pensar
Revista de Ciências Jurídicas
e-ISSN: 2317-2150
Universidade de Fortaleza

Guidelines for protecting the fundamental right to informational self-determination in the digital age[1]

Diretrizes para a proteção do direito fundamental à autodeterminação informativa na era digital

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

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 lack of a regulatory framework capable of guaranteeing their protection. In this context, this article seeks to contribute to overcoming this problem by formulating guidelines aimed at improving the national legal framework, based on the analysis of foreign experiences. To this end, the research adopts a qualitative approach, using deductive and inductive methods, based on a bibliographic and documentary review of national and foreign doctrine and jurisprudence. 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 delves deeper into the study of informational self-determination as an autonomous manifestation of the subject over his/her personal data. The work also examines the regulatory 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 rapid mechanisms for judicial and administrative protection. It is concluded that the protection of informational self-determination constitutes today an ethical and legal imperative for the preservation not only of human dignity, but also for safeguarding trust in the digital ecosystem, undeniably inseparable from life in society in contemporary times.

Keywords: fundamental rights; informational self-determination; data protection; German 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,

[1] Artigo traduzido a partir de Inteligência Artificial.

[*]Doutora em Direito Constitucional pela Universidade Federal de Minas Gerais. Professora Titular do Programa de Pós-Graduação em Direito Constitucional da Universidade de Fortaleza. Bolsista de Produtividade em Pesquisa do CNPq

[**]Mestre e Doutorando em Direito Constitucional pela Universidade de Fortaleza (Unifor). Especialista em Políticas Públicas para Cidades Inteligentes (SmartCities) (Usp), 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.

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 Introduction

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

The transition to a connected society affects both the most industrialized nations and developing economies, configuring a global paradigm based on information technologies (Castells, 2000). Social relations have come to be mediated by digital networks and surveillance systems capable of reorganizing economic and political structures, redefining the contours of private life and individual autonomy.

In this scenario, the collection, storage and monetization of data have become widespread practices, especially by large digital platforms. Although these information flows allow for innovation and personalization of services, they also generate power asymmetries, risks to privacy, algorithmic discrimination and behavioral manipulation. Such vulnerabilities highlight the urgency of a more appropriate legal response.

In view of this reconfiguration of social and legal structures driven by digital technologies, it is essential to rethink the configuration 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 and, at the same time, most relevant rights of this new era.

In this context, this article aims to formulate guidelines for improving the legal framework of the fundamental right to informational self-determination, in view of a still deficient normative structure. In this way, we seek to analyze its emergence as a constitutional response to the asymmetries and risks imposed by contemporary digital logic, which jeopardize the rights of individuals to decide which personal data can be collected and how they can be used.

The research is developed through bibliographic and documentary analysis, of a qualitative and narrative nature, using deductive and inductive methods. The approach mobilizes national and foreign doctrine, as well as case law from the Federal Supreme Court, the German Federal Constitutional Court and the Court of Justice of the European Union, with the aim of offering a critical reading of informational self-determination in the digital society.

In an era of information and interconnection, guaranteeing this right represents an indispensable ethical imperative for safeguarding human dignity, under penalty of remaining as a declaratory right in the face of disproportionate and asymmetrical private structures of informational power.

2 Fundamental rights in the digital age

Fundamental rights are one of the most important pillars on which the Democratic State of Law is built. They are rights that are held by all human beings, regardless of nationality, sex, ethnic or racial origin, religion, language, or any other condition. “A previsão dos direitos humanos fundamentais direciona-se basicamente para a proteção à dignidade humana em seu sentido mais amplo” (Moraes, 1998, p. 22).

These rights encompass several dimensions, including, but not limited to, civil, political, economic, social, and cultural rights, reflecting the complexity and interdependence of the aspects that make up life in society. The affirmation of these rights, of a human nature, “indica, por exemplo, se um Estado pode ou não ser reconhecido como democrático ou se assume ares de barbárie” (Souza; Mezzaroba, 2012, p. 175).

In the civil dimension, fundamental rights focus on the protection of freedom and personal integrity. This includes the right to life, liberty, equality, privacy and property. These rights are essential for the development of the individual, allowing him/her to express himself/herself freely, seek and receive information. Furthermore, “tendem a limitar o poder do Estado e a reservar para o indivíduo, ou para grupos particulares, uma esfera de liberdade e relação ao Estado” (Bobbio, 2004, p. 23).

