (objective) civil liability. This regime stems from the defect identified via the irregular processing of data, as well as from the connection between Articles 42, 44, and 46, sole paragraph, of the LGPD. The study also explains why a fault-based regime is less preferable and, in confirming its research hypothesis, proposes an interpretative framework for the liability regime established in the law.

In this context, the central research question explored here involves assessing whether the provisions of these laws—particularly the LGPD—are sufficient to facilitate the resolution of conflicts arising from improper data collection, processing, and storage, and whether the legislator's proposed

framework is suitable for determining civil liability in potential violations.

The hypothesis advanced here aligns with the need to establish robust guidelines for implementing the personal data protection policies set forth in the legislation, primarily to prevent lawsuits and liabilities—especially in light of the recognition of personal data protection as a fundamental right and a contemporary expression of a core element of individual personality.

This study employs a historical-sociological approach, combined with bibliographical and doctrinal analysis. The concluding remarks aim to provide a more precise understanding of the issues raised, in light of the reflections presented.

I. RATIONALES FOR THE LEGAL SAFEGUARDING OF PERSONAL DATA

Scholars have long persistently emphasized the imperative for more profound theoretical exploration into the legal ramifications of information[1]. As sociological thought matured and metamorphosed—revealing the contours of an informationally driven society, subsequently christened the "network society"[2]—the foundational modalities of human interaction were recalibrated in response to newly emerging instruments and techniques[3].

In this context, humanity gradually abandoned the rudimentary conditions characteristic of antecedent epochs, thereby inaugurating a post-industrial societal model. Here, the transformative potential of information technology, operative at individual, organizational, and societal tiers, began to eclipse the surveillance concerns initially articulated in the literature (not least by George Orwell[4]). This evolution, in turn, dissipated the initial haze of visionary yet uncritical enthusiasm that had accompanied the genesis of this paradigm. Concurrently, the concept of surveillance expanded beyond its classical confines to encompass three realms: (i) physical; (ii) psychological; and (iii) data-based (dataveillance).

Nevertheless, Ian Lloyd observes that, with the capability to digitize any form of information, the boundaries between different types of surveillance are disappearing[5]. Indeed, this phenomenon springs from the extraordinary capacity for informational personalization, emerging from the nexus between data and a specific individual. Once accessible data permit inferences about

---

[1] Duff, Alistair A. *Information Society Studies*. London: Routledge, 2000, 99.

[2] Van Dijk, Jan. *The Network Society.* 3rd ed. London: Sage Publications, 2012, 6-11.

[3] Català, Pierre. "Ebauche d'une Théorie Juridique de l'Information." *Informatica e Diritto*, Naples, IX (January/April 1983), 20.

[4] Orwell, George. *Nineteen Eighty-Four*. New York: Penguin/Signet Classics, 1961, 3.

[5] Lloyd, Ian J. *Information Technology Law*. 6th ed. New York/Oxford: Oxford University Press, 2011, 5.

that individual's characteristics or behaviors—be it through legal determinants such as one's civil name or domicile, or through personal disclosures like consumer habits, expressed viewpoints, and geolocation—the landscape of surveillance inevitably broadens[6].

Against this backdrop, one finds an environment wherein social norms of behavior are generated and self-produced, underscoring that privacy is safeguarded across all spheres of private law. Yet, as is frequently the case, the grounds used to justify such protections differ, and these safeguards are by no means absolute[7]. Certain domains afford possibilities for restrictive inferences that impinge upon personal autonomy.

Here, it is apt to foreground the seminal 1890 study by Samuel Warren and Louis Brandeis, which examined the very existence of a "right to privacy"—an inquiry that later gained substantial doctrinal prominence, particularly in relation to the indispensable protection of fundamental rights.

Envisioning personal data protection as a "facet" of the fundamental right to privacy reveals the necessity of maintaining robust standards to guard against and remedy any violations visited upon this vital dimension of human personality.

This ambition to "strike a balance among various values—ranging from the reverberations of technology's role in processing personal data, and its implications for free personal development, to its utility in the marketplace"—highlights a distinctly 'negative' dimension concerning the perils that future technologies may pose. Such a perspective aligns with the viewpoint of thinkers espousing a "technological dystopia," among them Hans Jonas[8], Martin Heidegger[9], and Herbert Marcuse[10]. Yet subsequent theoretical developments coalesced into what Hans Achterhuis dubbed "philosophy of technology," heralding the so-called 'empirical turn'[11] from technique to technology. Within the specific context of safeguarding the free development of one's personality, theorists have posited that data protection must be construed as an autonomous subset of personality rights[12]—distinct

---

[6] Brzezinski, Zbigniew K. *Between Two Ages: America's Role in the Technetronic Era.* New York: Viking Press, 1971, 11.

[7] Westin, Alan F. *Information Technology in a Democracy*. Cambridge: Harvard University Press, 1971, 40-41.

[8] Jonas, Hans. *Frontiere della Vita, Frontiere della Tecnica*. Translated by Giovanna Bettini; edited by Vallori Rasini. Bologna: Il Mulino, 2011.

[9] Heidegger, Martin. *The Question Concerning Technology, and Other Essays*. Translated by William Lovitt. New York: Harper Perennial, 2013.

[10] Marcuse, Herbert. *One-Dimensional Man: Studies in the Ideology of Advanced Industrial Society.* Boston: Beacon, 1964.

[11] Achterhuis, Hans. Introduction: American Philosophers of Technology. In *American Philosophy of Technology: The Empirical Turn*, edited by Hans Achterhuis, translated by Robert P. Crease. Indianapolis: Indiana University Press, 2001, 1-10.

[12] Brüggemeier, Gert, Aurelia Colombi Ciacchi, and Patrick O'Callaghan. "A Common

from the fundamental right to privacy, which operates as a negative liberty[13].

This issue has attained such significance that, while legal doctrine had long endorsed recognizing personal data protection as a fundamental right, the Brazilian National Congress ultimately formalized this status through Constitutional Amendment No. 115/2022, which incorporated personal data protection into the roster of rights and guarantees under Article 5 of the Constitution[14]. The amendment further establishes that legislative authority over data-protection issues resides exclusively with the Federal Government.

Civil liability operates as a cornerstone in safeguarding personal data precisely because it provides a legal mechanism through which individuals can seek redress when their data privacy rights are infringed. In contrast to purely administrative or criminal sanctions, which primarily serve punitive or regulatory objectives, civil liability foregrounds the interests of the injured parties by allowing them to claim compensation. This remedial focus ensures that the consequences of unlawful or negligent data processing are not merely addressed in the abstract, but rather directly mitigated for those who suffer harm. By holding data controllers or processors financially accountable, civil liability compels these actors to internalize the costs of noncompliance—thereby incentivizing them to adopt robust data protection policies and safeguards.

Moreover, civil liability wields a potent deterrent effect[15] in the realm of personal data protection. A clearly delineated liability framework signals to organizations and public bodies that lax standards, negligent handling, or willful misuse of data can entail substantial legal and financial repercussions. This threat of liability operates as a catalyst for the implementation of more stringent data security measures, employee training, and compliance protocols. In effect, it elevates data protection from a peripheral consideration

---

Core of Personality Protection." In *Personality Rights in European Tort Law*, edited by Gert Brüggemeier, Aurelia Colombi Ciacchi, and Patrick O'Callaghan. Cambridge: Cambridge University Press, 2010, 567-569.

[13] In fact, "Data is inherently both subjective and incomplete, rather than objective and determinant. Without being filtered and theoretically-driven, mere data only produces a meaningless sea of correlations and must be simplified in order to be understood. This act of simplification (and aggregation), like legal interpretation, requires theory. Even the very act of deciding what data to gather in the first place—what to measure and observe, when and how—necessitates a theory". Devins, Caryn, Teppo Felin, Stuart Fauffman, and Roger Koppl. "The Law and Big Data." *Cornell Journal of Law and Public Policy* 27, no. 2 (January/April 2017): 357–413, 372.

[14] Sarlet, Ingo Wolfgang. "Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada." *Direitos Fundamentais & Justiça* 14, no. 42 (January/June 2020): 179–218.

[15] Dresch, Rafael de Freitas Valle. *Fundamentos do Direito Privado: Uma Teoria da Justiça e da Dignidade Humana*. 2nd ed. Rio de Janeiro, 2019, 74-76.

to a paramount corporate and institutional priority, reducing the risk of breaches, unauthorized disclosures, and other privacy-violative practices.

Another vital aspect of civil liability in data protection lies in its capacity to adapt to evolving technological and societal conditions[16]. As innovations in big data analytics, artificial intelligence, and digital platforms transform the nature and scale of personal data processing, civil liability doctrines can be calibrated—through legislative updates or judicial interpretation—to address novel harms[17]. This adaptability is particularly relevant in cross-border data flows, where multiple jurisdictions' legal regimes can overlap, and in contexts where intangible yet significant injuries (such as reputational damage or identity theft) call for clear, enforceable standards.

Lastly, civil liability reinforces the status of data protection as a fundamental right by concretizing the principle that violations should not remain solely within the realm of regulatory enforcement. By empowering data subjects to bring private actions against organizations, this legal institute fosters a more participatory and rights-driven culture of accountability. It affirms that personal data protection is not a theoretical guarantee, but one that, when violated, entitles individuals to tangible legal remedies. As a result, civil liability contributes decisively to the broader architecture of data protection law, embedding privacy norms into the very fabric of legal and social relations.

