Jornal of Legal Sciences
Pensar
e-ISSN: 2317-2150
Universidade de Fortaleza

10.5020/2317-2150.2025.15238

Guidelines for the Protection of the Fundamental Right to Informational Self-Determination in the Digital Age

Diretrizes para a Proteção do Direito Fundamental à Autodeterminação Informativa na Era Digital

Directrices para la Protección del Derecho Fundamental a la Autodeterminación Informativa en la Era Digital

Ana Maria D´Ávila Lopes *[1], **Rodrigo Martiniano Ayres Lins** *[2]

*Universidade de Fortaleza, Fortaleza, Ceará, Brasil

Editorial

Histórico do Artigo
Recebido: 10/05/2025
Aceito: 22/07/2025

Eixo Temático 3: Direito, Tecnologia e Sociedade em Transformação

Editores-chefes
Katherinne de Macêdo Maciel Mihaliuc
Universidade de Fortaleza, Fortaleza, Ceará, Brasil
katherinne@unifor.br

Sidney Soares Filho
Universidade de Fortaleza, Fortaleza, Ceará, Brasil
sidney@unifor.br

Editor Responsável
Sidney Soares Filho
Universidade de Fortaleza, Fortaleza, Ceará, Brasil
sidney@unifor.br

Autores
Ana Maria D´Ávila Lopes
anadavilalopes@yahoo.com.br
Contribuição: Supervision, Writing – Review & Editing.

Rodrigo Martiniano Ayres Lins
r.martiniano@gmail.com
Contribuição: Conceptualization, Investigation, Writing - Original Draft.

Como citar:
LOPES, Ana Maria D´Ávila; LINS, Rodrigo Martiniano Ayres. Diretrizes para a proteção do direito fundamental à autodeterminação informativa na era digital. **Pensar – Revista de Ciências Jurídicas**, Fortaleza, v. 30, e15238, 2025. DOI: https://doi.org/ 10.5020/2317-2150.2025.15238

Declaração de disponibilidade de dados

A Pensar – Revista de Ciências Jurídicas adota práticas de Ciência Aberta e disponibiliza, junto à presente publicação, a Declaração de Disponibilidade de Dados (Formulário Pensar Data) preenchida e assinada pelos autores, a qual contém informações sobre a natureza do artigo e a eventual existência de dados complementares. O documento pode ser consultado como arquivo suplementar neste site.

Abstract

The consolidation of the digital society has imposed profound transformations on social, economic, and legal dynamics, generating unprecedented risks to fundamental rights, especially with regard to privacy and informational self-determination, whose fragility is exacerbated by the deficiency of a normative framework capable of ensuring their protection. In this context, the present article seeks to help overcome this problem by formulating guidelines aimed at enhancing the national legal framework, on the basis of an analysis of foreign experiences. To this end, the research adopts a qualitative approach, employing deductive and inductive methods, grounded in a literature and documentary review of national and foreign legal doctrine and case law. The analysis begins with an understanding of the multiple dimensions of fundamental rights in the digital age, discusses the application of the principle of human dignity, and deepens the study of informational self-determination as an autonomous manifestation of the subject over their personal data. The work also examines the normative and jurisprudential frameworks of Brazil, Germany, and the European Union. Finally, it proposes guidelines for the practical implementation of the right to informational self-determination, such as the adoption of institutional policies based on privacy by design and privacy by default, and the provision of swift mechanisms of judicial and administrative protection. It concludes that the protection of informational self-determination today constitutes an ethical and legal imperative for preserving not only human dignity, but also for safeguarding trust in the digital ecosystem, which is undeniably inseparable from social life in contemporary society.

Keywords: fundamental rights; informational self-determination; data protection; German Federal Constitutional Court; Court of Justice of the European Union.

Resumo

A consolidação da sociedade digital impôs profundas transformações às dinâmicas sociais, econômicas e jurídicas, gerando riscos inéditos aos direitos fundamentais, sobretudo no que tange à privacidade e à autodeterminação informativa, cuja fragilidade extrapola-se diante da deficiência de uma estrutura normativa capaz de garantir sua proteção. Nesse contexto, o presente artigo busca contribuir a superar essa problemática a partir da formulação de diretrizes direcionadas a aprimorar o arcabouço jurídico nacional, a partir da análise de experiências forâneas. Para tal, a pesquisa adota abordagem qualitativa, valendo-se dos métodos dedutivo e indutivo, com base em revisão bibliográfica e documental da doutrina e jurisprudência nacionais e estrangeiras. A análise parte da compreensão das múltiplas dimensões dos direitos fundamentais na era digital, discute a aplicação do princípio da dignidade da pessoa humana e aprofunda o estudo da autodeterminação informativa enquanto manifestação autônoma do sujeito sobre seus dados pessoais. O trabalho também examina os marcos normativos e jurisprudenciais do Brasil, da Alemanha e da União Europeia. Por fim, propõe diretrizes para a efetivação prática do direito à autodeterminação informativa, tais como a adoção de políticas institucionais baseadas em privacy by design e privacy by default, e a previsão de mecanismos céleres de tutela jurisdicional e administrativa. Conclui-se que a proteção da autodeterminação informativa constitui hoje um imperativo ético e jurídico para a preservação não apenas da dignidade humana, mas também para salvaguardar a confiança no ecossistema digital, inegavelmente inseparável da vida em sociedade na contemporaneidade.