In the political sphere, fundamental rights guarantee the participation of citizens in political life and in the decision-making processes that affect their lives. This includes the right to vote and be voted for, as well as to hold public office. These are rights of

“participação cada vez mais ampla, generalizada e frequente dos membros de uma comunidade no poder político” (Bobbio, 2004, p. 23).

From an economic point of view, fundamental rights aim to ensure free initiative, in order to protect and promote individual economic development, which will have an impact on the development of the State itself.

In the social sphere, fundamental rights allow the State to be required to implement actions aimed at meeting the minimum conditions for a dignified life, such as labor protection, including, for example, fair and satisfactory remuneration, in addition to fundamental rights for the economic well-being of individuals and their families, such as the right to education, health, assistance to the destitute, social security, and an adequate standard of living. They are essential to ensure that everyone has access to the basic resources necessary to live with dignity and participate fully in society.

Finally, in the cultural dimension, fundamental rights recognize cultural diversity, in order to protect the right of each person to participate in the cultural life of the community to which they belong, enjoying traditions, arts and other manifestations that are part of their own identity.

In short, fundamental rights are the deepest expression of the protection of human dignity, serving 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, which broadens the scope of application of fundamental rights and highlights new vulnerabilities and challenges that arise from their confluence with technology.

And, “no ambiente digital, os atores privados surgem ao lado dos Estados-Nação como potenciais infratores dos direitos fundamentais” (Celeste, 2021, p. 86). Thus, the protection and promotion of fundamental rights require constant interpretative updating in order 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 the protection of personal data becomes central, given the unprecedented capacity to collect, store and process personal information online. Respect for privacy and autonomy over one's own data are

essential to guarantee individual freedom in the digital age. This poses challenges related to mass surveillance, online tracking and the misuse of data by private and government entities.

In the political sphere, the Internet enables an unprecedented dissemination of ideas, promoting citizen participation and democracy. However, it also exposes risks related to digital censorship, disinformation and hate speech online. Ensuring that the digital environment is a space for democratic discourse, respecting diversity of opinions and protecting against abuse, becomes an imperative.

Economically, the digital age has transformed the labor market and the global economy, creating new forms of employment and challenges related to job security, the protection of labor rights, and economic inequality. The ability to work remotely and the gig economy are examples of how economic rights need to be adapted and protected in the digital context.

Socially, digital inclusion is crucial to ensuring that everyone has equal access to public social welfare policies, ensuring that economic inequalities are overcome. However, the need to be digitally connected to public platforms brings with it the risk of losing privacy.

Culturally, the digital context offers new platforms that promote knowledge and exchange between cultures. However, it also raises questions about copyright, cultural appropriation, and the preservation of cultural diversity in the digital age.

Thus, the intersection of fundamental rights with the digital context demands a rebalancing between freedom and security, privacy and transparency, inclusion and diversity. It requires ongoing reflection on how fundamental rights can be effectively exercised and protected in the digital environment, ensuring that technology serves human well-being and promotes a more just and inclusive society. The challenge lies in developing policies, regulations and technologies that respect and strengthen fundamental rights, ensuring that digital advances contribute positively to humanity.

The digital age, characterized by the technological revolution and the ubiquity of information and communication technologies, has brought with it unprecedented transformations in virtually every aspect of human life. These changes have profoundly impacted the way 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 increase in processing power and data storage have enabled greater connection between people and access to an infinite amount of information. However, this same expansion has brought significant challenges to the

protection and promotion of fundamental rights. Issues such as mass surveillance, the collection and misuse of personal data, the spread of disinformation, online hate speech and digital censorship are just some of the emerging problems that require urgent attention.

We have achieved the establishment of a digital identity, but we still do not have a safe space that can be considered its legitimate home. Nor are there effective institutional mechanisms for collective data protection or a cyberspace that guarantees belonging and autonomy. Not even technology giants such as Google and Meta — and even less so the State and its security and information agencies — guarantee this shelter. It is important to recognize, however, that this "digital self" does not correspond to an ontological extension of the subject, but to a relational construction, shaped by systems of continuous surveillance, civil registries, univocal identification of citizens, connected devices, cloud storage, drones, biometric data, communication databases and algorithmic profiling. In this context, guarantees such as privacy, the right to be forgotten, or the possibility of becoming invisible in the digital environment emerge as expressions of new fundamental rights. It is in this context that we can speak of a notion of digital fundamentality (Canotilho, 2019).