II. RISKS AND CONTINGENCIES: ESSENTIAL PARAMETERS FOR DELIMITING A NEW PROTECTIVE SPHERE OF PRIVACY

Legislatures worldwide have increasingly recognized the emergence of novel risks within the information society, prompting them to develop guiding principles for safeguarding personal data. This legislative endeavor aims to ensure the *effective* deployment of protective instruments capable of mitigating the adverse consequences flowing from modern data-centric practices[18]. As technology permeates diverse spheres of social interaction, the legal system can no longer remain confined to rigid doctrines. It must instead adapt to prevent a purely technocratic outlook from overshadowing the ethical imperative to protect individuals. By adopting such measures, the law

[16] Dresch, Rafael de Freitas Valle, and José Luiz de Moura Faleiros Júnior. "Reflexões sobre a Responsabilidade Civil na Lei Geral de Proteção de Dados (Lei nº 13.709/2018)." In *Responsabilidade Civil: Novos Riscos*, edited by Nelson Rosenvald, Rafael de Freitas Valle Dresch, and Tula Wesendonck. Indaiatuba: Foco, 2019, 67-71.

[17] Miragem, Bruno. "A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor." Revista dos Tribunais 1009 (November 2019): 173–222.

[18] Faleiros Júnior, José Luiz de Moura. "Accountability e Devida Diligência como Vetores da Governança Corporativa nos Mercados Ricos em Dados." *Revista Semestral de Direito Empresarial* 26 (2020): 183–211.

not only curbs the nihilism of unregulated innovation but also directs technological progress toward a more responsible path.

In this context, the legal framework surrounding data protection takes on heightened importance, particularly when it comes to civil liability. This legal institute functions as a linchpin for redressing harm caused by improper or negligent data processing. It dissuades potential wrongdoers by shifting the costs of data-related harm back onto those who fail to uphold adequate standards. As a result, civil liability not only provides compensation to injured parties but also sets a clear benchmark, compelling data controllers and processors to enact strong preventive measures and adhere to sound ethical practices.

Yet the necessity for fresh legal "filters" is undeniable. Digital technology operates at a pace far outstripping conventional legislative responsiveness. Hence, lawmakers must go beyond the traditional scope of civil liability in order to accommodate new categories of harm and to integrate broader principles of prevention[19]. This dynamic and proactive posture can, in turn, strengthen legal protections against emergent privacy violations and address the intricate power imbalances that characterize the data economy.

A. Personality protection on the Internet

The evolution of digital technology has led some scholars to suggest that a person's identity—encompassing thoughts, behaviors, preferences, and communications—can now manifest itself virtually as an "electronic body."[20] Stefano Rodotà's observations on the creation of this digital self underscore the necessity of rethinking privacy protections that transcend older, more territorial notions of individual rights. In the online realm, new attributes of personality arise, demanding legal recognition and robust safeguards[21].

These principles apply with special force to the digital environment. Sophisticated data-harvesting techniques—particularly those powered by algorithms—give platform operators the ability to analyze and monetize user behavior at unprecedented scales. Civil liability thus emerges as a counterweight against such expansive monitoring. By holding companies accountable for abusive data practices, it helps preserve an individual's

[19] Martins, Guilherme Magalhães, and José Luiz de Moura Faleiros Júnior. "Compliance Digital e Responsabilidade Civil na Lei Geral de Proteção de Dados." In *Responsabilidade Civil e Novas Tecnologias*, 2nd ed., edited by Guilherme Magalhães Martins, Nelson Rosenvald, and José Luiz de Moura Faleiros Júnior. Indaiatuba: Foco, 2023, p. 362-370.

[20] Faleiros Júnior, José Luiz de Moura, and Cristiano Colombo. "A Tutela Jurídica do Corpo Eletrônico: Alguns Conceitos Introdutórios." In *Tutela Jurídica do Corpo Eletrônico: Novos Desafios ao Direito Digital*, edited by Cristiano Colombo, Wilson Engelmann, and José Luiz de Moura Faleiros Júnior. Indaiatuba: Foco, 2022, 3-32.

[21] Rodotà, Stefano. *Intervista su Privacy e Libertà*. Rome/Bari: Laterza, 2005, 120.

autonomy, dignity, and free development of personality in the virtual space.

Aurelia Tamò-Larrieux, for instance, emphasizes how personal data processing has become a keystone of modern economic and social activity. Enterprises harness large datasets and advanced profiling tools to anticipate consumer behavior—even before users themselves are fully aware of their preferences[22]. This phenomenon highlights just how vital civil liability can be: once enshrined in legislation, it compels corporations to consider the potential harms of data exploitation and, correspondingly, to internalize the costs of mishandling user information.

It is, however, not only private entities that collect data in vast quantities. States, too, wield expansive surveillance capabilities. This dual, overlapping scrutiny by both government and industry places individuals in a precarious position. Civil liability, by offering private recourse to those whose data rights are violated, serves as an essential bulwark. It reaffirms that personal data cannot be exploited with impunity, injecting ethical standards into a sphere where information asymmetry and corporate or governmental might could otherwise dominate.

B. Self-determination and consent

The fast-paced digital ecosystem often leaves users vulnerable when it comes to granting consent. Many individuals unwittingly authorize extensive data processing or fail to grasp the ramifications of disclosures they make online. This setting paves the way for violations of consumer rights, the erosion of personal autonomy, and discriminatory or manipulative practices, all of which the LGPD aims to curtail. Indeed, the law explicitly cites *informational self-determination* and the *free development of personality* among its guiding tenets.

The notion of the *"glass consumer,"* introduced by Susanne Lace[23], underscores how the typical user becomes increasingly transparent, subjected to ceaseless monitoring by data-driven enterprises. Scholars like Zygmunt Bauman and David Lyon[24] have likewise explored how surveillance tools—once confined to narrower settings—now pervade daily life, ostensibly to deliver "security." Yet this expanded vigilance often engenders fresh risks, including the normalization of excessive data collection that undermines individual freedoms.

---

[22] Tamò-Larrieux, Aurelia. *Designing for Privacy and Its Legal Framework: Data Protection by Design and Default for the Internet of Things*. Basel: Springer, 2018, 3.

[23] Lace, Susanne. *The Glass Consumer: Life in a Surveillance Society*. Bristol: Policy Press, 2005, 5.

[24] Bauman, Zygmunt, and David Lyon. *Vigilância Líquida*. Translated by Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013, 95-96.

Given these challenges, consent stands as a nominal precondition for lawful data processing. The European GDPR references it extensively, requiring that it be freely given and informed. Brazilian law follows a similar route, demanding that consent be unequivocal and explicit. Civil liability connects to this concept by providing a remedy for individuals when consent is improperly obtained, misleadingly represented, or disregarded altogether. In an environment where consent can be devalued through asymmetrical power[25] relationships and obscure data policies, civil liability steps in to realign incentives: it holds data handlers answerable for any unlawful usage of personal information and protects the personhood of users who might otherwise be powerless in the face of complex digital platforms.

C. Security and governance

To cope with the rapidly evolving digital realm, legal systems increasingly emphasize preventive mechanisms alongside traditional modes of post-hoc compensation. Among these mechanisms is the insistence on robust governance structures—often manifested as *compliance* programs—within organizations that process personal data. The LGPD itself calls for effective *governance* in Articles 50 and 51, insisting that data controllers demonstrate unwavering commitment to risk assessment, the adoption of internal privacy policies, and thorough data oversight[26].

These governance practices are closely interwoven with civil liability. When companies fail to maintain the requisite security protocols, thereby breaching the expected standard of care, they risk incurring liability for any resulting harm. This dual emphasis—prevention via compliance and accountability through liability—seeks to mold a culture of safety. Instead of being relegated to an afterthought, data protection must become integral to every phase of business operations, from system design to customer relations.

---

[25] Regarding the topic, it is important to highlight the role of Behavioral Economics, which, based on the limited rationality of the agent, justifies the need for regulation of market activities. This need is particularly significant in the virtual environment, dominated by algorithms and the massive collection of data, which poses significant risks. On this subject, see the following references: Thaler, Richard H. "Mental Accounting Matters." *Journal of Behavioral Decision Making* 12, no. 3 (July 1999): 183–206; Ariely, Dan, George Loewenstein, and Drazen Prelec. "Coherent Arbitrariness: Stable Demand Curves Without Stable Preferences." *Quarterly Journal of Economics* 118, no. 1 (February 2003): 73–106; Samson, Alain, and Benjamin Voyer. "Emergency Purchasing Situations: Implications for Consumer Decision-Making." *Journal of Economic Psychology* 44, no. 1 (September 2014): 21–33.

[26] Peroli, Kelvin, and José Luiz de Moura Faleiros Júnior. "Artigo 50." In *Comentários à Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018)*, 2nd ed., edited by Guilherme Magalhães Martins, João Victor Rozatti Longhi, and José Luiz de Moura Faleiros Júnior. Indaiatuba: Foco, 2024, 496.

