

THE OFFER OF REWARD FOR OBTAINING BIOMETRIC DATA AND DIGITAL VULNERABILITY: A STUDY OF THE WORLD ID PROTOCOL IN LIGHT OF THE GENERAL DATA PROTECTION LAW

*Patricia F. Macedo Possamai **

Abstract: This article examines whether the World ID protocol's offer of financial rewards in exchange for biometric data may compromise valid consent under the Brazilian General Data Protection Law (LGPD). Through deductive reasoning, a case study, and bibliographic and documentary research, it analyzes the legal requirements for processing sensitive personal data, especially biometric identifiers, in light of informational self-determination, qualified consent, and digital vulnerability. The study argues that, although consent remains a central legal basis for data processing, its validity depends on a free, informed, specific, and unambiguous manifestation of will. In the World ID case, the payment of cryptoasset-based rewards, particularly when directed at socioeconomically vulnerable individuals, may operate as undue interference in the formation of consent. The article concludes that such practice may vitiate consent under Article 11(I) of the LGPD and highlights the need for substantive data governance, digital compliance, transparency, and ethical conduct to prevent the abusive exploitation of informational and economic asymmetries in technological environments.

Keywords: biometric data; sensitive personal data; informed consent; digital vulnerability; Brazilian General Data Protection Law.

INTRODUCTION

Computers, software, and networks have been part of everyday life for decades. Yet it was with the spread of the internet and the technological innovations that followed it that profound transformations reached not only technological environments, but also social, economic, and political relations themselves, producing a genuine rupture that Klaus Schwab described as the Fourth Industrial Revolution.¹

Marked by instantaneous communications and by the broad interaction between technology and the most diverse fields of knowledge, this revolution has shortened distances, made it possible to connect people located in different countries simultaneously, and enabled the rapid capture and exchange of information. Among many other consequences, a simple smartphone command now allows research that once required

* Master of Laws in Economic and Social Relations, Milton Campos Law Faculty, Nova Lima/MG, Brazil. Professor of Law at Faculdade Mais de Ituiutaba - FacMais Ituiutaba/MG, Brazil. Email: patricia.possamai@facmais.edu.br / ORCID iD: <https://orcid.org/0009-0007-9256-8523>

¹ Klaus Schwab, *A quarta revolução industrial* 20-21 (Edipro 2016).

visits to libraries.²

In a world characterized by connectivity and by the massive use of technologies for activities ranging from routine tasks, such as ordering transport through an application, to more complex matters, such as monitoring patients through personal assistants that form part of the Internet of Things, the capture and interconnection of data constitute one of the most important pillars on which this new model of society grows.³

At the same time that individuals benefit, as users, from these new technologies, digital platforms collect personal data when a person fills out a store registration form or simply accesses a social network. In many cases, however, users are not clearly informed of the purpose for which their information will be used, who is responsible for processing it, or how long the data will remain under the control of those companies.

For this reason, authors such as Romualdo Baptista dos Santos have argued that, given the contours assumed by the Digital Revolution, society has moved from an information society to a surveillance society, in which individuals are not only exposed and constantly monitored, but in which their personal information is frequently captured and stored without proper authorization or on the basis of flawed consent.⁴

Although the Brazilian General Data Protection Law - LGPD regulates the processing of personal data in Brazilian law and includes the right to informational self-determination, debates remain necessary, including ethical debates, about the manner in which technology companies collect personal data and about the destination given to that information.⁵

In this context, attention is drawn to the World ID protocol launched by Tools for Humanity Corporation (TFH), whose purpose is to form a biometric database by capturing images of individuals' irises, thereby allowing them to prove, safely and anonymously, that the holder of that image is a living human being.

According to reports published in the Brazilian press in recent months, the offer of a financial reward, to be paid in cryptoassets, has led thousands of citizens to make their biometric data available without, in some cases, actually understanding why the company is collecting such data and rewarding them for doing so.

² Thami Covatti Piaia, Bárbara Silva Costa & Miriane Maria Willers, *Quarta Revolução Industrial e a proteção do indivíduo na sociedade digital: desafios para o direito*, 28 *Revista Paradigma* 122, 125 (2019).

³ Silze Cristina Massola & Giuliano Scombatti Pinto, *O uso da internet das coisas (IoT) a favor da saúde*, 15 *Revista Interface Tecnológica* 124, 131 (2018), <https://doi.org/10.31510/inf.v15i2.515>.