In this scenario, Digital Constitutionalism gains prominence, conceived as the theoretical and normative effort to recognize, affirm, and protect fundamental rights in cyberspace, given the asymmetry of informational power between users, corporations, and States. In addition to protecting rights, Digital Constitutionalism seeks to restore balance among the various actors in the digital sphere, addressing the risks posed by surveillance capitalism, the massive and non-consensual extraction of data — the so-called behavioral surplus — and the global practices of informational colonialism that compromise 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, considering that "o reconhecimento e a proteção dos direitos do homem são a base das constituições democráticas" (Bobbio, 2004, p. 223). This implies adapting existing regulatory frameworks and developing new approaches that take into account the particularities of the digital environment. The aim is to ensure that technology acts as a facilitator of freedom and democracy, and not as a tool for their erosion.

In addition, the digital age highlights the need to promote inclusion and ensure that everyone has access to information and communication technologies, as mentioned. After all, the ability to access and use information is fundamental to the exercise of human rights and effective participation in contemporary society.

Therefore, as we navigate this new era, it is essential that governments, companies, civil society organizations and individuals work together to ensure that technology serves the common good, promoting fundamental rights and contributing to a more just, inclusive and democratic society.

3 The fundamental right to informational self-determination on digital platforms

Within the Federal Constitution of 1988 (Brazil, 1988), Brazil enshrined a series of fundamental rights and guarantees, reflecting the democratic aspirations and desires of a society in search of justice, freedom and equality. Such is the importance of these rights and guarantees that the constituent did not limit himself to listing them expressly, but established an opening clause in order to include those that, by chance, had been omitted or that, due to the natural development of society, it was necessary to add them to the constitutional order. This clause is included in article 5, §2, which establishes that the fundamental rights and guarantees provided for in the Constitution do not exclude others derived from the principles or regime adopted by it, or those contained in the international treaties to which Brazil is a party (Brazil, 1988). This rule reflects the intention of the constituent to consider the existence of fundamental rights and guarantees outside the constitutional text, that is, of materially constitutional rules that, due to their quality as axiological parameters, should be considered part of the constitutional order. Along these lines, Piovesan (2006, p. 52) states that "[...] advém de interpretação sistemática e teleológica do texto, especialmente em face da força expansiva dos valores da dignidade humana e dos direitos fundamentais, como parâmetros axiológicos a orientar a compreensão do fenômeno constitucional".

After all, "os direitos fundamentais não se esgotam naqueles direitos reconhecidos no momento constituinte originário, mas estão submetidos a um permanente processo de expansão". (Pardo, 2015, p. 12).

In this context, the notion emerged in the doctrine that informative self-determination, although not expressly provided for as a fundamental right in the Constitution, is implicitly protected as such by the constitutional text, considering that it derives from the fundamental principle of human dignity. The dignity of the human person, consolidated in article 1, section III of the Constitution (Brazil, 1988), is the cornerstone of the Brazilian legal system. This principle is directly related to autonomy, free development and recognition of the intrinsic

value of each human being. In the contemporary digital environment, where information and personal data become extensions of the individual's personality, ensuring their integrity and control becomes imperative to preserve this dignity.

In the current digital environment, companies – and not just the State – play a central role in the collection, processing and storage of personal data. Global technology companies, social networks and online platforms have access to an unprecedented amount of data about individuals, often more than the State itself. And the truth is that "controle sobre os dados pessoais por parte dos titulares é uma ilusão diante da economia digital capitalizada pelas big techs" (Pessoa; Limberger; Witschoreck, 2024, p. 11).

In this context, it is becoming increasingly clear that control over one's personal data is an inseparable part of individual freedom and autonomy of will. As Zuboff (2019) points out, the logic of surveillance capitalism operates through the unilateral extraction of behavioral data, transforming every aspect of daily life into raw material for predictive models. This informational asymmetry, often invisible and unavoidable, compromises the self-determination of individuals by subjecting their choices to algorithmic structures without transparency and commercial interests that are beyond their control. Protecting data, therefore, means protecting the very possibility of acting freely in a digitalized society.