Palavras-chave: direitos fundamentais; autodeterminação informativa; proteção de dados; Tribunal Constitucional Alemão; Tribunal de Justiça da União Europeia.

[1] Mestre (1995 - bolsa CAPES) e Doutora (1999 - bolsa CNPq) em Direito Constitucional pela Universidade Federal de Minas Gerais. Pesquisa de pós-doutorado sobre os direitos humanos das minorias e pessoas em situação de vulnerabilidade em: University of British Columbia (Centre for Feminist Legal Studies - 2001), University of Ottawa (Centre de recherche et denseignement sur les droits de la personne - 2001), York University (Osgoode Hall Law School - 2001/ 2002), Yale University (Yale Law School - 2008) e em The University of Auckland (Faculty of Law - 2009/2010) com Bolsa PDE CNPq. Coordenadora da Comissão Qualis-Direito da CAPES (janeiro 2015 - março 2018). Membro da Comissão Qualis-Direito da Capes (2010-2014). Atual Representante da Grande Área das Ciências Sociais no Grupo Assessor Especial da Diretoria de Relações Internacionais (GAE-DIR) da CAPES). Membro Efetivo do Grupo Assessor Especial da Diretoria de Relações Internacionais (GAE-DIR) da CAPES (2017-2019).

[2] Mestre e Doutorando em Direito Constitucional e Teoria Política (UNIFOR - CAPES 6). Especialista em Políticas Públicas para Cidades Inteligentes (USP). Especialista em Direito Eleitoral (PUC/MG), em Direito Processual Civil (Unicap) e em Direito Público (Esmape). Atualmente é Procurador-Geral da Assembleia Legislativa do Estado do Ceará e Professor de Cursos de Pós-Graduação em Direito. Membro-fundador da Academia Brasileira de Direito Eleitoral e Político (ABRADEP).

Resumen

La consolidación de la sociedad digital impuso profundas transformaciones a las dinámicas sociales, económicas y jurídicas, generando riesgos inéditos para los derechos fundamentales, especialmente en lo que atañe a la privacidad y a la autodeterminación informativa, cuya fragilidad se ve acrecentada ante la insuficiencia de una estructura normativa capaz de garantizar su protección. En este contexto, el presente artículo busca contribuir a superar esta problemática mediante la formulación de directrices orientadas a perfeccionar el armazón jurídico nacional, a partir del análisis de experiencias foráneas. Para ello, la investigación adopta un enfoque cualitativo, valiéndose de los métodos deductivo e inductivo, con base en una revisión bibliográfica y documental de la doctrina y la jurisprudencia nacionales y extranjeras. El análisis parte de la comprensión de las múltiples dimensiones de los derechos fundamentales en la era digital, discute la aplicación del principio de la dignidad de la persona humana y profundiza el estudio de la autodeterminación informativa como manifestación autónoma del sujeto sobre sus datos personales. El trabajo también examina los marcos normativos y jurisprudenciales de Brasil, Alemania y la Unión Europea. Por último, propone directrices para la efectivación práctica del derecho a la autodeterminación informativa, tales como la adopción de políticas institucionales basadas en privacy by design y privacy by default, y la previsión de mecanismos expeditos de tutela jurisdiccional y administrativa. Se concluye que la protección de la autodeterminación informativa constituye hoy un imperativo ético y jurídico para la preservación no solo de la dignidad humana, sino también para salvaguardar la confianza en el ecosistema digital, innegablemente inseparable de la vida en sociedad en la contemporaneidad.

Palabras clave*: derechos fundamentales; autodeterminación informativa; protección de datos; Tribunal Constitucional Federal de Alemania; Tribunal de Justicia de la Unión Europea.*

1 Introduction

The technological revolution and the consolidation of the information society have radically transformed the way individuals interact, produce knowledge, and exercise their rights. At the heart of these transformations lies the growing centrality of personal data, whose large-scale processing by public and private entities presents new challenges to contemporary constitutional law.

The transition to a connected society affects both highly industrialized nations and developing economies, shaping a global paradigm rooted in information technologies (Castells, 2000). Social relations have become mediated by digital networks and surveillance systems capable of reshaping economic and political structures, thereby redefining the boundaries of privacy and individual autonomy.

The collection, storage, and monetization of data have become widespread practices, particularly by major digital platforms. Although these data flows enable innovation and personalized services, they also create power asymmetries, pose risks to privacy, foster algorithmic discrimination, and enable behavioral manipulation. These vulnerabilities underscore the urgent need for a more adequate legal response.

Because of the ongoing reconfiguration of social and legal structures driven by digital technologies, it is essential to rethink the framework of fundamental rights in light of the dynamics inherent to the information society. Informational self-determination — conceived as an expression of human dignity and individual autonomy — emerges as one of the most challenged yet most vital rights of our time.

The present article aims to formulate guidelines for enhancing the legal framework protecting the fundamental right to informational self-determination, in view of a still-deficient normative structure. To do so, it examines the emergence of this right as a constitutional response to the asymmetries and risks imposed by the digital logic that threatens individuals' ability to decide what personal data may be collected and how such data may be used.

2 Fundamental Rights in the Digital Age

Fundamental rights are among the most important pillars underpinning the Democratic Rule of Law. They are rights held by all human beings, regardless of nationality, sex, ethnic or racial origin, religion, language, or any other condition. "The inclusion of fundamental human rights is essentially aimed at protecting human dignity in its broadest sense" (Moraes, 1998, p. 22, free translation).