In many jurisdictions, data protection authorities encourage industry-specific "codes of practice" that facilitate more flexible application of statutory obligations. The idea is to unify high-level legislative mandates with practical guidelines attuned to the realities of each sector[27]. Brazil has likewise leaned on international standards—such as ISO/IEC 27002—to establish best practices in information security, dovetailing with LGPD requirements that *data controllers* and *processors* adopt suitable technical and administrative precautions to protect personal data[28]. Ultimately, civil liability undergirds these efforts by reinforcing the notion that noncompliance carries tangible legal and financial consequences.

As data collection expands and becomes ever more sophisticated, civil liability serves as a vital legal institute to deter misconduct and secure redress for those harmed. It fills the gaps that inevitably emerge when legislation and policy lag behind technical innovation, ensuring that the overarching right to privacy is not merely formal but truly actionable. By integrating proactive governance with the corrective force of liability, the law enhances both individual rights and societal trust in the digital environment, guiding technological progress in a direction that respects human dignity and autonomy.

III. THE SPECIAL STRICT CIVIL LIABILITY REGIME UNDER THE LGPD

In a manner akin to the debates spurred by Brazil's Internet Civil Framework (Law No. 12,965 of April 23, 2014)—which prompted intense scholarly and judicial deliberations over the liability of service providers for user-generated content[29]—the General Data Protection Law (LGPD) has

---

[27] Silverman, Michal G. *Compliance Management for Public, Private, or Nonprofit Organizations*. New York: McGraw Hill, 2008, 206.

[28] Faleiros Júnior, José Luiz de Moura. "Compliance Digital y Gobernanza: El Diálogo Interdisciplinario en la Era Digital." *Juris Studia* 1 (2024): 145–158.

[29] On December 4, 2024, the Plenary of Brazil's Supreme Federal Court (STF) resumed deliberations on the constitutionality of Article 19 of the Marco Civil da Internet (Law 12.965/2014) and the potential civil liability of major technology companies for third-party content. Minister Dias Toffoli, the rapporteur for one of the cases under review, continued presenting his vote, which he had begun on November 28. Although he has not yet concluded, Toffoli has indicated that he considers Article 19 unconstitutional. This article stipulates that digital platforms and providers can only be held civilly liable if they fail to comply with a judicial order to remove content deemed "infringing." Toffoli argues that this provision effectively grants platforms immunity, as they are only held accountable upon non-compliance with a court order. He suggests that platform liability should be governed by Article 21 of the Marco Civil, which allows for liability following extrajudicial notification, though this is currently limited to cases involving the dissemination of sexual content. The STF is examining two cases with general repercussions: Extraordinary Appeal 1.037.396,

likewise sparked questions regarding how operators and controllers may be held accountable for data-processing violations. Given the law's foundational principles and the realities of modern data-intensive activities, these uncertainties demand a thoughtful and systematic evaluation.

Heavily influenced by the EU General Data Protection Regulation (GDPR)[30], the LGPD enumerates in Article 2 several core values: respect for privacy, informational self-determination, freedom of expression and opinion, protection of intimacy, honor, and image, and the right to free personal development. It also highlights economic and technological development, free enterprise, fair competition, and consumer defense. By articulating these aims, the law underscores that "real conditions for developing core human values or capacities" must guide legal protections for personal data. Consequently, Article 6 lays out foundational principles—purpose, adequacy, necessity, free access, data quality, transparency, and non-discrimination—all of which shape the statutory framework for civil liability.

A. Joint and several liability for controllers and operators

Article 42 of the LGPD serves as the fulcrum of its liability provisions:

> Art. 42. The controller or the operator who, through data processing activities, causes pecuniary or non-pecuniary harm (whether to an individual or a collective) in violation of data protection legislation shall be required to provide compensation.
> § 1. To ensure effective reparation for the data subject:
> (i) The operator is jointly and severally liable for damages resulting from the processing if it fails to comply with data protection obligations or disregards the controller's lawful instructions—under which circumstances it is treated equivalently to a controller, except as provided in Article 43;

---

concerning the constitutionality of Article 19, and Extraordinary Appeal 1.057.258, which addresses the responsibility of internet application providers for user-generated content and the possibility of removing illicit content based on extrajudicial notifications. Additionally, the court is considering ADPF 403, which debates whether judicial decisions can block applications or if such interventions infringe upon freedom of expression and communication rights. For mor details, cf. Brazil. Supremo Tribunal Federal. "Marco Civil da Internet: Relator Considera Inconstitucional Exigência de Ordem Judicial para Retirada de Conteúdo." *STF Notícias*, December 4, 2024. Accessed January 23, 2025. https://noticias.stf.jus.br/postsnoticias/marco-civil-da-internet-relator-considera-inconstitucional-exigencia-de-ordem-judicial-para-retirada-de-conteudo/.

[30] Bennett, Colin J. "Convergence Revisited: Toward a Global Policy for Protection of Personal Data?" In *Technology and Privacy: The New Landscape*, edited by Philip E. Agre and Marc Rotenberg. Cambridge: The MIT Press, 1997, 114-115.

> (ii) Controllers who were directly involved in the damaging data processing shall also be jointly and severally liable, barring the exclusions contained in Article 43.
> § 2. In civil proceedings, the judge may shift the burden of proof in favor of the data subject when the allegations appear credible, when the data subject demonstrates particular difficulty in producing evidence, or when such evidentiary production would be unduly burdensome.
> § 3. Collective claims for damages arising under the *caput* may be litigated collectively, consistent with relevant legislation.
> § 4. Any party who compensates the data subject has a right of recourse against other liable parties, in proportion to each party's involvement in the harmful conduct.

A preliminary observation is the interrelationship between controllers and operators in bearing potential liability. Article 5(VI) designates the controller as "the individual or legal entity, whether public or private, responsible for deciding how personal data are processed," while Article 5(VII) defines the operator as "the individual or legal entity, whether public or private, that processes personal data on behalf of the controller." The statute collectively labels both as "processing agents" (Article 5, IX).

Both the Brazilian General Data Protection Law (LGPD) and the Consumer Protection Code (Law No. 8,078/1990, CDC)[31] stem from a common goal of safeguarding individuals against abuses that arise in the course of commercial or data-processing activities[32]. While the CDC focuses on preventing and remediating unfair consumer practices, the LGPD addresses the protection of personal data in increasingly technology-driven relationships. Nevertheless, each law seeks to uphold individuals' rights by promoting equitable treatment, transparency, and accountability for entities—be they businesses or data-processing agents—that hold superior bargaining power or specialized knowledge[33].

Tellingly, the statute does not require proof of fault in order to hold either entity liable, thus evidencing an objective liability principle founded on risk, in line with Article 927 of the Brazilian Civil Code. Reinforcing the data subject's position, Article 42(§2) allows for a reversal of the burden of proof.

---

[31] Cravo, Daniela Copetti, and Marcela Joelsons. "A importância do CDC no tratamento de dados pessoais de consumidores no contexto da pandemia e de *vacatio legis* da LGPD." *Revista de Direito do Consumidor* 131 (September/October 2020): 111–145..

[32] Miragem, Bruno. "A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor." *Revista dos Tribunais* 1009 (November 2019): 173–222.

[33] Dresch, Rafael de Freitas Valle, and Lílian Brandt Stein. "A responsabilidade civil como mecanismo de incentivo à observância do direito fundamental à proteção de dados: uma análise da interpretação do art. 42 e seguintes da LGPD." *Revista de Direito da Responsabilidade* 5 (2023): 978–980.

Although not a novel mechanism—given its presence in the Consumer Protection Code and the 2015 Code of Civil Procedure—this explicit reference in the LGPD underscores the law's intent to safeguard individuals whose data are mishandled.

Article 42(§1) further clarifies that (i) controllers typically bear broad authority over data processing, and thus broad responsibility; (ii) controllers must issue lawful instructions to operators, who are likewise bound by LGPD obligations; and (iii) if operators deviate from these requirements or directions, they may face joint and several liability.

B. Exclusions of liability

Article 43 specifies the limited circumstances in which processing agents may avoid liability:

> Art. 43. Processing agents are not liable if they prove:
> (i) that they did not perform the personal data processing attributed to them;
> (ii) that, although they did carry out the attributed processing, there was no violation of data protection legislation; or
> (iii) that the harm arose solely from the data subject's actions or from a third party.

Clause (i) correlates with the duty of controllers to maintain processing records (Article 37), which—when coupled with the potential reversal of proof—helps clarify who engaged in data processing. Clause (ii) references a "regular exercise of rights," akin to the principle in Article 188(I) of the Civil Code, and must be read alongside the LGPD's broader stipulations, including documentation requirements and the best practices outlined in Article 50. Clause (iii) comprises classic exculpatory scenarios such as the exclusive fault of the victim (the data subject) or a third party[34].

One frequently noted omission is the absence of explicit liability for the data protection officer (*encarregado*). This individual plays a pivotal role in preventing harmful incidents by advising both controllers and operators. If they were to issue incorrect directives causing damage, liability could conceivably be shifted to them under Article 43(iii), although supplementary legal provisions might be required to formalize such a claim[35].

---

[34] Dresch, Rafael de Freitas Valle, and Gustavo da Silva Melo. "Artigo 43." In *Comentários à Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018)*, 2nd ed., edited by Guilherme Magalhães Martins, João Victor Rozatti Longhi, and José Luiz de Moura Faleiros Júnior. Indaiatuba: Foco, 2024, 433-436.