In this sense, the right to informational self-determination consists of the individual's power to decide which personal data can be collected and how it can be used. It is the exercise of autonomy over one's information, allowing one to have control over one's digital identity and personal narrative. One should have the "direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular" (Rodotà, 2008, p.15).

Informational self-determination represents the "direito a controlar o uso que os outros fazem das informações que digam respeito à esfera privada do indivíduo" (Doneda, 2000, p. 120). "Um cadastro pode armazenar um número quase ilimitado de informação. Assim, o indivíduo que confia seus dados deve contar com a tutela jurídica para que estes sejam utilizados corretamente, seja em entidades públicas ou privadas" (Limberger, 2009, p. 58). By conceiving the intimate sphere as a grouping of attitudes, behaviors, preferences, opinions and actions that the subject wishes to preserve under his/her exclusive domain, protection [of privacy] must be based on the "right to informational self-determination" (Doneda, 2020, p. 129).

The ease of access to personal data through digital platforms, in addition to the speed of this access, transmission and its cross-referencing, "potencializa as possibilidades de afetação de direitos fundamentais das pessoas, mediante o conhecimento e o controle de informações sobre a sua vida pessoal, privada e social" (Sarlet, 2020, p. 181). This means that, before any collection or use of data and information, the individual must have clear knowledge and give their informed consent. The handling of personal data, therefore, if not governed by clear criteria and strict limits, can violate this intimate sphere of the individual.

The idea behind this self-determination is that the individual is the main agent in deciding the destination and use of their information. It is not just about being informed, but about having the capacity and power to actively influence decisions about their data.

The right to informational self-determination should not be confused with the right to privacy and the right to data protection, because, although they are interrelated and often overlap, they have different nuances and focuses. It is essential to recognize these differences to ensure their effective protection in the digital world.

Thus, the right to privacy, which is connected to but distinct from the right to informational self-determination, is a broader and older concept that protects the individual from unwanted interference in his or her private life. While informational self-determination is specifically focused on the management of personal data, privacy encompasses a series of broader aspects of individual privacy, such as the protection of one's telephone communications and the inviolability of one's home.

Although both concepts are interconnected, it is possible to have an invasion of privacy without necessarily affecting informational self-determination, and vice versa. For example, wiretapping without consent violates privacy, but if the data collected is not used or shared, informational self-determination may not be compromised.

The right to data protection, recently incorporated into the Federal Constitution through Constitutional Amendment No. 115, of February 10, 2022 (Brazil, 2022), in turn, refers to legal and practical guarantees that ensure that personal data are collected, processed, stored and shared securely and in accordance with established standards. Although it is intrinsically related to informational self-determination, data protection has a more technical and procedural focus, while informational self-determination has an approach centered on the autonomy of the subject holding such data. Thus, for example, it is possible for a company to follow all data protection standards (such as encryption and access policies) but still violate

the principle of informational self-determination by not obtaining adequate consent or by using data in a way that the individual has not actually agreed to.

The principle of informational self-determination was recognized in 1983 by the German Federal Constitutional Court (Bundesverfassungsgericht), when it issued a decision declaring the "Census Law" unconstitutional. The rule prescribed that German citizens should provide a comprehensive set of personal data for the purpose of allowing the State to conduct a statistical analysis on demographic distribution, both in spatial and geographic terms, in addition to allowing these data to be cross-referenced with other types of public records (Bioni, 2021).

This decision represents, as noted by Laura Schertel Mendes (2020), a turning point in the protection of personality, as it recognizes that the State cannot collect personal data in a coercive manner without respecting the individual's private sphere. This judgment confirmed the understanding 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 aforementioned Court once again recognized that the right to informational self-determination is not limited to relations with the State but also extends to practices of commercial exploitation of data by large technology companies, giving greater density to the horizontal application of fundamental rights in the digital environment. When facing the effects of the so-called datafication, marked by the omnipresence of data and the concentration of informational power in the hands of a few platforms, the Court reaffirmed the need for individuals to have real control over the processing of their personal information, not only as a formal expression of consent, but as a concrete manifestation of informational autonomy in the face of private agents. (Gstrein; Beaulieu, 2022).