These rights encompass multiple dimensions — which includes but is not limited to civil, political, economic, social, and cultural rights — reflecting the complexity and interdependence of the various aspects that shape social life. The codification of these human rights "indicates, for example, whether a State can be recognized as democratic or whether it assumes the character of barbarism" (Souza; Mezzaroba, 2012, p. 175, free translation).

In the civil sphere, fundamental rights focus on protecting personal freedom and integrity. This includes the right to life, liberty, equality, privacy, and property. These rights are essential for individual development, allowing people to express themselves freely and to seek and receive information. Moreover, "they tend to limit state power and reserve for the individual — or for private groups — a sphere of freedom in relation to the State" (Bobbio, 2004, p. 23, free translation).

In the political sphere, fundamental rights guarantee citizens' participation in political life and in decision-making processes that affect their lives. This includes the right to vote and to be elected as well as to hold public office. These are rights of "increasingly broad, generalized, and frequent participation of community members in political power" (Bobbio, 2004, p. 23, free translation).

From an economic standpoint, fundamental rights aim to ensure free enterprise, thereby protecting and promoting individual economic development, which, in turn, contributes to the development of the State itself.

In the social domain, fundamental rights enable individuals to demand that the State take action to ensure the minimum conditions for a dignified life. This includes labor protection, such as fair and satisfactory wages, as well as essential rights for the economic well-being of individuals and their families, such as the rights to education, health care, assistance for the vulnerable, social security, and an adequate standard of living. These rights are fundamental to ensuring access to the basic resources needed to live with dignity and to fully participate in society.

Lastly, in the cultural domain, fundamental rights recognize cultural diversity and protect each person's right to participate in the cultural life of the community to which they belong — enjoying traditions, the arts, and other expressions that are part of their individual identity.

In short, fundamental rights are the deepest expression of the protection of human dignity. They serve as legal norms that enable the peaceful and harmonious coexistence of all members of society. In the digital age, the exercise, protection, and promotion of fundamental rights take on new dimensions, challenging societies to rethink and adapt traditional principles to virtual environments.

This is a new era — one that expands the scope of fundamental rights and highlights new vulnerabilities and challenges that arise from their convergence with technology.

As "in the digital environment, private actors emerge alongside Nation-States as potential violators of fundamental rights" (Celeste, 2021, p. 86, free translation), the protection and promotion of these rights require continuous interpretive updates to ensure their effectiveness in the face of new vulnerabilities and power asymmetries that emerge in the virtual space.

In the civil dimension, the protection of the right to privacy and personal data has become central, given the unprecedented capacity to collect, store, and process personal information online. Respect for privacy and autonomy over one's own data is essential to ensuring individual freedom in the digital age. This gives rise to significant challenges, including mass surveillance, online tracking, and the misuse of data by both private and governmental entities.

In the political sphere, the internet enables an unprecedented dissemination of ideas, fostering civic participation and democratic engagement. However, it also exposes users to risks such as digital censorship, disinformation, and online hate speech. Ensuring that the digital environment remains a space for democratic discourse — one that respects the diversity of opinions and protects against abuse — has become imperative.

Economically, the digital era has transformed the labor market and the global economy, creating new forms of employment and introducing challenges related to job security, labor rights, and economic inequality. Remote work and the gig economy are examples of how economic rights must be reinterpreted and safeguarded in the digital context.

Socially, digital inclusion is crucial to ensuring equal access to public welfare policies and addressing economic disparities. However, the need to be digitally connected to public platforms also brings the risk of privacy erosion.

Culturally, the digital context offers new platforms that promote knowledge sharing and intercultural exchange. Yet it also raises concerns about copyright, cultural appropriation, and the preservation of cultural diversity in the digital age.

Thus, the intersection of fundamental rights and the digital environment demands a new balance between freedom and security, privacy and transparency, inclusion and diversity. It calls for ongoing reflection on how fundamental rights can be effectively exercised and protected in digital settings, ensuring that technology serves human well-being and contributes to a more just and inclusive society. The challenge lies in developing policies, regulations, and technologies that respect and reinforce fundamental rights, ensuring that digital advancements contribute positively to humanity.

The digital age — characterized by technological revolution and the ubiquity of information and communication technologies — has brought about unprecedented transformations in nearly every aspect of human life. These changes have deeply affected how we understand and exercise fundamental rights such as freedom of expression, the right to privacy, freedom of the press, access to information, and protection against discrimination.

The expansion of digital networks and the increased capacity for data processing and storage have enabled greater connectivity among people and access to an infinite volume of information. However, this same expansion has brought serious challenges to the protection and promotion of fundamental rights. Issues such as mass surveillance, the improper collection and use of personal data, the spread of disinformation, online hate speech, and digital censorship are just a few of the emerging problems that demand urgent attention.

We have reached a point where a digital identity has been constructed, yet we still lack a secure space that can be considered its legitimate home. There are no effective institutional mechanisms for the collective protection of data, nor is there a cyberspace that guarantees belonging and autonomy. Not even technological giants such as Google and Meta — let alone the State and its security and intelligence agencies — provide such shelter. It is important to recognize, however, that this "digital self" is not an ontological extension of the subject, but rather a relational construct shaped by continuous surveillance systems, civil registries, unique citizen identifiers, connected devices, cloud storage, drones, biometric data, communication databases, and algorithmic profiling. In this context, guarantees such as privacy, the right to be forgotten, and the ability to become invisible in digital environments emerge as expressions of new fundamental rights. It is within this horizon that we may speak of a notion of digital fundamentality (Canotilho, 2019).