[35] Queiroz, Renata Capriolli Zocatelli. *Encarregado de Proteção de Dados Pessoais – DPO: Regulamentação e Responsabilidade Civil*. São Paulo: Quartier Latin, 2022, 91-95.

C. General duty of security and data breaches

The Brazilian General Data Protection Law (LGPD) does not provide a direct legal definition for the term "data breach," which is often referred to in Brazil simply as *vazamento* (or "leak") when reported by the media. Rather, the LGPD uses the phrase "security incident" to cover a range of adverse events involving personal data, including unauthorized access, data destruction, loss, or alteration. These events can stem from cyberattacks, such as ransomware, or from internal vulnerabilities—often avoidable or foreseeable—that betray deficient security measures and governance policies within organizations[36].

Article 46 dovetails with Article 50 to establish compliance obligations—mechanisms that extend beyond a superficial reading of statutory text. While the LGPD unambiguously endorses an objective civil liability regime for processing agents, it also underscores a new baseline for addressing *risk* as a central element of objective theory. The linchpin here is the general duty of security, which elevates the user's "legitimate expectations" of data safety to a paramount concern in any discussion of "defects" in data collection, processing, or storage.

Unlike the European GDPR, which offers a precise definition of "personal data breach," the LGPD leaves this concept somewhat implicit. Article 46 of the Brazilian law requires *agents of data processing*—both controllers and operators—to employ technical and administrative safeguards that protect personal data from unauthorized access and from accidental or unlawful circumstances. Meanwhile, Article 48 imposes a notification duty on controllers in the event of a "security incident." In an effort to bridge the definitional gap, Brazil's National Data Protection Authority (ANPD) has issued guidance describing a "security incident" as *any confirmed adverse event involving a breach of personal data security*, encompassing unauthorized, accidental, or unlawful access resulting in the destruction, loss, alteration, or disclosure of personal data[37].

By embedding compliance into its legal structure, the LGPD encourages controllers and operators to adopt sound internal policies, practical safeguards, security procedures, data-minimization approaches,

---

[36] Faleiros Júnior, José Luiz de Moura. "O Que É, Afinal, um Vazamento de Dados?" *Migalhas de Proteção de Dados*, March 10, 2022. Accessed January 23, 2025. https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/351388/o-que-e-afinal-um-vazamento-de-dados

[37] Brazil. Autoridade Nacional de Proteção de Dados (ANPD). "Incidente de Segurança." Accessed January 23, 2025. https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca.

anonymization measures, and employee training programs. Each of these elements serves to prevent wrongdoing and reduce potential damages—and to demonstrate that the entity acted diligently. In line with emerging international commentaries, this requirement for demonstrable good practices influences how authorities, courts, and even the public at large gauge accountability[38].

Ultimately, civil liability acts as a vital legal backbone in this framework: it incentivizes data handlers to treat security and governance as integral facets of daily operations and not merely optional add-ons. By ensuring that financial or reputational costs attach to noncompliance, the LGPD closes the gap between legal theory and concrete risk management in the data economy.

Notwithstanding the lack of a formal statutory definition for data breaches, the LGPD embeds prevention as a core principle. Article 6(VIII) enshrines the principle of prevention, mandating proactive measures to avert harm to data subjects. In practice, this translates into an expectation that organizations maintain robust security systems—consistent with Articles 44 and 46—that address both technical and administrative vulnerabilities[39]. This emphasis on prevention is reinforced by the statutory requirement of *compliance,* coupled with standards of good faith and transparency (Articles 6, *caput*, and 6(VI)), ensuring that data subjects receive timely and adequate information about how their personal data are handled and how security incidents are managed.

Under the LGPD, civil liability for damage resulting from security incidents or "data leaks" does not hinge on demonstrating fault. Instead, the law's provisions—especially Articles 42, 44, and 46—point to a *strict (objective) liability* regime[40], where liability arises upon the mere showing of harm and an irregularity in the data processing activity. In other words, if a breach or security incident occurs and causes economic, moral, or collective damage, data controllers and operators may be held responsible, regardless of any proven negligence or intent. This approach is well-suited to the fast-paced and complex nature of data processing, wherein users often cannot

---

[38] Rosenvald, Nelson, and José Luiz de Moura Faleiros Júnior. "Accountability e Mitigação da Responsabilidade Civil na Lei Geral de Proteção de Dados Pessoais." In *Compliance e Políticas de Proteção de Dados*, edited by Ana Frazão and Ricardo Villas Bôas Cueva. São Paulo: Thomson Reuters Brasil, 2021, 771-808.

[39] Dresch, Rafael de Freitas Valle, and Lílian Brandt Stein. "A responsabilidade civil como mecanismo de incentivo à observância do direito fundamental à proteção de dados: uma análise da interpretação do art. 42 e seguintes da LGPD." *Revista de Direito da Responsabilidade* 5 (2023): 978–980.

[40] Dresch, Rafael de Freitas Valle, and José Luiz de Moura Faleiros Júnior. "Reflexões sobre a Responsabilidade Civil na Lei Geral de Proteção de Dados (Lei nº 13.709/2018)." In *Responsabilidade Civil: Novos Riscos*, edited by Nelson Rosenvald, Rafael de Freitas Valle Dresch, and Tula Wesendonck. Indaiatuba: Foco, 2019, 88-89.

establish the precise fault of a data handler. By removing the burden of proving negligence, the LGPD ensures that organizations internalize the costs of substandard data protection and are incentivized to adopt best practices.

The LGPD's reliance on strict liability in cases of security incidents underscores the law's commitment to robust data protection and preventive measures. As ransomware attacks and other cyberthreats become increasingly common, organizations can no longer hide behind claims of ignorance or blame technical complexities for breaches[41]. By imposing an objective standard, the LGPD places the onus on companies to build effective and transparent security protocols. This approach not only promotes the rights of data subjects but also fosters a culture of proactive risk management, ultimately raising compliance standards across the board and strengthening the overall data protection landscape in Brazil.

D. Divergent doctrinal perspectives: fault versus strict liability

Despite widespread agreement that Article 42 (and related provisions) sets forth an objective civil liability regime, certain scholars have proposed fault-based interpretations. Gustavo Tepedino, Aline de Miranda Valverde Terra and Gisela Sampaio da Cruz Guedes, for instance, argue that because the LGPD defines numerous duties of conduct for processing agents, the law introduces a species of "normative fault."[42] In their view, agents who breach these duties act with a legally recognized form of culpability[43], making the liability regime effectively fault-based[44].

Others, such as Bernardo Grossi, advance the notion of "relative presumed fault,"[45] suggesting that statutory obligations place the burden on

---

[41] Dresch, Rafael de Freitas Valle, and Gustavo da Silva Melo. "O papel do operador no tratamento de dados: entre deveres e responsabilização" In *Compliance e Políticas de Proteção de Dados*, edited by Ana Frazão and Ricardo Villas Bôas Cueva. São Paulo: Thomson Reuters Brasil, 2021, 679–687.

[42] Tepedino, Gustavo, Aline de Miranda Valverde Terra, and Gisela Sampaio da Cruz Guedes. "Responsabilidade civil dos agentes de tratamento de dados" In *Compliance e Políticas de Proteção de Dados*, edited by Ana Frazão and Ricardo Villas Bôas Cueva. São Paulo: Thomson Reuters Brasil, 2021, 744–754.

[43] That's also Cícero Dantas Bisneto's point of view, cf. Dantas Bisneto, Cícero. "Reparação por danos morais pela violação à LGPD e ao RGPD: uma abordagem de direito comparado." *Civilistica.com* 9, no. 3 (2020): 1–23.

[44] Madalena, Juliano. "A Responsabilidade Civil Decorrente do Vazamento de Dados Pessoais." In *Lei Geral de Proteção de Dados: Aspectos Relevantes*, edited by Fabiano Menke and Rafael de Freitas Valle Dresch. Indaiatuba: Foco, 2021, 258.

[45] Grossi, Bernardo Menicucci. "Responsabilidade Civil na LGPD: A Culpa Presumida Relativa." *Migalhas de Responsabilidade Civil*, April 24, 2023. Accessed January 23, 2025. https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-

processing agents to prove their innocence of any wrongful act[46]. However, a close reading of the LGPD, considered in light of its guiding principles, definitions, and data-subject rights, appears to undercut these fault-centered approaches. Not only does the Act avoid explicit references to fault, but its systematic interpretation—particularly through the principle of accountability in Article 6(X)—reinforces the view that liability is premised on a risk-based, objective paradigm.

From a practical perspective, imposing a fault-based model would arguably dilute the LGPD's protective ethos by requiring data subjects to demonstrate the processor's wrongdoing or negligence—a task often complicated by informational asymmetries[47], especially when processing sensitive personal data[48]. By contrast, an objective regime aligns with the law's overarching purpose of ensuring tangible security and effective remedies[49], regardless of whether the agent's breach arises from willful misconduct, negligence, or mere operational failures. In this manner, according to Laura Schertel Mendes and Danilo Doneda[50], civil liability provides a cohesive and user-centric remedy, enabling data subjects to vindicate their rights even when they may lack technical expertise.