⁴ Romualdo Baptista dos Santos, *Responsabilidade civil do Estado na sociedade de vigilância: análise à luz da Lei Geral de Proteção de Dados*, in *Direito público e tecnologia* 397, 404 (Daniela Cravo, Eduardo Jobim & José Luiz de Moura Faleiros Júnior eds., Foco 2022).

⁵ Lei No. 13,709, de 14 de agosto de 2018, *Lei Geral de Proteção de Dados Pessoais (LGPD)*, *Diário Oficial da União [D.O.U.]* de 15.8.2018 (Braz.).

Considering the nature of the data collected through the World ID protocol and the rules established by the LGPD, the central question arises whether the collection of sensitive personal data, such as biometric data, through the promise of financial compensation, could impair the consent granted by the data subject and, therefore, the rule set forth in Article 11(I) of Law No. 13,709/2018.⁶

The relevance of the discussion lies in the fact that the legal provision expressly requires qualified consent by the data subject or legal representative for the processing of sensitive personal data. This opens space for reflection on whether the offer of financial consideration to obtain information may induce data subjects to provide it without actually understanding the reasons behind the collection, thereby vitiating the consent given.

The issue addressed here is capable of raising debate not only about the possible unlawfulness of the conduct carried out by Tools for Humanity Corporation, but also about the ethical questions surrounding the exploitation of the digital vulnerability of a large part of the population.

Accordingly, this article - through the deductive method, a case study, and predominantly bibliographic and documentary research - begins with an analysis of the Brazilian rules on personal data protection, especially informational self-determination and the importance of informed consent, as well as the problem of digital vulnerability. It then examines the World ID case and, finally, assesses whether the offer of a financial reward may configure a defect in the consent of data subjects. It also points to the need to impose ethical and responsible conduct in technological environments, with data governance and digital compliance serving as relevant instruments for that purpose.

The hypothesis defended is that, when financial compensation is proposed for obtaining sensitive data, especially from financially vulnerable groups, there is an exploitation of the informational and socioeconomic vulnerability of those individuals, which may cause the manifestation of will to be guided by such factors and, consequently, to be vitiated.

I. INFORMATIONAL SELF-DETERMINATION AND CONSENT FOR THE PROCESSING OF SENSITIVE PERSONAL DATA UNDER THE BRAZILIAN GENERAL DATA PROTECTION LAW

After approximately ten years of discussion not only in the legislative sphere, but also within Brazilian society, Federal Law No. 13,709 was enacted in August 2018. It regulates the processing of personal data, including in digital media, by natural persons or by public or private legal entities, and aims to protect the fundamental rights of freedom and privacy

⁶ Lei No. 13,709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), Diário Oficial da União [D.O.U.] de 15.8.2018 (Braz.).

and the free development of the personality of natural persons.⁷

The LGPD filled a gap in Brazilian legislation by providing a specific and unified framework for regulating the processing of personal data. As Renato Leite Monteiro notes, it is a statute essentially designed to systematize principles, concepts, foundations, and rights that ensure the protection of data subjects.⁸

Beyond the clarity of the statutory text as to its objective, Article 2 establishes the foundations of the discipline of personal data, including respect for privacy and informational self-determination; freedom of expression, information, communication, and opinion; the inviolability of intimacy, honor, and image; human rights; the free development of personality; dignity; and the exercise of citizenship.⁹

Although this point is no longer controversial, the statute reinforces the implicit fundamental-right nature attributed to personal data protection, evidencing the close relationship between that right and the free development of personality, dignity, and freedom.¹⁰

This close connection between the protection of personal data and the development of personality exists because some of the information encompassed by the concept of personal data expresses characteristics that distinguish one person from another and is therefore included within personality rights. As Bruno R. Bioni teaches, data connected to an individual's life will be considered a personality right when it constitutes a projection or dimension of its holder.¹¹

Establishing the concept of personal data is therefore crucial for the legal analysis proposed here, because only data falling within that definition receives the special protection conferred by the statute.

For that purpose, Article 5(I) of the LGPD defines personal data as any information relating to an identified or identifiable natural person. Although the concept is open-ended, the following item distinguishes sensitive personal data, defining it as data concerning racial or ethnic origin, religious belief, political opinion, union membership, membership in a religious, philosophical, or political organization, health or sex life, genetic data, or biometric data, when linked to a natural person.¹²

From the combination of these legal definitions, it follows that personal data, as information related to the sphere of the individual's

⁷ Lei No. 13,709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), Diário Oficial da União [D.O.U.] de 15.8.2018 (Braz.).