Against this backdrop, Digital Constitutionalism takes on growing importance. It is conceived as the theoretical and normative effort to recognize, assert, and protect fundamental rights in cyberspace, in the face of informational power asymmetries between users, corporations, and States. Beyond the protection of rights, Digital Constitutionalism seeks to restore balance among the various actors in the digital sphere by confronting the risks posed by surveillance capitalism, the massive and nonconsensual extraction of data — referred to as behavioral surplus — and global practices of informational colonialism that undermine both individual and collective sovereignty over data (Cantarini, 2023).

It is therefore imperative that societies reflect on how fundamental rights can be preserved and strengthened in the digital age, bearing in mind that "the recognition and protection of human rights are the foundation of democratic constitutions" (Bobbio, 2004, p. 223, free translation). This requires adapting existing regulatory frameworks and developing new approaches that consider the specific characteristics of the digital environment. The ultimate goal is to ensure that technology serves as a tool for enhancing freedom and democracy, rather than as an instrument for their erosion.

Moreover, the digital era highlights the pressing need to promote inclusion and ensure that all individuals have access to information and communication technologies, as previously discussed. After all, the ability to access and use information is essential for the exercise of human rights and effective participation in contemporary society.

As we navigate this new era, it is crucial that governments, corporations, civil society organizations, and individuals work together to ensure that technology serves the common good — advancing fundamental rights and contributing to a more just, inclusive, and democratic society.

3 The Fundamental Right to Informational Self-Determination on Digital Platforms

In the heart of Brazil's 1988 Federal Constitution, a series of fundamental rights and guarantees were enshrined, reflecting the democratic aspirations and the pursuit of justice, freedom, and equality by Brazilian society. Such is the importance of these rights and guarantees that the framers of the Constitution did not limit themselves to listing them explicitly but included an open clause to encompass those rights that may have been omitted or that may arise naturally from the evolution of society and thus require constitutional recognition. This open clause is found in Article 5, §2, which establishes that the fundamental rights and guarantees provided for in the Constitution do not exclude others deriving from the principles or regime it adopts, or from international treaties to which Brazil is a party (Brasil, 1988). This provision reflects the intention to recognize the existence of fundamental rights and guarantees beyond the text of the Constitution itself — that is, materially constitutional norms that, by their axiological quality, must be treated as part of the constitutional order. In this sense, Piovesan (1998, p. 52, free translation) states: "[…] this derives from a systematic and teleological interpretation of the constitutional text, particularly in light of the expansive force of human dignity and fundamental rights as axiological parameters that guide the understanding of the constitutional phenomenon."

Indeed, "fundamental rights are not limited to those recognized at the moment of the original constitutional drafting, but are subject to an ongoing process of expansion" (Pardo, 2015, p. 12, free translation,).

Within this framework, legal scholarship has increasingly embraced the notion that informational self-determination, although not explicitly recognized as a fundamental right in the Constitution, is implicitly protected as such — deriving from the foundational principle of human dignity.

Human dignity, established in Article 1, item III of the Constitution, stands as a foundational pillar of the Brazilian legal system. This principle is closely tied to autonomy, the free development of the individual, and the recognition of each human being's intrinsic value. In today's digital environment, where personal information and data have become extensions of one's personality, ensuring their integrity and control is imperative to upholding human dignity.

In today's digital environment, companies — not only the State — play a central role in the collection, processing, and storage of personal data. Global tech corporations, social media platforms, and online services have access to an unprecedented amount of data about individuals — often more than the State itself. As Pessoa, Limberger, and Witschoreck (2024, p. 11, free translation) argue, "individuals' control over their personal data is an illusion in the face of a digital economy capitalized by big techs."

Control over one's personal data is inseparable from individual freedom and the autonomy of will. As Zuboff (2019) points out, the logic of surveillance capitalism operates through the unilateral extraction of behavioral data, turning every aspect of daily life into raw material for predictive models. This informational asymmetry — often invisible and inescapable — undermines individual self-determination by subjecting personal choices to algorithmic structures that lack transparency and are driven by commercial interests beyond individual control. Thus, to protect personal data is to protect the very possibility of acting freely in a digitalized society.

In this sense, the right to informational self-determination is the individual's power to decide what personal data may be collected and how it may be used. It is the exercise of one's autonomy over their information, enabling control over their digital identity and personal narrative. As Rodotà (2008, p. 15, free translation) affirms, individuals must have "the right to retain control over their own information and to determine how to construct their private sphere."

Informational self-determination represents "the right to control the use others make of information concerning the private sphere of the individual" (Doneda, 2000, p. 120, free translation). "A database may store an almost unlimited amount of information. Therefore, individuals who entrust their data must rely on legal protection to ensure proper use, whether by public or private entities" (Limberger, 2009, p. 58, free translation). If intimacy is conceived as a set of attitudes, behaviors, preferences, opinions, and actions that the individual wishes to preserve under their exclusive control, then privacy protection must be grounded in the "right to informational self-determination" (Doneda, 2020, p. 129, free translation).