Some authors, such as Maria Celina Bodin de Moraes and João Quinelato de Queiroz[51], advocate for an even stricter approach to strict liability, which

civil/385155/responsabilidade-civil-na-lgpd-a-culpa-presumida-relativa.

[46] Grossi, Bernardo Menicucci. "A violação dos direitos de personalidade na LGPD: a problemática do dano moral *in re ipsa*" In *Direito, Tecnologia e Inovação, vol. 4: estudos de casos*, edited by Leonardo Parentoni. Belo Horizonte: Centro DTIBR, 2022, 117–119.

[47] Mulholland, Caitlin. "A LGPD e o Fundamento da Responsabilidade Civil dos Agentes de Tratamento de Dados Pessoais: Culpa ou Risco?" *Migalhas de Responsabilidade Civil*, June 30, 2020. Accessed January 23, 2025. https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais--culpa-ou-risco

[48] Mulholland, Caitlin. "Responsabilidade Civil por Danos Causados pela Violação de Dados Sensíveis e a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018)." In *Responsabilidade Civil e Novas Tecnologias*, 2nd ed., edited by Guilherme Magalhães Martins, Nelson Rosenvald, and José Luiz de Moura Faleiros Júnior. Indaiatuba: Foco, 2023, 109–124.

[49] Gondim, Glenda Gonçalves. "A Responsabilidade Civil no Uso Indevido dos Dados Pessoais." In *Responsabilidade Civil e Novas Tecnologias*, 2nd ed., edited by Guilherme Magalhães Martins, Nelson Rosenvald, and José Luiz de Moura Faleiros Júnior. Indaiatuba: Foco, 2023, 308.

[50] Mendes, Laura Schertel, and Danilo Doneda. "Reflexões Iniciais sobre a Nova Lei Geral de Proteção de Dados." *Revista de Direito do Consumidor* 120 (November/December 2018): 469–483.

[51] Bodin de Moraes, Maria Celina, and João Quinelato de Queiroz. "Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD." In *Cadernos Adenauer*, no. 3 (2019): 113–137. Rio de Janeiro: Fundação Konrad Adenauer.

they call proactive liability, based on the principle of *accountability* outlined in Article 6(X) of the LGPD. From the duties established—which include demonstrating the effectiveness of the measures adopted to comply with the law—the duty to indemnify would already arise, thereby reinforcing the effectiveness of the law's principles.

One striking resemblance between the LGPD and the CDC is the adoption of an objective (or strict) liability framework in certain contexts. Under the Consumer Protection Code, businesses can be held strictly liable for damages resulting from defective products or services, regardless of fault. Analogously, the LGPD, particularly in Articles 42 and 44, embraces a form of objective civil liability for data controllers and operators when personal data breaches or irregular processing activities harm data subjects. In both statutes, the burden often shifts to the defendant to demonstrate that no wrongdoing occurred or that an applicable exemption applies—reinforcing the protective ethos that underlies Brazilian consumer- and privacy-oriented legislation[52].

Just as the CDC requires suppliers to provide clear and adequate information about products and services, the LGPD demands transparency from data-processing agents regarding how they handle personal data. This requirement is integral to fostering trust, as both laws recognize that information asymmetry can place individuals at a disadvantage. Under the CDC, a lack of clear product disclosures or contract terms can invalidate certain business practices. Under the LGPD, insufficient clarity about data-processing policies can lead to administrative sanctions and civil liability, reflecting a parallel commitment to ensuring that individuals are fully informed before entering into a consumer or data-driven relationship.

The Consumer Protection Code and the LGPD both endorse a preventive approach aimed at mitigating harm before it occurs. Within the CDC, consumer protection agencies and courts often take proactive measures, such as injunctions, to halt dangerous or deceptive practices[53]. In a similar vein, the LGPD mandates that data controllers adopt technical and administrative precautions to safeguard personal data, thereby reducing the likelihood of breaches or unauthorized disclosures. This shared focus on prevention underscores the legislature's recognition that reactive measures alone are insufficient in complex consumer and data-processing environments.

Lastly, both statutes allow for the protection of collective interests

---

[52] Dresch, Rafael de Freitas Valle, and José Luiz de Moura Faleiros Júnior. "Reflexões sobre a Responsabilidade Civil na Lei Geral de Proteção de Dados (Lei nº 13.709/2018)." In *Responsabilidade Civil: Novos Riscos*, edited by Nelson Rosenvald, Rafael de Freitas Valle Dresch, and Tula Wesendonck. Indaiatuba: Foco, 2019, 88-89.

[53] Miragem, Bruno. "A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor." *Revista dos Tribunais* 1009 (November 2019): 173–222.

through collective or class actions. The CDC pioneered collective mechanisms to address widespread consumer harm, enabling consumer protection organizations and public authorities to pursue claims on behalf of affected individuals. The LGPD similarly contemplates collective lawsuits for data breaches or other violations that impact large groups of data subjects. In both frameworks, collective redress ensures that individuals are not left defenseless against well-resourced companies or data handlers, affirming the law's purpose of balancing power differentials and safeguarding broader societal interests.

E. Jurisprudential perspective (so far)

The *Superior Tribunal de Justiça* (STJ) has been progressively delineating the parameters of civil liability in cases involving data breaches and the misuse of personal information within the ambit of Brazil's LGPD. Through pivotal rulings, the court has endeavored to reconcile the principles of consumer protection, accountability, and data privacy, all while navigating the intricate interplay between newly instituted legal frameworks and entrenched doctrinal concepts. While these decisions constitute significant advancements in the application of the LGPD, they also expose latent inconsistencies and deficiencies in judicial reasoning, thereby highlighting opportunities for enhancing the protection of data subjects. Notably, the decision involving Eletropaulo, a public utility concessionaire subject to the State's civil liability provision under Article 37, §6º, of the Brazilian Constitution, alongside the LGPD, has garnered critical attention for its perceived inadequacies in addressing the unique legal regime applicable to such entities.

In *REsp No. 1.758.799 - MG*, the STJ adjudicated that the infringement of a consumer's right to be informed about the handling of their personal data triggers the presumption of moral damages, under the doctrine of *in re ipsa*. This ruling aligns with the LGPD's commitment to promoting transparency and ensuring accountability, thereby fortifying the rights of data subjects over their personal information[54]. Nonetheless, the reliance on the *in re ipsa* presumption has been criticized for its potential to oversimplify the multifaceted nature of assessing moral harm in data-related disputes[55]. Although this approach enhances consumer protection, it simultaneously raises concerns about the undue burden placed on data controllers, who may

[54] Brazil. Superior Tribunal de Justiça. *Recurso Especial No. 1.758.799 - MG*. Rapporteur: Ministra Nancy Andrighi. Brasília, 19 de novembro de 2019.

[55] Cardoso, João Victor Gontijo. "O Dano Moral 'In Re Ipsa' e o Tratamento Indevido de Dados sob o Prisma dos Julgados: REsp 1.758.799/MG e ADI 6387 MC-REF." *Revista IBERC* 4, no. 1 (January/April 2021): 133–153.

be held liable in the absence of concrete evidence of harm.

In *AREsp No. 2.130.619 - SP*, the STJ provided critical clarification by ruling that not all personal data qualify as sensitive under the LGPD and that moral damages cannot be presumed solely on account of a data breach. This decision illustrates the court's attempt to draw a distinct line between sensitive and non-sensitive data, acknowledging their differing levels of legal protection[56]. However, the judgment has sparked debates over whether requiring proof of harm undermines the LGPD's preventive and reparative objectives. Critics contend that shifting the evidentiary burden onto data subjects could discourage individuals from pursuing redress, particularly in instances where the consequences of data breaches are diffuse or challenging to quantify[57].

Conversely, *REsp No. 2.133.261 - SP* underscored the principle of accountability, mandating that data controllers adopt proactive measures to prevent harm in accordance with the LGPD's preventive ethos. This judgment exemplifies the court's recognition of the structural obligations incumbent upon data handlers[58]. Nevertheless, the absence of clear, standardized benchmarks for determining what constitutes sufficient proactive measures introduces a troubling degree of legal uncertainty. This ambiguity could result in inconsistent judicial interpretations, thereby complicating the efforts of data controllers striving to align their practices with both legislative and judicial expectations.

In *Recurso Especial No. 2.147.374 - SP*, the Superior Tribunal de Justiça (STJ) dealt with a case involving a data breach where non-sensitive personal information was exposed due to a cyberattack. The court examined whether the data controller (a public utility company) could be held liable under the General Data Protection Law (LGPD), specifically regarding compliance with Articles 19 and 43[59]. The STJ ruled that the defendant failed to demonstrate that the breach was exclusively caused by a third party, which would exempt it from liability under Article 43 of the LGPD. Furthermore, the court emphasized the principle of "legitimate expectation of protection" and ruled that data controllers must implement sufficient technical and administrative measures to prevent breaches, as required by the LGPD. The STJ also addressed the proactive accountability obligations imposed by the

---

[56] Brazil. Superior Tribunal de Justiça. *Agravo em Recurso Especial No. 2.130.619 - SP*. Rapporteur: Ministro Francisco Falcão. Brasília, 7 de março de 2023.