More recently, in the judgment of case 1 BvR 1160/19, of October 1, 2024 (Germany, 2024), the Bundesverfassungsgericht once again addressed the constitutional limits of state action in the processing of personal data, reaffirming the normative contours of the right to informational self-determination. The Court declared the unconstitutionality of provisions of the Federal Criminal Investigation Office Act (BKA-Gesetz) that authorized, in a disproportionate manner, the invasive surveillance of persons merely linked to suspects — the so-called “contact persons” — as well as the preventive storage of data on federal police platforms, without clear criteria for linking them to the purpose of the measure.

In its decision, the Court reiterated that the collection and storage of personal data must respect objective limits of necessity, adequacy and temporality. The mere potential for future

usefulness does not, in itself, legitimize the conservation of information, and it is essential to legally provide for retention periods and update criteria, in addition to the obligation to delete data when the purpose that justified its collection has been achieved. The decision thus highlights the maturity of German constitutional doctrine in the defense of the private sphere in times of digital surveillance and reinforces the role of informational self-determination as a pillar of personality protection in the face of advances in state monitoring technologies and interoperability between databases.

In Brazil, the Supreme Federal Court recognized informational self-determination as a fundamental right in the judgment of the Precautionary Measure of the Direct Action of Unconstitutionality No. 6387-DF (MC-ADI 6387-DF), on May 7, 2020, in which the constitutionality of Provisional Measure No. 954, of April 17, 2020, which determined the transfer of data from users of telephone services to the Brazilian Institute of Geography and Statistics (IBGE), in the context of the covid-19 pandemic (Brazil, 2022), was debated. Justice Rosa Weber understood, ad referendum of the Court, that such transfer, without the due consent of the holders, would violate, among other rights, informational self-determination:

> A afirmação da autonomia do direito fundamental à proteção de dados pessoais – há de se dizer – não se faz tributária de mero encantamento teórico, mas antes da necessidade inafastável de afirmação de direitos fundamentais nas sociedades democráticas contemporâneas. Considerando que os espaços digitais são controlados por agentes econômicos dotados de alta capacidade de coleta, armazenamento e processamento de dados pessoais, a intensificação do fluxo comunicacional na internet aumenta as possibilidades de violação de direitos de personalidade e de privacidade.

Therefore, the concern of the Supreme Federal Court, guardian of the Constitution, is evident in granting constitutional protection to informational self-determination in the context of the digital age, controlled by economic agents with great power to put fundamental rights at risk.

Although years before, Law 13,709, the General Data Protection Law (LGPD), of August 14, 2018, had expressly provided for the protection of informational self-determination in art. 2, II (Brazil, 2018), it was necessary to formally recognize its status as a fundamental right, which came with this decision of the Supreme Federal Court, which also has the merit of having expressly referred to the risks that this right faces in the context of the digital age. In this way, it filled a serious protective gap by confirming the horizontal effectiveness of the fundamental right to informational self-determination.

In the European legal system, the General Data Protection Regulation (GDPR - EU Regulation 2016/679) (European Union, 2016) consolidates the protection of the right to informational self-determination by establishing obligations directly applicable to the State and private entities that act as controllers or processors of personal data. This express link arises from Article 1.2, which defines the objective of the regulation as the protection of individuals regardless of the sector (public or private), in addition to the general principles of data processing (Article 5).

One of the paradigmatic decisions of the Court of Justice of the European Union (CJEU) was in the Google Spain case, in which it established that search engines, as private operators, are subject to the obligations of the regulation, recognizing the so-called 'right to be forgotten' (Article 17 of the GDPR) as a fundamental right applicable even in relations between private individuals (CJEU, 2014).

Subsequently, in Schrems II, the Court expanded on this understanding by declaring the Privacy Shield — a data transfer agreement between the EU and the US — invalid because it considered that US companies did not guarantee 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 extraterritoriality of the regulation and the direct liability of data controllers, including in cross-border transactions, subjecting them to the scrutiny of European fundamental rights (especially Articles 7 and 8 of the EU Charter).

Furthermore, the CJEU has highlighted that private companies must carry out independent assessments on the legality of international transfers, which must take into account the local legislation of the destination country and the access of public authorities to such data (CJEU, 2020).