The ease and speed with which digital platforms can access, transmit, and cross-reference personal data "amplify the potential for violating fundamental rights through the knowledge and control of individuals' personal, private, and social lives" (Sarlet, 2020, p. 181, free translation). This implies that, before any collection or processing of personal data occurs, individuals must be clearly informed and must give their informed consent. Without clear criteria and strict limits, data handling may violate the individual's private sphere.

The core idea of informational self-determination is that individuals must be the primary agents in deciding the fate and use of their information. It is not just about being informed — it is about having the capacity and power to actively influence how one's data is handled.

Informational self-determination must not be confused with the rights to privacy or to data protection. While these rights are interrelated and often overlap, they have different focuses and nuances. Recognizing these distinctions is essential to ensuring effective protection in the digital world.

The right to privacy, although closely linked to informational self-determination, is a broader and older concept that protects individuals against unwanted intrusions into their private lives. Informational self-determination, on the other hand, focuses specifically on the management of personal data, while privacy includes broader aspects of individual intimacy, such as the protection of telephone communications and the inviolability of one's home.

Although these concepts are connected, one can be violated without necessarily affecting the other. For instance, unauthorized phone tapping violates privacy, but if the data is not used or shared, informational self-determination may remain intact.

The right to data protection, which was recently incorporated into Brazil's Federal Constitution through Constitutional Amendment No. 115 of February 10, 2022 (Brasil, 2022), refers to legal and procedural safeguards that ensure personal data is collected, processed, stored, and shared securely and in accordance with applicable regulations. While inherently related to informational self-determination, data protection focuses more on technical

and procedural aspects, whereas informational self-determination emphasizes the subject's autonomy. For example, a company may comply with all data protection rules (e.g., encryption and access control policies) and still violate the principle of informational self-determination by failing to obtain valid consent or by using the data in a way that the individual never truly agreed to.

The principle of informational self-determination was recognized in 1983 by the German Federal Constitutional Court (Bundesverfassungsgericht) in a landmark decision that declared the "Census Law" unconstitutional. The law required German citizens to provide an extensive set of personal data to allow the State to conduct statistical analyses of demographic distribution — both spatial and geographic — and to cross-reference these data with other public records (Bioni, 2021).

As Laura Schertel Ferreira Mendes (2020) observes, this decision marked a turning point in the protection of personality rights, recognizing that the State cannot collect personal data coercively without respecting the individual's private sphere. The ruling established that informational self-determination is an indispensable condition for the free development of personality, placing data protection at the core of fundamental rights.

In 2019, the Bundesverfassungsgericht reaffirmed that the right to informational self-determination is not limited to relations with the State, but also extends to the commercial exploitation of personal data by large technology companies — thus strengthening the horizontal application of fundamental rights in the digital environment. In addressing the consequences of datafication — characterized by the omnipresence of data and the concentration of informational power in the hands of a few platforms — the Court emphasized that individuals must have real control over how their personal data is processed. This control must go beyond a mere formal expression of consent and reflect a concrete exercise of informational autonomy in relation to private entities (Gstrein; Beaulieu, 2022).

More recently, in its ruling on case 1 BvR 1160/19, issued on October 1, 2024 (Germany, 2024), the Bundesverfassungsgericht again examined the constitutional limits of State activity concerning personal data processing. The Court declared several provisions of the Federal Criminal Police Office Act (BKA Act) unconstitutional. These provisions had allowed for disproportionate surveillance of individuals merely associated with suspects — so-called "contact persons" — as well as for the preventive retention of personal data in federal police databases without clear criteria linking the data to the intended purpose of the measure.

In its decision, the Court reaffirmed that the collection and retention of personal data must comply with objective standards of necessity, proportionality, and time limitation. The mere potential usefulness of the data in the future does not, by itself, justify its retention. Legal provisions must establish concrete retention periods and update criteria, as well as mandate the deletion of data once the purpose that justified its collection has been fulfilled. This decision reflects the maturity of German constitutional doctrine in defending the private sphere amid digital surveillance and reinforces the role of informational self-determination as a cornerstone of personality protection in the face of expanding State monitoring technologies and the interoperability of databases.

In Brazil, the Federal Supreme Court (STF) recognized informational self-determination as a fundamental right in its ruling on the Preliminary Injunction in Direct Action of Unconstitutionality No. 6387-DF (MC-ADI 6387-DF), issued on May 7, 2020 (Brasil, 2020). The case concerned the constitutionality of Provisional Measure No. 954 of April 17, 2020, which required telecommunications service providers to transfer user data to the Brazilian Institute of Geography and Statistics (IBGE) during the COVID-19 pandemic (Brasil, 2022). Justice Rosa Weber, in a decision subject to review by the full Court (ad referendum), concluded that such data transfers, without the informed consent of data subjects, would violate, among other rights, the right to informational self-determination:

> The affirmation of the autonomy of the fundamental right to personal data protection must not be attributed to mere theoretical enthusiasm, but rather to the unavoidable need to uphold fundamental rights in contemporary democratic societies. Considering that digital spaces are controlled by economic actors with high capacities for collecting, storing, and processing personal data, the intensification of online communication flows increases the risks of violations of personality and privacy rights (Brasil, 2020, p. 14, free translation).

This decision highlights the concern of STF — Brazil's constitutional guardian — with ensuring that informational self-determination receives constitutional protection in a digital context dominated by economic actors with the power to endanger fundamental rights.