[57] Couto, José Henrique Oliveira. "Vazamentos De Dados E Dano Moral '*in re ipsa*': Comentários Ao Agravo Em Recurso Especial nº 2.130.619/SP." *Revista IBERC* 6, no. 2 (May/August 2023): 171–188.

[58] Brazil. Superior Tribunal de Justiça. *Recurso Especial No. 2.133.261 - SP*. Rapporteur: Ministra Nancy Andrighi. Brasília, 10 de outubro de 2024.

[59] Brazil. Superior Tribunal de Justiça. *Recurso Especial No. 2.147.374 - SP*. Rapporteur: Ministro Ricardo Villas Bôas Cueva. Brasília, 4 de dezembro de 2024.

LGPD[60]. These include the duty to provide data subjects with information about the origin, criteria, and purpose of data processing, as well as copies of personal data held in databases. The court highlighted that compliance programs and proactive risk mitigation measures are essential for data controllers to demonstrate adherence to LGPD standards. The decision reinforced the importance of transparency, prevention, and accountability in data processing activities, particularly for entities handling personal data as part of their business operations. The court rejected the defendant's argument that the breach should be considered a fortuitous external event, absolving it of liability. The STJ ruled that cybersecurity failures are part of the inherent risks of data processing activities and thus constitute an "internal risk" for which the controller remains accountable. Consequently, the defendant was ordered to provide detailed information about the data shared and processed, in compliance with Articles 18 and 19 of the LGPD.

Collectively, these rulings reflect the STJ's commitment to embedding data protection within Brazil's legal system; however, they also expose a fragmented and, at times, inconsistent judicial approach. The court's oscillation between embracing strict liability principles, such as the *in re ipsa* doctrine, and requiring demonstrable proof of harm reveals a lack of coherence in the application of LGPD standards. Discussions on moral damage are also problematic due to this reductionist approach[61], which may wrongly convey the idea that non-patrimonial torts are the only types of damages virtually indemnifiable under the LGPD provisions, given the difficulty of proving how harm arises from violations of the law. These inconsistencies not only risk eroding legal certainty but also leave data subjects and controllers uncertain about their respective rights and obligations under the law.

F. Sustaining the preventive spirit of the LGPD and strict's liability role

Informational self-determination—underscored in multiple provisions of modern data protection laws—does not equate to an unconstrained right of ownership over personal data. Instead, it represents a nuanced and context-dependent mechanism of control[62]. As Helen Nissenbaum posits, privacy in

[60] Bodin de Moraes, Maria Celina, and João Quinelato de Queiroz. "Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD." In *Cadernos Adenauer*, no. 3 (2019): 113–137. Rio de Janeiro: Fundação Konrad Adenauer.

[61] Rosenvald, Nelson. "A multifuncionalidade da responsabilidade civil e a incongruência do dano moral como equivalente funcional." *Revista Fórum de Direito Civil* 12, no. 33 (May/August 2023): 221–242.

[62] Dresch, Rafael de Freitas Valle, and José Luiz de Moura Faleiros Júnior. "Reflexões

contemporary society is not solely a matter of individual sovereignty but a shared understanding of how information may legitimately flow within social, moral, and political frameworks[63]. Given that these frameworks continually shift in tandem with technological progress, the scope of this right cannot be fixed in statute alone; it requires ongoing interpretation and adaptive governance.

This dynamic environment inherently produces novel hazards and intricate risks for data subjects. No single legislative enactment can fully anticipate the complexities of emerging technologies or the unprecedented threats posed by cybercriminals and evolving data-processing practices. These developments frequently outpace lawmakers, meaning that protections must be proactively embedded into both the architecture of information systems and the legal mechanisms responsible for adjudicating disputes. As a result, the law must encourage not only compliance but also flexibility in how organizations safeguard personal data.

In this context, civil liability fulfills a dual function. On one hand, it aims to compensate those harmed by negligent or improper data practices. On the other, it functions as a powerful deterrent that incentivizes organizations to invest in robust data security and governance from the outset. This principle resonates with M. Stuart Madden's assertion that liability mechanisms do more than merely impose penalties: they actively discourage an unwarranted increase in extracontractual risk and simultaneously encourage safer conduct.

The Brazilian General Data Protection Law (LGPD) exemplifies this twofold purpose by integrating objective (strict) liability, compliance mandates, security requirements, and a pathway for redress. Far from operating as a simple punitive framework, the LGPD prioritizes proactive prevention and continuous risk management. It channels organizations toward the principle of prevention—woven throughout its articles—to ensure that data handlers adopt best practices aligned with transparency, good faith, and accountability.

By embracing an objective liability model, the LGPD reduces the burden on data subjects to establish fault or negligence when a breach or security incident occurs. Instead, the focus rests on verifying whether the organization in question upheld the requisite duty of care and adhered to the statute's standards. Under this regime, the law's deterrent effect is heightened: businesses that fail to invest in thorough governance, risk assessment, and compliance measures may face legal repercussions simply by virtue of

---

sobre a Responsabilidade Civil na Lei Geral de Proteção de Dados (Lei nº 13.709/2018)." In *Responsabilidade Civil: Novos Riscos*, edited by Nelson Rosenvald, Rafael de Freitas Valle Dresch, and Tula Wesendonck. Indaiatuba: Foco, 2019, 88-89.

[63] Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press, 2010, 231.

endangering data subject rights, regardless of intent.

This structure harmonizes theoretical constructs with the realities of a technology-driven society. Civil liability, as codified under the LGPD, compels entities to integrate security and privacy by design, rather than treating them as afterthoughts. By demanding rigorous internal controls and transparent operational practices, the law ensures that personal data is not only shielded from foreseeable harms but that such protections continually evolve to match the shifting digital landscape. This responsiveness is essential, given the inherent unpredictability of advanced technologies and cyber threats.

Ultimately, the LGPD's emphasis on prevention, objective liability, and robust compliance underscores its aspiration to transcend mere symbolic protection of personal data. It seeks to anchor privacy rights firmly in day-to-day organizational processes, thus binding legal theory to tangible practice. In so doing, it helps safeguard individual rights in an era where information flows at unparalleled speed—reminding organizations that, even as technology pushes boundaries, the responsibility to uphold data subjects' legitimate expectations remains a steadfast imperative.

CONCLUSION

In light of the foregoing exposition, it becomes incontrovertible that Brazil's legislative architecture for personal data protection materialized rather belatedly, especially given that information—long exalted as the indispensable substrate of the so-called "information society"—has been pivotal to modern social, economic, and cultural frameworks for many years. Beyond the essential principles of private law that govern civil liability, particularly those embodied in the Civil Code and in the microsystem instituted by the Consumer Protection Code, two overarching statutes have emerged to regulate the internet within Brazil's jurisdiction: the 2014 Internet Civil Framework (*Marco Civil da Internet*) and the 2018 General Data Protection Law (LGPD). Nonetheless, these laws function largely as embryonic forays into an expansive new sphere of legal inquiry, one that must inexorably evolve if it is to furnish adequate solutions to the plethora of novel disputes and contingencies likely to arise from ceaseless technological innovation—a sphere in which legislative bodies invariably lag behind the swift cadence of scientific progress.

Although the legislature's aspirations merit approbation, the reality is that jurisprudence cannot match the singular velocity at which technology advances. This disparity casts doubt upon the efficacy of legal protections—particularly those erected to safeguard fundamental rights—when transposed into an increasingly digital milieu. Consequently, cultivating a nuanced

understanding of what has been termed the "information society" emerges as an imperative objective in grappling with the uncertainties of the future. While promulgating regulatory landmarks undoubtedly forms a critical preliminary step in establishing a legal framework for protection, it cannot constitute the final horizon.

From a technical standpoint, the present analysis underscores the integration of pivotal themes associated with the defense of personality in online contexts and with the delineation of the essential scope of informational self-determination and consent. Adequate security measures and robust corporate governance are indispensable in enabling the comprehensive protection of personal data. Hence, the construct of "digital compliance" has acquired renewed prominence, merging with—and enhancing—existing mechanisms of civil liability within specifically delineated scenarios.

Given the formidable challenge lawmakers face in capturing the myriad complexities pertinent to data protection and assessing "defects" in services provided by controllers and operators, data-processing activities could easily have remained elusive to governmental oversight had the legislature confined itself to promulgating normative frameworks without imposing clear obligations regarding prevention and transparency.

Yet what transpired is quite the opposite: cognizant of the myriad obstacles that hamper the enforcement of duly codified rights, the legislature introduced governance as a delineated (albeit not strictly mandatory) benchmark for defining the contours of causation in instances of improper data handling. This legislative choice fosters debates around a novel liability paradigm that, should it indeed crystallize, is less about inaugurating fresh dogmatic concepts and more about consolidating interrelational elements pivotal to shaping the nucleus of objective theory. Fundamentally, one observes the enshrinement of a general duty of care, derived from a liability structure predicated on verifying and demonstrating "defects" in data collection, processing, and storage procedures. A breach of this duty—signified by the violation of the data subject's legitimate expectations—precipitates accountability for the implicated agent.

In conclusion, while the STJ has made commendable strides in grappling with the complexities of data protection under the LGPD, its jurisprudence highlights the need for a more unified and predictable framework. Articulating consistent criteria for the application of LGPD principles—balancing the rights of data subjects against the legitimate interests of data controllers—will be crucial. Such clarity will bolster privacy protections while fostering an environment conducive to responsible data governance and compliance within Brazil's legal system.