Companies operating in the digital environment have the potential to profoundly affect informational self-determination and, therefore, must be held accountable when they neglect or violate this right.

It is worth noting that recognizing the right to informational self-determination does not mean that companies cannot process personal data. It does mean that this processing must be done in a transparent, responsible manner and in line with constitutional and legal principles, guaranteeing individuals control and self-determination over their own information.

The nature of the services offered by digital platforms, which is based on the extensive use of data, makes it imperative that they operate under a rigorous standard of protection. In this sense, entities cannot exempt themselves from their responsibilities by relying on the

argument that they are merely private entities. Their actions in the digital world place them in a position that can be compared to true public entities in terms of the magnitude of their responsibilities towards fundamental rights.

The indiscriminate use of data or the lack of transparency about how this data is used and shared can have devastating consequences. Individuals may face violations of their privacy and manipulation of behavior (such as in the case of microtargeting for political purposes). Therefore, it is unacceptable for such platforms to operate in a vacuum of responsibility.

It is therefore imperative to recognize and internalize the moral and ethical duty that these platforms have. After all, beyond the legislation, this is a commitment to the dignity and fundamental rights of their users. In view of this scenario, some guidelines can be formulated with a view to improving the Brazilian regulatory framework regarding informational self-determination, especially because, even if the data subject provides his/her consent for the use of his/her data, such manifestation may be insufficient to guarantee his/her right, as reported by Silva and Ehrhardt Júnior (2023), given the asymmetry of powers, cognitive limitations, need to enjoy essential services, use of difficult to access technical terms, lack of time to read long contractual terms and the difficulty of predicting future risks arising from the processing of personal data.

Firstly, it is necessary to adopt institutional data protection policies based on the principles of privacy by design and privacy by default, provided for in article 25 of the GDPR (European Union, 20160).

The privacy by design principle, originally conceived in Canada, consists of defending the need to guarantee privacy proactively and preventively in technological architectures, policies and organizational practices, so that data protection is not an afterthought, but an essential and structuring element of the entire system (Cavoukian, 2010). Instead of reacting to privacy violations, the model proposes anticipating and avoiding them from the outset, through the incorporation of technical and organizational safeguards. This includes the adoption of measures such as data minimization, pseudonymization and encryption, which should be incorporated systematically and not as later additions.

The privacy by default principle ensures that, in the default configurations of products and services, only the data strictly necessary for a specific purpose is collected and processed, thus reducing unnecessary exposure of users.

Both privacy by design and privacy by default function as concrete instruments to limit the discretionary power of large digital platforms, establishing objective compliance parameters that precede the occurrence of violations..

In Brazil, the LGPD (Brazil, 2018) did not expressly adopt the terms privacy by design and privacy by default, but their foundations are implicitly and principle-based in its regulatory architecture. This indirect incorporation may reflect an option by the Brazilian legislator for a more flexible regulatory model. The LGPD opts for a more open language, which assigns to the National Data Protection Authority (ANPD), and consequently to the development of case law, the task of densifying these principles. However, it is possible to identify, in the LGPD, provisions that materially translate the principles of privacy by design and privacy by default. The principle of prevention (art. 6, VIII) imposes on data processing agents the duty to adopt proactive measures to prevent the occurrence of damage, which presupposes the incorporation of safeguards from the conception of products and services. The principle of data minimization (art. 6, III), in turn, is in line with the logic of privacy by default, by requiring that only data strictly necessary for the intended purpose be collected and processed. In addition, art. 46 requires the adoption of technical and administrative measures to protect personal data, paving the way for the incorporation of technologies aimed at protecting privacy from the beginning of the information life cycle.

It is also essential to create fast and accessible administrative and judicial mechanisms for resolving disputes regarding the processing of personal data, similar to the experience of the European Union, where informational self-determination can be invoked as a basis for holding data controllers liable for abusive or non-consensual use of personal information. On this subject, article 82 of the GDPR (European Union, 2016) establishes that any person who suffers material or immaterial damage due to the unlawful processing of personal data has the right to compensation from the controller or operator responsible.

The rule adopts an objective logic, imposing on the controller the duty to repair the damage unless it is proven that it had no responsibility for the harmful event. In addition, it establishes joint liability between data processing agents when both contribute to the same harmful event, ensuring the victim full compensation and the subsequent right of recourse between the jointly obligated parties.