⁸ Renato Leite Monteiro, [complete bibliographic data unavailable] 175 (2021).

⁹ Lei No. 13,709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), Diário Oficial da União [D.O.U.] de 15.8.2018 (Braz.).

¹⁰ Ingo Wolfgang Sarlet, *Proteção de dados pessoais como direito fundamental na Constituição Federal Brasileira de 1988*, 14 *Revista Brasileira de Direitos Fundamentais & Justiça* 179, 185 (2020).

¹¹ Bruno R. Bioni, *Proteção de dados pessoais: a função e os limites do consentimento* 56 (3d ed., Forense 2021).

¹² Lei No. 13,709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), Diário Oficial da União [D.O.U.] de 15.8.2018 (Braz.).

being, must be safeguarded in terms of privacy and accuracy, granting data subjects the broadest possible spectrum of protection.

Nevertheless, although the statute aims to protect privacy, informational self-determination, intimacy, honor, and image, it also expressly includes economic and technological development and innovation among its foundations.¹³

That inclusion is not accidental. The capture, circulation, and storage of personal data are unquestionably among the fuels of contemporary economies and are a true support for new business models and public policies, making society dependent on the informational flow enabled by data.¹⁴

In view of this double function of the LGPD, and of the international data protection framework more broadly, which oscillates between the protection of fundamental rights and economic development, it became necessary to develop a system capable of providing legal certainty to all subjects involved in the chain of data exchange and use.¹⁵

In this sense, the consent of the data subject emerges as the main instrument of control granted to citizens regarding the availability and processing of their personal data, operating as an expression of individual freedom of choice and of informational and existential self-determination.¹⁶

On this point, Danilo Doneda states:¹⁷

Consent, in matters that directly involve personality, today assumes a very specific character. Technological evolution is responsible for expanding the possibilities of choice that may directly affect personality, since several possible configurations relating to privacy, image, personal identity, dispositions over one's own body, and others depend to some extent on a manifestation of private autonomy. Consent, by synthesizing the exercise of private autonomy at a given moment, must be interpreted as the instrument par excellence of individual choice, while also making direct reference to the fundamental values at stake.

The debate on the importance of the data subject's consent is not new.

¹³ Lei No. 13,709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), Diário Oficial da União [D.O.U.] de 15.8.2018 (Braz.).

¹⁴ Bruno R. Bioni, *Proteção de dados pessoais: a função e os limites do consentimento* 107 (3d ed., Forense 2021).

¹⁵ Indyanara Cristina Pini, *O consentimento, os dados sensíveis e a responsabilidade civil na LGPD: uma análise à luz dos contratos de seguro*, 94 *Revista Acadêmica da Faculdade de Direito do Recife* 230, 232 (2022), <https://doi.org/10.51359/2448-2307.2022.251044>.

¹⁶ Chiara Antonia Spadaccini de Teffé & Gustavo Tepedino, *O consentimento na circulação de dados pessoais*, 25 *Revista Brasileira de Direito Civil* 83, 93 (2020), <https://doi.org/10.33242/rbdc.2020.03.005>.

¹⁷ Danilo Doneda, *Da privacidade à proteção de dados pessoais RB-4.6* (2d ed., Thomson Reuters Brasil 2021).

It had already been addressed by the OECD when, in the 1980s, it drafted privacy guidelines that, in addition to ensuring the free flow of information among member countries, established the need for the data subject to be informed of the purpose of data processing so that the subject could authorize it and participate in the informational flow.¹⁸

This measure appears as a way of ensuring what is called the right to informational self-determination, an expression that, although already used in North American doctrine, gained prominence when adopted by the German Constitutional Court in the case challenging the constitutionality of the German Census Act. The expression designated the right of individuals to decide for themselves not only when, but also within what limits, their data could be used.¹⁹

Informational self-determination is one of the foundations not only of German law, but also of the Brazilian General Data Protection Law, which lists it as one of the foundations of data protection and thereby enshrines the individual's right to control personal data and decide both whether to provide information and what will be done with it.²⁰

This is confirmed by the fact that the law defines consent as the free, informed, and unambiguous manifestation by which the data subject agrees to the processing of personal data for a specific purpose. It also provides that personal data processing may be carried out upon the data subject's consent, and that, in the case of sensitive personal data, processing is permitted when the data subject or legal representative consents in a specific and highlighted manner for specific purposes.²¹

Although Faleiros Júnior notes that there is no hierarchy among the legal bases of Articles 7 and 11, it is evident that, because of the nature of sensitive personal data, greater care is required in protecting such information.²²

For this reason, not only the LGPD but also foreign legislation, such as the European Union's GDPR, has given stricter treatment to these data, since the risks linked to them are greater and are correlated with harm to individual fundamental freedoms.