Although years earlier Law No. 13,709 — Brazil's General Data Protection Law (LGPD), enacted on August 14, 2018 — had explicitly recognized the protection of informational self-determination in Article 2, item II (Brasil, 2018), formal recognition of its status as a fundamental right was still necessary. This recognition came with the STF's ruling, which also had the merit of explicitly addressing the risks this right faces in the digital age. The decision thus filled a critical protective gap by confirming the horizontal effectiveness of the fundamental right to informational self-determination.

In the European legal framework, the General Data Protection Regulation ([GDPR], Regulation EU 2016/679) consolidates the protection of the right to informational self-determination by establishing obligations directly applicable to both the State and private entities acting as data controllers or processors. This binding effect stems from Article 1.2, which defines the regulation's objective as the protection of natural persons regardless of the sector (public or private), along with the general principles of data processing (Article 5).

One of the Court of Justice of the European Union's (CJEU) landmark decisions was in the Google Spain case, which established that search engines, as private operators, are subject to the GDPR's obligations. The CJEU recognized the so-called "right to be forgotten" (European Union, 2016, Article 17) as a fundamental right, applicable even in relationships between private parties (CJEU, 2014).

Later, in Schrems II, the Court expanded this interpretation by declaring the Privacy Shield — a data transfer agreement between the EU and the US — invalid, on the grounds that US companies did not ensure a level of protection "essentially equivalent" to that of the EU, as required by Article 45 of the GDPR (CJEU, 2020). This decision reinforced the regulation's extraterritorial reach and the direct accountability of data controllers, including in cross-border data operations, subjecting them to the scrutiny of European fundamental rights (European Union, 2012, Articles 7 and 8).

Moreover, the CJEU emphasized that private companies must independently assess the legality of international data transfers, considering the destination country's domestic legislation and the extent of public authority access to such data (CJEU, 2020).

Digital companies have the potential to deeply impact informational self-determination and must therefore be held accountable when they neglect or violate this right.

The recognition of the right to informational self-determination does not mean that companies are prohibited from processing personal data. Rather, it means that such processing must be carried out transparently, responsibly, and in accordance with constitutional and legal principles, ensuring that individuals retain control and autonomy over their own information.

Because the services offered by digital platforms are fundamentally based on the extensive use of data, they should operate under a rigorous standard of data protection. These entities cannot absolve themselves of responsibility by claiming they are merely private actors. Their role in the digital world places them in a position that, in terms of the magnitude of their responsibilities toward fundamental rights, is comparable to that of public institutions.

The indiscriminate use of data or lack of transparency regarding how data is used and shared can have devastating consequences. Individuals may face violations of privacy or behavioral manipulation — such as microtargeting for political purposes. Thus, it is unacceptable for such platforms to operate in a responsibility vacuum.

It is therefore imperative to recognize and internalize the moral and ethical duty that digital platforms hold. Beyond legal obligations, this reflects a commitment to the dignity and fundamental rights of their users. In light of this scenario, several guidelines can be proposed to improve the Brazilian legal framework for informational self-determination. This is particularly relevant considering that, even when data subjects provide consent for the use of their data, such consent may be insufficient to safeguard their rights. As Silva and Ehrhardt Júnior (2023) observe, this is due to the imbalance of power, cognitive limitations, the essential nature of many digital services, the use of technical and inaccessible language, lack of time to read lengthy contractual terms, and the difficulty in foreseeing future risks associated with personal data processing.

First, the mandatory adoption of institutional data protection policies based on the principles of privacy by design and privacy by default, as outlined in Article 25 of the GDPR (European Union, 2016), is essential. The principle of privacy by design, originally developed in Canada, promotes the proactive and preventive integration of privacy into technological architectures, policies, and organizational practices, so that data protection is not an afterthought but a core and structural element of any system (Cavoukian, 2010). Instead of reacting to privacy violations, the model proposes anticipating and preventing them from the outset by incorporating technical and organizational

safeguards. These include systematic adoption of measures such as data minimization, pseudonymization, and encryption — not as add-ons, but as built-in protections.

The principle of privacy by default ensures that, by default, products and services collect and process only the data strictly necessary for a specific purpose, thereby reducing unnecessary exposure of user data.

Both privacy by design and privacy by default serve as concrete mechanisms for limiting the discretionary power of major digital platforms by establishing objective compliance parameters that precede potential violations.

In Brazil, the LGPD (Brasil, 2018) does not expressly adopt the terms privacy by design and privacy by default, but their underlying principles are implicitly present in the law's normative architecture. This indirect incorporation likely reflects the Brazilian legislature's choice for a more flexible regulatory model. The LGPD uses more open-ended language and assigns the task of elaborating on these principles to the National Data Protection Authority (ANPD) and to jurisprudential development.

Nevertheless, it is possible to identify specific provisions in the LGPD that materially reflect the principles of privacy by design and privacy by default. The principle of prevention (Brasil, 2018, Article 6, item VIII) imposes a duty on data controllers and processors to adopt proactive measures to prevent harm, which implies incorporating safeguards at the design stage of products and services. The principle of data minimization (Brasil, 2018, Article 6, item III), in turn, aligns with the logic of privacy by default, requiring that only data strictly necessary for the intended purpose be collected and processed. Moreover, Article 46 mandates the adoption of technical and administrative security measures to protect personal data, allowing for the incorporation of privacy-protective technologies from the beginning of the data lifecycle.