This normative structure reinforces the centrality of informational self-determination as a fundamental right, the protection of which requires effective remedies in the face of abusive

and disproportionate practices in the use of personal data. In Brazil, although the LGPD does not detail the mechanisms of joint liability with the same technical quality, its article 42 allows the liability of data processing agents and authorizes compensation for moral and material damages, thus constituting a normative basis capable of supporting compensation actions based on the violation of informational self-determination, despite having failed to provide for a system of objective liability. In other words, “a mera violação da legislação de proteção de dados não gera, automaticamente, o dever de reparar. Faz-se necessário que se comprove a existência de lesão a interesse existencial juridicamente tutelado” (Dantas Bisneto, 2020, p. 24). However, “ainda que o regime seja o de responsabilidade civil subjetiva, a culpa e autoria do agente de tratamento de dados são presumidas e, adicionalmente, pode haver a inversão do ônus da prova quanto aos demais pressupostos da responsabilidade civil” (Bioni; Dias, 2020, p. 19).

Case law must also evolve, for example, in the sense of recognizing the existence of presumed moral damage in cases of violation of informational self-determination, especially when associated with practices of invisible surveillance, advertising microtargeting or algorithmic exclusion, problems that are still little explored in doctrinal and case law, but which are already beginning to be part of people's daily lives.

From this analysis, it is confirmed that the protection arc of the right to informational self-determination is still in the construction process of the Brazilian State. Experiences such as Germany and the European Union can serve as a reference for the strengthening of the normative structure and jurisdictional provision, in order to give full effectiveness to the informational self-determination that, in the digital era, has unquestionably acquired prominence.

4 Final Considerations

Fundamental challenges, especially informational self-determination, face unprecedented challenges in the digital age. This article seeks to demonstrate that, as digital platforms become omnipresent in our lives, collecting and monetizing people's data on a large scale, the privacy and informational self-determination of users is increasingly at risk. This dynamic calls into question the existing regulatory framework and demands a critical reassessment of the applicability of fundamental rights in digital contexts.

The objectives outlined are not addressed, as they become evident as the direction of informational self-determination and impact on digital interactions, in addition to formulating directions to enhance their 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 their given people, thus promoting a more fair, inclusive and democratic digital society.

In this sense, some foreign jurisprudential experiences are presented, such as decisions of the German Federal Constitutional Court and the European Court of Justice, as well as normative experiences, for example the General Regulation on Data Protection (GDPR - EU Regulation 2016/679) that incorporates the principles of privacy by design and privacy by default in GDPR (União Europeia, 2016). We also refer to the GDPR to present some fast and accessible mechanisms for the resolution of disputes relating to the processing of personal data, especially not what refers to the joint liability of controllers and operators.

The challenge lies in guaranteeing that technological advances contribute positively to humanity, without compromising fundamental rights. Reconciling and reinforcing the protection of these rights becomes, therefore, an ethical-legal imperative in the construction of a global order that respects the dignity of every human person in the digital world..

References

ALEMANHA. **Bundesverfassungsgericht. 1 BvR 1160/19** – Urteilvom 1. Oktober 2024. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2024/10/rs20241001_1bvr116019.html Acesso em: 14 jun. 2025.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 3.ed. Rio de Janeiro: Forense, 2021.

BIONI, Bruno; DIAS, Daniel. 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: http://civilistica.com/responsabilidade-civil-na-protecao-de-dados-pessoais/ Acesso em: 18 jun. 2025.

BOBBIO, Norberto. **A Era dos Direitos**. Trad. Carlos Nelson Coutinho. Rio de Janeiro: Elsevier, 2004.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Casa Civil, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm Acesso em:10 maio. 2024.