As mentioned, in 2024, STJ also examined the proactive accountability

requirements established by the LGPD. Among these obligations is the responsibility of data controllers to inform data subjects about the origin, criteria, and purposes of data processing, in addition to providing access to copies of their personal data stored in databases. The court underscored the critical role of compliance programs and proactive risk management strategies in ensuring that data controllers meet the standards set by the LGPD. This decision reaffirmed the significance of transparency, preventative measures, and accountability in data processing practices, especially for entities that process personal data as part of their core operations.

By transcending the conventional rubric of fault, the legislative framework obviates purely technical justifications and reduces the broad spectrum of exculpatory grounds that traditionally hinge on the expertise surrounding software architectures, thereby prioritizing collaboration as the principal instrument for scrutinizing and delimiting the scope of civil liability.

Also, the proactive approach signals towards strict liability because it shifts the focus from proving fault or negligence to emphasizing accountability, prevention, and compliance measures. Data processing activities, especially those involving sensitive or large-scale personal data, inherently carry risks such as breaches or misuse. By requiring proactive measures, the law implicitly recognizes these risks and holds data controllers accountable for managing them, regardless of intent or negligence.

A comprehensive reading of the LGPD—reinforced by its principled architecture and by future regulatory provisions to be issued by the National Data Protection Authority (ANPD)—reveals that processing agents are, in practice, bound to observe precautionary measures against any confirmed adverse events or "undesirable results and risks" that would otherwise qualify as irregular data-processing activities. Article 44(II) of the LGPD likewise underscores that the law does not espouse a subjective liability model; rather, it propounds an *objective liability* regime of a distinctive nature.

The principle of prevention (Article 6(VIII)) serves as a linchpin in this analytical framework. By imposing an imperative—manifested in the verb *"dever"* ("must," "shall") in the chapeau of Article 46—for agents to adopt "technical and administrative security measures capable of safeguarding personal data," the LGPD crystallizes this requirement and corroborates it through the conditions outlined in Article 44's subdivisions.

Augmenting these arguments is the drive toward compliance, achieved through risk-management regulations grounded in a sense of reciprocity that integrates all actors involved in data-processing tasks. This integrated model promotes a cooperative ethos guided by the law's foundational principles—notably *bona fide* (Article 6, *caput*) and transparency (Article 6(VI))—aimed

at furnishing clear notice regarding processing activities and any security incidents (Articles 9 and 48(§1)).

Whether "leaks" are construed as a subset of "security incidents," as the ANPD appears to suggest, or deemed a sui generis category of unlawful personal data usage, the indisputable fact is that their legal characterization hinges on the resulting tangible harm—monetary or non-monetary—inflicted on individuals or collectives (Article 42). Such harm must arise from improper data-processing endeavors; the determination thereof rests not upon any proof of fault but rather upon an objective assessment of accidental or unlawful situations (Article 46). Evaluating those circumstances (Article 44(I)–(III)) should demonstrate whether, at some juncture of the data-processing chain—even subsequent to its ostensible conclusion (Article 47)—the requisite safeguards failed to meet the data subject's legitimate expectations of security (Articles 44, *caput*, and 49), barring those instances in which the causal link is extraordinarily negated (Article 43).

By adopting a strict liability-like approach through proactive obligations, the law ensures a higher standard of protection for data subjects. It eliminates the burden of proving negligence, making it easier for affected individuals to seek redress and promoting fairness in balancing power dynamics between data controllers and individuals.

In sum, this legal environment buttresses a special objective liability regime that moves beyond traditional fault-based analyses and underscores preventive obligations, governance strategies, and an ethos of collaboration, transparency, and accountability as foundational tenets for defending personal data within the contemporary digital landscape.

REFERENCES

Achterhuis, Hans. Introduction: American Philosophers of Technology. In *American Philosophy of Technology: The Empirical Turn*, edited by Hans Achterhuis, translated by Robert P. Crease. Indianapolis: Indiana University Press, 2001.

Ariely, Dan, George Loewenstein, and Drazen Prelec. "Coherent Arbitrariness: Stable Demand Curves Without Stable Preferences." *Quarterly Journal of Economics* 118, no. 1 (February 2003): 73–106.

Bauman, Zygmunt, and David Lyon. *Vigilância Líquida*. Translated by Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

Bennett, Colin J. "Convergence Revisited: Toward a Global Policy for Protection of Personal Data?" In *Technology and Privacy: The New Landscape*, edited by Philip E. Agre and Marc Rotenberg. Cambridge: The MIT Press, 1997.

Bodin de Moraes, Maria Celina, and João Quinelato de Queiroz.

"Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD." In *Cadernos Adenauer*, no. 3 (2019): 113–137. Rio de Janeiro: Fundação Konrad Adenauer.

Brazil. Autoridade Nacional de Proteção de Dados (ANPD). "Incidente de Segurança." Accessed January 23, 2025. https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca.

Brazil. Superior Tribunal de Justiça. *Agravo em Recurso Especial No. 2.130.619 - SP*. Rapporteur: Ministro Francisco Falcão. Brasília, 7 de março de 2023.

Brazil. Superior Tribunal de Justiça. *Recurso Especial No. 1.758.799 - MG.* Rapporteur: Ministra Nancy Andrighi. Brasília, 19 de novembro de 2019.

Brazil. Superior Tribunal de Justiça. *Recurso Especial No. 2.133.261 - SP*. Rapporteur: Ministra Nancy Andrighi. Brasília, 10 de outubro de 2024.

Brazil. Superior Tribunal de Justiça. *Recurso Especial No. 2.147.374 - SP*. Rapporteur: Ministro Ricardo Villas Bôas Cueva. Brasília, 4 de dezembro de 2024.

Brazil. Supremo Tribunal Federal. "Marco Civil da Internet: Relator Considera Inconstitucional Exigência de Ordem Judicial para Retirada de Conteúdo." *STF Notícias*, December 4, 2024. Accessed January 23, 2025. https://noticias.stf.jus.br/postsnoticias/marco-civil-da-internet-relator-considera-inconstitucional-exigencia-de-ordem-judicial-para-retirada-de-conteudo/.

Brüggemeier, Gert, Aurelia Colombi Ciacchi, and Patrick O'Callaghan. "A Common Core of Personality Protection." In *Personality Rights in European Tort Law*, edited by Gert Brüggemeier, Aurelia Colombi Ciacchi, and Patrick O'Callaghan. Cambridge: Cambridge University Press, 2010.

Brzezinski, Zbigniew K. *Between Two Ages: America's Role in the Technetronic Era.* New York: Viking Press, 1971.

Cardoso, João Victor Gontijo. "O Dano Moral 'In Re Ipsa' e o Tratamento Indevido de Dados sob o Prisma dos Julgados: REsp 1.758.799/MG e ADI 6387 MC-REF." *Revista IBERC* 4, no. 1 (January/April 2021): 133–153.

Català, Pierre. "Ebauche d'une Théorie Juridique de l'Information." *Informatica e Diritto*, Naples, IX (January/April 1983).

Couto, José Henrique Oliveira. "Vazamentos De Dados E Dano Moral 'in re ipsa': Comentários Ao Agravo Em Recurso Especial nº 2.130.619/SP." *Revista IBERC* 6, no. 2 (May/August 2023): 171–188.

Cravo, Daniela Copetti, and Marcela Joelsons. "A importância do CDC no tratamento de dados pessoais de consumidores no contexto da pandemia e de *vacatio legis* da LGPD." *Revista de Direito do Consumidor* 131 (September/October 2020): 111–145.

Dantas Bisneto, Cícero. "Reparação por danos morais pela violação à LGPD e ao RGPD: uma abordagem de direito comparado." *Civilistica.com* 9, no. 3 (2020): 1–23.

Devins, Caryn, Teppo Felin, Stuart Fauffman, and Roger Koppl. "The Law and Big Data." *Cornell Journal of Law and Public Policy* 27, no. 2 (January/April 2017): 357–413.

Dresch, Rafael de Freitas Valle, and Gustavo da Silva Melo. "Artigo 43." In *Comentários à Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018)*, 2nd ed., edited by Guilherme Magalhães Martins, João Victor Rozatti Longhi, and José Luiz de Moura Faleiros Júnior. Indaiatuba: Foco, 2024.

Dresch, Rafael de Freitas Valle, and Gustavo da Silva Melo. "O papel do operador no tratamento de dados: entre deveres e responsabilização" In *Compliance e Políticas de Proteção de Dados*, edited by Ana Frazão and Ricardo Villas Bôas Cueva. São Paulo: Thomson Reuters Brasil, 2021.

Dresch, Rafael de Freitas Valle, and José Luiz de Moura Faleiros Júnior. "Reflexões sobre a Responsabilidade Civil na Lei Geral de Proteção de Dados (Lei nº 13.709/2018)." In *Responsabilidade Civil: Novos Riscos*, edited by Nelson Rosenvald, Rafael de Freitas Valle Dresch, and Tula Wesendonck. Indaiatuba: Foco, 2019.