In this field, consent arises as one of the instruments allowing data subjects to exercise greater control over their information, since its manifestation requires that they be informed of the purpose of processing, the destination of the data, the identity of the processing agents, and the

¹⁸ Bruno R. Bioni, *Proteção de dados pessoais: a função e os limites do consentimento* 118 (3d ed., Forense 2021).

¹⁹ Danilo Doneda, *Da privacidade à proteção de dados pessoais RB-2.8* (2d ed., Thomson Reuters Brasil 2021).

²⁰ Lei No. 13,709, de 14 de agosto de 2018, *Lei Geral de Proteção de Dados Pessoais (LGPD)*, Diário Oficial da União [D.O.U.] de 15.8.2018 (Braz.).

²¹ Lei No. 13,709, de 14 de agosto de 2018, *Lei Geral de Proteção de Dados Pessoais (LGPD)*, Diário Oficial da União [D.O.U.] de 15.8.2018 (Braz.).

²² José Luiz de Moura Faleiros Júnior, *Compliance digital y gobernanza: el diálogo interdisciplinario en la era digital*, 1 *Juris Studia* 145, 146 (2024), <https://doi.org/10.52428/30074320.v1i2.940>.

means for revoking authorization.

With respect to sensitive data, the requirement of qualified consent - that is, consent that is highlighted and specific - reveals the need for consent to relate to concrete and well-defined purposes established by the controller. It is essential that the data subject have access to a document providing all relevant information concerning the personal data.

Given the fundamental and existential-right nature of sensitive personal data, consent must be free, specific, highlighted, and directed to predetermined purposes. The processing agent must also refrain from adopting measures that may induce the data subject to a certain behavior, since doing so may remove voluntariness from the manifestation of will and taint the consent granted.

Caitlin Mulholland clarifies this point as follows:²³

Free and informed consent - for purposes of this article, informed consent - is the consent, free of defects, of the data subject, after prior, complete, and detailed access to information about the processing of the data, including its nature, objectives, methods, duration, justification, purposes, risks, and benefits, as well as the subject's full freedom to refuse or interrupt the processing of data at any time, with the controller or processor having the obligation to inform the data subject, in appropriate and nontechnical language, so that the subject may understand it.

The National Data Protection Authority, together with the Superior Electoral Court, in the Guidance Document on the Application of the LGPD by Processing Agents in the Electoral Context, explained:²⁴

Consent will be free when the data subject may choose between accepting or refusing the intended processing without negative consequences or interventions by the controller that may vitiate or impair the manifestation of will.

Consent will be informed when all information necessary for a conscious assessment by the data subject is presented by the processing agent. The data subject must have prior knowledge of the form and period of processing, as well as of the purposes intended by the controller, and any change in the premises adopted for obtaining consent impairs the legal basis adopted, requiring new consent or the use of another legal basis.

Consent must also be unambiguous, meaning that the processing agent must obtain a clear manifestation of will from the data subject,

²³ Caitlin Mulholland, *Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais*, Migalhas (June 22, 2020).

²⁴ Tribunal Superior Eleitoral & Autoridade Nacional de Proteção de Dados, *Guia orientativo: aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) por agentes de tratamento no contexto eleitoral 21-22* (2021).

and it may not be inferred or obtained tacitly or from omission. It is the controller's responsibility to prove that consent was obtained in compliance with all parameters established by the LGPD.

Thus, for consent to be valid, the data subject must not only be clearly informed of the reasons for collection, the form of processing, the identity of the processing agents, and related matters. The subject must also suffer no external interference, direct or indirect, including by the data agent, that could alter or influence the formation of will.

The importance of consent for personal data processing is such that Article 8 of the LGPD prohibits the processing of personal data through defective consent. Although that provision does not expressly refer to sensitive personal data, its application to those cases follows logically from the nature of such data and the greater seriousness of harm caused to the data subject in case of violation.²⁵

Informed consent, which consists of transmitting information clearly and simply so that the data subject may manifest will free of defects, must be a prerequisite for validity, especially with regard to sensitive personal data, since the subject must unequivocally understand the purpose of processing.