It is also crucial to establish fast and accessible administrative and judicial mechanisms for resolving disputes concerning personal data processing — similar to the European Union's model, where informational self-determination may serve as a legal basis to hold data controllers accountable for abusive or unauthorized data use. On this topic, Article 82 of the GDPR (European Union, 2016) stipulates that any person who suffers material or non-material damage as a result from unlawful personal data processing has the right to receive compensation from the controller or processor for the damage suffered.

This rule adopts an objective liability model, imposing on the controller the duty to repair damages unless they can prove they were not responsible for the harmful event. It also establishes joint liability between data controllers and processors when both contribute to the same harmful event, thereby ensuring full compensation for the data subject and the right of recourse between jointly liable parties.

This regulatory framework reinforces the centrality of informational self-determination as a fundamental right that demands effective remedies in response to abusive or disproportionate personal data practices. In Brazil, although the LGPD does not contain the same degree of technical detail regarding joint liability, Article 42 does allow for the liability of data controllers and authorizes compensation for both material and moral damages. It therefore provides a normative basis for damages claims based on violations of informational self-determination, even though it does not establish a strict liability regime. As Dantas Bisneto (2020, p. 24, free translation) notes, "the mere violation of data protection law does not automatically give rise to a duty to compensate. It is necessary to demonstrate a violation of a legally protected existential interest." However, "even under a subjective liability regime, fault and agency on the part of the data controller are presumed, and the burden of proof may be shifted with respect to the other elements of civil liability" (Bioni; Dias, 2020, p. 19, free translation).

Jurisprudence must also evolve — for example, by recognizing the presumption of moral damage in cases of violations of informational self-determination, particularly in connection with invisible surveillance practices, microtargeted advertising, or algorithmic exclusion. These issues remain underexplored in both case law and legal scholarship, even as they increasingly affect people's daily lives.

This analysis makes it clear that the framework for protecting the right to informational self-determination in Brazil remains under construction. The experiences of Germany and the European Union may serve as valuable references for improving both the regulatory structure and judicial protection, thereby ensuring the full effectiveness of informational self-determination — a right that has taken on undeniable prominence in the digital age.

4 Final Considerations

Fundamental rights — especially the right to informational self-determination — face unprecedented challenges in the digital age. This article has sought to demonstrate that, as digital platforms become omnipresent in our lives

— collecting and monetizing personal data on a massive scale — users' privacy and informational self-determination are increasingly at risk. This dynamic calls into question the adequacy of the existing regulatory framework and demands a critical reassessment of the applicability of fundamental rights in digital contexts.

The article's objectives were met by highlighting how the right to informational self-determination is affected in digital interactions and by proposing guidelines for strengthening its protection.

It is concluded that a joint effort by governments, companies, civil society organizations, and individuals is imperative to develop policies, regulations, and technological practices that ensure individual autonomy over personal data — thus fostering a more just, inclusive, and democratic digital society.

To this end, the article presented several foreign judicial precedents — such as decisions from the German Federal Constitutional Court and the Court of Justice of the European Union — as well as regulatory experiences like the General Data Protection Regulation (GDPR – European Union, 2016), which incorporates the principles of privacy by design and privacy by default. The GDPR was also referenced to illustrate expedited and accessible mechanisms for resolving personal data-related disputes, particularly regarding joint liability of data controllers and processors.

The challenge lies in ensuring that technological advancements contribute positively to humanity without compromising fundamental rights. Recognizing and strengthening the protection of these rights is therefore an ethical and legal imperative in building a global order that respects the dignity of every human being in the digital world.

References

ALEMANHA. **Urteil vom 1. Oktober 2024, 1 BvR 1160/19.** Leitsätze zum Urteil des Ersten Senats vom 1. Oktober 2024. Karlsruhe: Bundesverfassungsgericht, 2024. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2024/10/rs20241001_1bvr116019.html Acesso em: 14 jun. 2025.

BIONI, B. R. **Proteção de dados pessoais**: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

BIONI, B.; DIAS, D. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **Civilistica**, Rio de Janeiro, v. 9, n. 3, p. 1-23, 2020. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/662. Acesso em: 18 jun. 2025.

BOBBIO, N. **A era dos direitos**. Rio de Janeiro: Elsevier, 2004.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2023]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 maio. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados – LGPD. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 10 maio. 2024

BRASIL. **Ação direta de inconstitucionalidade nº 6387, de 07 de maio de 2020.** Referendo na medida cautelar na ação direta de inconstitucionalidade 6.387 Distrito Federal. Brasília, DF: Supremo Tribunal Federal, 2020. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso em: 10 maio. 2024.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022.** Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Câmara dos Deputados; Senado Federal, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 10 maio. 2024.

BRASIL. **Medida provisória nº 954, de 17 de abril de 2020.** Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial

durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em: 10 maio. 2024.

CANOTILHO, J. J. G. Sobre a indispensabilidade de uma Carta de Direitos Fundamentais Digitais da União Europeia. **Revista do Tribunal Regional Federal da Primeira Região**, Brasília, v. 31, n. 1, p. 69–75, 2019. Disponível em: https://revista.trf1.jus.br/trf1/article/view/17. Acesso em: 04 jun. 2025.

CANTARINI, P. Desafios ao estado democrático de direito - inteligência artificial, direitos fundamentais e constitucionalismo digital. **Revista Jurídica Unicuritiba**, Curitiba, v. 2, n. 74, p. 800–836, 2023. Disponível em: https://revista.unicuritiba.edu.br/index.php/RevJur/article/view/6888/pdf. Acesso em: 05 jun. 2025.