Dresch, Rafael de Freitas Valle, and Lílian Brandt Stein. "A responsabilidade civil como mecanismo de incentivo à observância do direito fundamental à proteção de dados: uma análise da interpretação do art. 42 e seguintes da LGPD." *Revista de Direito da Responsabilidade* 5 (2023): 978–980.

Dresch, Rafael de Freitas Valle. *Fundamentos do Direito Privado: Uma Teoria da Justiça e da Dignidade Humana*. 2nd ed. Rio de Janeiro, 2019.

Duff, Alistair A. *Information Society Studies.* London: Routledge, 2000.

Faleiros Júnior, José Luiz de Moura, and Cristiano Colombo. "A Tutela Jurídica do Corpo Eletrônico: Alguns Conceitos Introdutórios." In *Tutela Jurídica do Corpo Eletrônico: Novos Desafios ao Direito Digital*, edited by Cristiano Colombo, Wilson Engelmann, and José Luiz de Moura Faleiros Júnior. Indaiatuba: Foco, 2022.

Faleiros Júnior, José Luiz de Moura. "Accountability e Devida Diligência como Vetores da Governança Corporativa nos Mercados Ricos em Dados." *Revista Semestral de Direito Empresarial* 26 (2020): 183–211.

Faleiros Júnior, José Luiz de Moura. "Compliance Digital y Gobernanza: El Diálogo Interdisciplinario en la Era Digital." *Juris Studia* 1 (2024): 145–158.

Faleiros Júnior, José Luiz de Moura. "O Que É, Afinal, um Vazamento de Dados?" *Migalhas de Proteção de Dados*, March 10, 2022. Accessed January 23, 2025. https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/351388/o-que-e-afinal-um-vazamento-de-dados

Gondim, Glenda Gonçalves. "A Responsabilidade Civil no Uso Indevido dos Dados Pessoais." In *Responsabilidade Civil e Novas Tecnologias*, 2nd ed., edited by Guilherme Magalhães Martins, Nelson Rosenvald, and José Luiz de Moura Faleiros Júnior. Indaiatuba: Foco, 2023.

Grossi, Bernardo Menicucci. "A violação dos direitos de personalidade na LGPD: a problemática do dano moral *in re ipsa*" In *Direito, Tecnologia e Inovação, vol. 4: estudos de casos*, edited by Leonardo Parentoni. Belo Horizonte: Centro DTIBR, 2022.

Grossi, Bernardo Menicucci. "Responsabilidade Civil na LGPD: A Culpa Presumida Relativa." *Migalhas de Responsabilidade Civil*, April 24, 2023. Accessed January 23, 2025. https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/385155/responsabilidade-civil-na-lgpd-a-culpa-presumida-relativa.

Heidegger, Martin. *The Question Concerning Technology, and Other Essays*. Translated by William Lovitt. New York: Harper Perennial, 2013.

Jonas, Hans. *Frontiere della Vita, Frontiere della Tecnica.* Translated by Giovanna Bettini; edited by Vallori Rasini. Bologna: Il Mulino, 2011.

Lace, Susanne. *The Glass Consumer: Life in a Surveillance Society.* Bristol: Policy Press, 2005.

Lloyd, Ian J. *Information Technology Law*. 6th ed. New York/Oxford: Oxford University Press, 2011.

Madalena, Juliano. "A Responsabilidade Civil Decorrente do Vazamento de Dados Pessoais." In *Lei Geral de Proteção de Dados: Aspectos Relevantes*, edited by Fabiano Menke and Rafael de Freitas Valle Dresch. Indaiatuba: Foco, 2021.

Marcuse, Herbert. *One-Dimensional Man: Studies in the Ideology of Advanced Industrial Society*. Boston: Beacon, 1964.

Martins, Guilherme Magalhães, and José Luiz de Moura Faleiros Júnior. "Compliance Digital e Responsabilidade Civil na Lei Geral de Proteção de Dados." In *Responsabilidade Civil e Novas Tecnologias*, 2nd ed., edited by Guilherme Magalhães Martins, Nelson Rosenvald, and José Luiz de Moura Faleiros Júnior. Indaiatuba: Foco, 2023.

Mendes, Laura Schertel, and Danilo Doneda. "Reflexões Iniciais sobre a Nova Lei Geral de Proteção de Dados." *Revista de Direito do Consumidor* 120 (November/December 2018): 469–483.

Miragem, Bruno. "A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor." *Revista dos Tribunais* 1009 (November 2019): 173–222.

Mulholland, Caitlin. "A LGPD e o Fundamento da Responsabilidade Civil dos Agentes de Tratamento de Dados Pessoais: Culpa ou Risco?" *Migalhas de Responsabilidade Civil*, June 30, 2020. Accessed January 23, 2025. https://www.migalhas.com.br/coluna/migalhas-de-

responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais--culpa-ou-risco

Mulholland, Caitlin. "Responsabilidade Civil por Danos Causados pela Violação de Dados Sensíveis e a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018)." In *Responsabilidade Civil e Novas Tecnologias*, 2nd ed., edited by Guilherme Magalhães Martins, Nelson Rosenvald, and José Luiz de Moura Faleiros Júnior. Indaiatuba: Foco, 2023.

Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press, 2010.

Orwell, George. *Nineteen Eighty-Four*. New York: Penguin/Signet Classics, 1961.

Peroli, Kelvin, and José Luiz de Moura Faleiros Júnior. "Artigo 50." In *Comentários à Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018)*, 2nd ed., edited by Guilherme Magalhães Martins, João Victor Rozatti Longhi, and José Luiz de Moura Faleiros Júnior. Indaiatuba: Foco, 2024.

Queiroz, Renata Capriolli Zocatelli. *Encarregado de Proteção de Dados Pessoais – DPO: Regulamentação e Responsabilidade Civil.* São Paulo: Quartier Latin, 2022.

Rodotà, Stefano. *Intervista su Privacy e Libertà*. Rome/Bari: Laterza, 2005.

Rosenvald, Nelson, and José Luiz de Moura Faleiros Júnior. "Accountability e Mitigação da Responsabilidade Civil na Lei Geral de Proteção de Dados Pessoais." In *Compliance e Políticas de Proteção de Dados*, edited by Ana Frazão and Ricardo Villas Bôas Cueva. São Paulo: Thomson Reuters Brasil, 2021.

Rosenvald, Nelson. "A multifuncionalidade da responsabilidade civil e a incongruência do dano moral como equivalente funcional." *Revista Fórum de Direito Civil* 12, no. 33 (May/August 2023): 221–242.

Samson, Alain, and Benjamin Voyer. "Emergency Purchasing Situations: Implications for Consumer Decision-Making." *Journal of Economic Psychology* 44, no. 1 (September 2014): 21–33.

Sarlet, Ingo Wolfgang. "Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada." *Direitos Fundamentais & Justiça* 14, no. 42 (January/June 2020): 179–218.

Silverman, Michal G. *Compliance Management for Public, Private, or Nonprofit Organizations*. New York: McGraw Hill, 2008.

Tamò-Larrieux, Aurelia. *Designing for Privacy and Its Legal Framework: Data Protection by Design and Default for the Internet of Things*. Basel: Springer, 2018.

Tepedino, Gustavo, Aline de Miranda Valverde Terra, and Gisela Sampaio

da Cruz Guedes. "Responsabilidade civil dos agentes de tratamento de dados" In *Compliance e Políticas de Proteção de Dados*, edited by Ana Frazão and Ricardo Villas Bôas Cueva. São Paulo: Thomson Reuters Brasil, 2021.

Thaler, Richard H. "Mental Accounting Matters." *Journal of Behavioral Decision Making* 12, no. 3 (July 1999): 183–206.

Van Dijk, Jan. *The Network Society*. 3rd ed. London: Sage Publications, 2012.

Westin, Alan F. *Information Technology in a Democracy*. Cambridge: Harvard University Press, 1971.

* * *

Rafael de Freitas Valle Dresch
Associate Professor at the School of Law and the Graduate Program in Law at the Federal University of Rio Grande do Sul (UFRGS), and Partner at Coulon, Dresch e Masina Advogados. He holds a Bachelor's degree in Legal and Social Sciences from the Pontifical Catholic University of Rio Grande do Sul (PUCRS, 1998), a specialization in Contracts and Civil Liability from UFRGS (2001), and a Master's degree in Private Law from UFRGS (2005). He earned his PhD in Law from PUCRS (2011), which included a doctoral internship (Sandwich Doctorate – CAPES) at the University of Edinburgh in the UK (2010). He completed his postdoctoral research as a Visiting Scholar at the University of Illinois at Urbana-Champaign (2014).
Email: rafael.dresch@ufrgs.br
ORCID iD: https://orcid.org/0000-0001-5534-567X

José Luiz de Moura Faleiros Júnior
PhD in Private Law, University of São Paulo (USP/Largo de São Francisco). Currently pursuing a PhD in Law, specializing in 'Law, Technology, and Innovation' at the Federal University of Minas Gerais (UFMG). Holds a Master's and Bachelor's degree in Law from the Federal University of Uberlândia (UFU). Specialist in Digital Law. Lawyer. Professor.
Email: josefaleirosjr@outlook.com
ORCID iD: https://orcid.org/0000-0002-0192-2336

10.59224/bjlti.v2i2.98-128
ISSN: 2965-1549