At this point, ethical conduct grounded in loyalty and good faith by data processing agents becomes necessary, so that they fulfill their informational duty and allow the data subject to self-determine freely and consciously in deciding whether to provide personal data.

II. DIGITAL VULNERABILITY AND DEFECTS IN CONSENT

Defining the term vulnerability is not one of the easiest tasks for researchers, since delimiting the concept requires attention to the context under analysis. Multiple definitions therefore arise depending on the field of knowledge involved.

In legal science, the study of vulnerability from the perspective of consumer law gained particular prominence after the enactment of the Brazilian Consumer Protection Code, which established vulnerability as one of its principles. The contributions of that field are relevant for analyzing vulnerability in its digital dimension.²⁶

Claudia Lima Marques and Guilherme Mucelin state that, in law, the notion of vulnerability is directly connected to the identification of an individual's fragility in a given legal relationship, arising from inherent conditions or qualities, from a position of strength held by the other subject, from unjustified confrontation of interests in the market, or from the various situations to which subjects are exposed.²⁷

²⁵ Lei No. 13,709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), Diário Oficial da União [D.O.U.] de 15.8.2018 (Braz.).

²⁶ Lei No. 8,078, de 11 de setembro de 1990, Diário Oficial da União [D.O.U.] de 12.9.1990 (Braz.).

²⁷ Claudia Lima Marques & Guilherme Mucelin, Vulnerabilidade na era digital: um

Júlio Camargo Azevedo argues that it is necessary not only to elaborate a notion of vulnerability, but to construct a legal concept endowed with scientific rigor. He defines vulnerability as a situation of predisposition to risk, borne by a subject or group, which, due to historical, social, and cultural determinants, favors a specific condition of human-rights violation and reproduces situations of disrespect, subjugation, power asymmetry, or diminished citizenship, thereby offending dignified existence.²⁸

In delimiting digital vulnerability, Azevedo defines it as a state of predisposition to risk in cyberspaces that favors the appearance of inequities, power asymmetries, diminished citizenship, and violations of privacy, intimacy, and informational self-determination.²⁹

Following Micklitz, Helberger, Strycharz, and others, digital vulnerability is not intrinsic to human beings, but situational, arising from certain conditions or situations to which people are subjected. Individual circumstances may aggravate or mitigate this state of fragility in relation to the environment.³⁰

Because of its specific features, which are largely unknown to many users, the digital environment creates risks capable of increasing this vulnerability and exposing individuals to serious violations of their personality rights.

In this regard, data collected by the Brazilian Institute of Geography and Statistics through the Continuous National Household Sample Survey showed that, in 2023, the internet was used in 92.5 percent of private households in Brazil, with particularly visible expansion in rural areas.³¹

Although the study revealed an increase compared with the data collected in 2022, it also observed a slowdown trend, because the country is approaching the universalization of internet use.³²

Even though the research shows that nearly all Brazilian households have internet access, indicating a trend toward digital inclusion, this does not mean that those people master the use of the internet and all the functionalities it makes available.

estudo sobre os fatores de vulnerabilidade da pessoa natural nas plataformas, a partir da dogmática do Direito do Consumidor, 11 *Civilistica.com* 1, 6 (2022).

²⁸ Júlio Camargo de Azevedo, *Tutela jurisdicional adequada às pessoas em situação de vulnerabilidade* 110 (2019) (Master's dissertation, Universidade de São Paulo), <https://doi.org/10.11606/D.2.2019.tde-24072020-003648>.

²⁹ Júlio Camargo de Azevedo, *Delimitando o conceito de vulnerabilidade digital* - Parte I, *Jota* (Dec. 9, 2021).

³⁰ Hans-W. Micklitz, Natali Helberger, Joanna Strycharz et al., *EU Consumer Protection 2.0: Structural Asymmetries in Digital Consumer Markets* 15 (BEUC 2021).

³¹ Instituto Brasileiro de Geografia e Estatística - IBGE, *Acesso à Internet e à televisão e posse de telefone móvel celular para uso pessoal 2023*, PNAD Contínua 6 (2024).

³² Instituto Brasileiro de Geografia e Estatística - IBGE, *Acesso à Internet e à televisão e posse de telefone móvel celular para uso pessoal 2023*, PNAD Contínua 6 (2024).

It is reasonable to think that many connected users constantly access websites and applications, agree to privacy policies they do not read, accept cookies without knowing what they are, and thus expose their data in virtual environments and authorize their online behavior to be tracked.