BRASIL. Supremo Tribunal Federal. **Ação direta de inconstitucionalidade nº 6387/DF – Distrito Federal.** Ação direta de inconstitucionalidade. Direitos fundamentais. Compartilhamento de dados por empresas de telecomunicações prestadoras de serviço telefônico com a fundação Instituto Brasileiro de Geografia e Estatística – IBGE. Suporte à produção estatística oficial durante situação de emergência de saúde pública de importância internacional decorrente do Coronavirus - COVID 19. Alegada violação à inviolabilidade da intimidade, da vida privada, da honra das pessoas e ao sigilo dos dados. Princípio da dignidade da pessoa humana. Direito à autodeterminação informativa. Medida Provisória 954/2020. CF/88, ARTS. 1º, III; 2º; 5º, X E XII; E 62. Relator: Ministra Rosa Weber. Pesquisa de Jurisprudência, Acórdãos, 07 abr. 2020. Brasília, DF: STF, 1988. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629Acesso em: 10 maio. 2024.

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

BRASIL. **Emenda Constitucional nº 115**, **de 10 de fevereiro de 2022.** Brasília, DF: Casa Civil, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm Acesso em: 10 maio. 2024.

CANOTILHO, José Joaquim Gomes. 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, Paola. Desafios ao estado democrático de direito - inteligência artificial, direitos fundamentais e constitucionalismo digital. **Revista Juridica 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: 5 jun. 2025.

CASTELLS, Manuel. **A Sociedade em rede**. São Paulo: Paz e Terra, 2000.

CAVOUKIAN, Ann. Privacy by design: the 7 foundational principles. Identity in the **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, Edoardo. Constitucionalismo digital: mapeando a resposta constitucio-nal aos desafios da tecnologia digital. Tradução de Paulo Rená da Silva Santarém. Revisão de Graziela Azevedo. **Direitos Fundamentais & Justiça**, Porto Alegre, v. 15, n. 45, p. 63-91, Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/1219/1043 Acesso em: 24 jun. 2025.

DANTAS BISNETO, Cícero. 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: http://civilistica.com/reparacao-por-danos-morais-pela-violacao/ Acesso em 18 jun. 2025.

DONEDA, Danilo Cesar Maganhoto Considerações Iniciais sobre os Bancos de Dados Informatizados e o Direito à Privacidade. *In*: TEPEDINO, Gustavo (coord.). **Problemas de Direito Civil-Constitucional**. Rio de Janeiro: Renovar, 2000.

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

LIMBERGER, Têmis. 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, 2° quadrimestre, 2009.

MENDES, Laura Schertel Ferreira. 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, Alexandre de. **Direitos humanos fundamentais**: teoria geral. 2. ed. São Paulo: Atlas, 1998.

PARDO, David Wilson de Abreu. **Direitos Fundamentais não enumerados**: justificação e aplicação. Tese (Doutorado). Centro de Ciências Jurídicas. Universidade Federal de Santa Catarina, Florianópolis, 2015.

PESSOA, João Pedro Seefeldt; Limberger, Têmis; Witschoreck, Pedro Victor dos Santos. 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. Disponível em: https://ojs.unifor.br/rpen/article/view/15201 Acesso em: 24 jun. 2025.

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

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

SARLET, Ingo Wolfgang. 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.

SILVA, Gabriela Buarque Pereira; EHRHARDT JÚNIOR, Marcos. Challenges to Enforcing Informative Self-Determination under the General Law of Data Protection (GLDP). Civilistica, Rio de Janeiro, v. 12, n. 1, 2023. Disponível em: http://civilistica.com/challenges-to-enforcing/ Acesso em: 18 jun. 2025.

SOUZA, José Fernando Vidal de; MEZZAROBA, Orides. Direitos Humanos no século XXI: uma utopia possível ou uma quimera irrealizável? *In:* BAEZ, Leandro Narciso Xavier; SILVA, Rogério Nery da; SMORTO, Guido (orgs). **Os desafios dos direitos fundamentais na América Latina e na Europa.** Joaçaba: Ed. Unoesc, 2012.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA (TJUE). **Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems II)**, Processo C‑311/18, 16 jul. 2020. Disponível em: https://curia.europa.eu/juris/liste.jsf?num=C-311/18 Acesso em: 14 jun. 2025.

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

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**. Jornal Oficial da União Europeia, Luxemburgo, 26 out. 2012. C 326/391. Disponível em: https://eur-lex.europa.eu/eli/treaty/char_2012/oj. Acesso em: 02 jun. 2025.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, 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). Jornal Oficial da União Europeia, L 119, p. 1–88, 4 maio 2016. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679 Acesso em: 02 jun. 2025.

ZUBOFF, Shoshana. 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.