CASTELLS, M. **A sociedade em rede**. São Paulo: Paz & Terra, 2000.

CAVOUKIAN, A. Privacy by design: the 7 foundational principles. Implemation and mapping of fair information practices. **Information Society**, [*s. l.*], v. 3, n. 2, p. 261–267, 2010. Disponível em: https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf Acesso em: 14 jun. 2025.

CELESTE, E. Constitucionalismo digital: mapeando a resposta constitucional aos desafios da tecnologia digital. **Direitos Fundamentais & Justiça**, Porto Alegre, v. 15, n. 45, p. 63-91, 2021. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/1219/1043 Acesso em: 24 jun. 2025.

DANTAS BISNETO, C. Reparação por danos morais pela violação à LGPD e ao RGPD: uma abordagem de direito comparado. **Civilística**, Rio de Janeiro, v. 9, n. 3, p. 1-29, 2020. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/493. Acesso em: 18 jun. 2025.

DONEDA, D. C. M. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. *In:* TEPEDINO, G. (coord.). **Problemas de direito civil-constitucional**. Rio de Janeiro: Renovar, 2000. p. 111-136.

GSTREIN, O. J.; BEAULIEU, A. How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. **Philosophy & Technology**, [*s. l.*], v. 35, n. 3, p. 1-38, 2022. Disponível em: https://link.springer.com/article/10.1007/s13347-022-00497-4. Acesso em: 14 jun. 2025.

LIMBERGER, T. Da evolução do direito a ser deixado em paz à proteção dos dados pessoais. **Revista Novos Estudos Jurídicos**, Vale do Itajaí, v. 14, n. 2, p. 27-53, 2009. DOI: https://doi.org/10.17058/rdunisc.v0i30.580

MENDES, L. S. F. Autodeterminação informativa: a história de um conceito. **Pensar – Revista de Ciências Jurídicas**, Fortaleza, v. 25, n. 4, p. 1–18, out./dez. 2020. Disponível em: https://ojs.unifor.br/rpen/article/view/10828/pdf. Acesso: 24 jun. 2025.

MORAES, A. de. **Direitos humanos fundamentais**: teoria geral. 2. ed. São Paulo: Atlas, 1998.

PARDO, D. W. de A. **Direitos fundamentais não enumerados**: justificação e aplicação. 2015. Tese (Doutorado em Direito) – Centro de Ciências Jurídicas, Universidade Federal de Santa Catarina, Florianópolis, 2015. Disponível em: https://repositorio.ufsc.br/handle/123456789/102251. Acesso em: 24 jun. 2025.

PESSOA, J. P. S.; LIMBERGER, T.; WITSCHORECK, P. V. dos S. O direito à proteção de dados pessoais na fronteira do capitalismo de dados e do colonialismo digital. **Pensar – Revista de Ciências Jurídicas**, Fortaleza, v. 29, n. 4, p. 1-13, out./dez. 2024. DOI: https://doi.org/10.5020/2317-2150.2025.15201

PIOVESAN, F. **Temas de direitos humanos**. São Paulo: Max Limonad, 1998.

RODOTÀ, S. **A vida na sociedade de vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SARLET, I. W. Proteção de dados como direito fundamental na Constituição Federal Brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. **Direitos Fundamentais & Justiça**, Porto Alegre, v. 14, n. 42, p. 179-218, jan./jun. 2020. DOI: https://doi.org/10.30899/dfj.v14i42.875

SILVA, G. B. P; EHRHARDT JÚNIOR, M. Challenges to enforcing informative self-determination under the general law of data protection (GLDP). **Civilistica**, Rio de Janeiro, v. 12, n. 1, p. 1-16, 2023.

SOUZA, J. F. V. de; MEZZAROBA, O. Direitos humanos no século XXI: uma utopia possível ou uma quimera irrealizável? *In:* BAEZ, L. N. X.; SILVA, R. N. da; SMORTO, G. (org.). **Os desafios dos direitos fundamentais na América Latina e na Europa.** Joaçaba: Editora Unoesc, 2012. p. 175-176.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. **Processo C-131/12, de 13 de maio de 2014.** Google Spain SL e Google Inc. contra Agencia Española de Protección de Datos (AEPD) e Mario Costeja González. Luxemburgo: TJUE, 2014. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131. Acesso em: 14 jun. 2025.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. **Acórdão C-311/18 - Facebook Ireland e Schrems, de 16 de julho de 2020.** Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais. Irlanda: TJUE, 2020. Disponível em: https://curia.europa.eu/juris/liste.jsf?num=C-311/18 Acesso em: 14 jun. 2025.

UNIÃO EUROPEIA. Carta dos direitos fundamentais da União Europeia. **Jornal Oficial da União Europeia**, Luxemburgo, 26 out. 2012. Disponível em: https://eur-lex.europa.eu/eli/treaty/char_2012/oj. Acesso em: 02 jun. 2025.

UNIÃO EUROPEIA. **Regulamento 679, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados – GDPR). Bruxelas: UE, 2016. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679 . Acesso em: 02 jun. 2025.

ZUBOFF, S. What is surveillance capitalism? **New Labor Forum**, [*s. l.*], v. 28, n. 1, p. 10-29, 2019. Disponível em: https://www.oru.se/contentassets/911b03b7ff614b14a58782b9ee183bf2/zuboff-2019.pdf . Acesso em: 03 jun. 2025.