At this point, informational vulnerability, so well explored in consumer law, emerges as one of the main risk factors in the digital field as a facet of digital vulnerability. It is not limited to the lack or poor quality of information provided, but also relates to the absence of skill or familiarity with the digital environment, which affects both the interpretation of manifestations made or received in that environment and the ability to respond adequately to one's interests in the resulting legal relationships.³³

Through the collection and processing of user data, digital platforms obtain information and learn, through a digital architecture, how different users interact with cyberspace. This mapping of patterns allows behaviors to be suggested. As systems learn from user experiences and responses to stimuli, their potential to manipulate vulnerabilities increases.

Marques and Mucelin, citing Laura Schertel Mendes, state that at least two situations capable of increasing user vulnerability in personal data processing arise from this scenario: apparent consent and lack of transparency by data agents.³⁴

As analyzed above, user consent for the processing of personal data is a fundamental element of the right to informational self-determination. Any failure, intentional or not, in transmitting information about the purpose and destination of personal data may impair the validity of the manifestation of will.

In other words, if the user is pressured, constrained, or improperly induced to provide data in order to obtain a service, product, or advantage without being properly informed about how the data will be processed, there will be a serious violation of the freedom to consent and, consequently, of informational self-determination.

This is an extreme situation of user vulnerability. As Mônia Clarissa Hennig Leal and Lucas Moreschi Paulo argue, users have difficulty controlling the data they make available through clicks on pop-ups that appear during web browsing.³⁵

A logical consequence of this vulnerability is that, in certain cases, a deficit in the transmission of the information necessary for personal data processing will result in defective consent, which is prohibited by Article

³³ Bruno Miragem, *Princípio da vulnerabilidade: perspectiva atual e funções no direito do consumidor contemporâneo*, in *Direito do Consumidor - 30 anos de CDC 248* (Claudia Lima Marques ed., Forense 2020).

³⁴ Laura Schertel Mendes, [complete bibliographic data unavailable] 18 (2022).

³⁵ Mônia Clarissa Hennig Leal & Lucas Moreschi Paulo, *A Lei Geral de Proteção de Dados, a vulnerabilidade dos usuários da internet e a tutela dos direitos*, 12 *Civilistica.com* 1, 25 (2023).

8(3) of the LGPD.³⁶

As Faleiros Júnior explains in his comments on that statutory provision, a defect in consent in matters of personal data protection, consisting of the inadequate or insufficient obtainment of the data subject's assent, may compromise its legitimacy and validity and create significant risks for data protection.³⁷

The irregularities that may compromise the consent of data subjects are the same ones that affect legal transactions in general, such as mistake, fraud, duress, and simulation, as provided for in the Civil Code.³⁸

Although this correlation is possible, it is essential to note that the object of regulation of the Civil Code and the LGPD differs. The former deals with defects concerning legal transactions, whereas the latter concerns consent obtained in the context of personal data processing, which may or may not occur within a legal transaction.³⁹

This delimitation is relevant because the LGPD hypothesis is narrower. Consent in that statute is a condition for the activity of processing personal data, and when consent results from conduct by the data agent that lacks transparency or is abusive or misleading, it will be considered null under Article 9(1) of the LGPD.⁴⁰

Once again, the need for data agents to act ethically and responsibly becomes evident. They must consider the vulnerabilities of data subjects in light of the peculiarities of digital environments and provide them with all necessary information so that they may consciously form and manifest their will regarding data processing.

III. THE WORLD ID PROTOCOL AND THE ACTION OF THE NATIONAL DATA PROTECTION AUTHORITY

Tools for Humanity Corporation (TFH), founded in 2019 by Alex Blania and Sam Altman, CEO of OpenAI, states on its website that it is a technology company created for humans in the age of AI.⁴¹

In November 2024, representatives of the company met with members of the Board of Directors of the National Data Protection Authority to present the World protocol, one of whose objectives would be to create a

³⁶ Lei No. 13,709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), Diário Oficial da União [D.O.U.] de 15.8.2018 (Braz.).

³⁷ Guilherme Magalhães Martins, João Victor Rozatti Longhi & José Luiz de Moura Faleiros Júnior, *Comentários à Lei Geral de Proteção de Dados Pessoais* (2d ed., Foco 2024).

³⁸ Lei No. 10,406, de 10 de janeiro de 2002, Diário Oficial da União [D.O.U.] de 11.1.2002 (Braz.).

³⁹ Guilherme Magalhães Martins, João Victor Rozatti Longhi & José Luiz de Moura Faleiros Júnior, *Comentários à Lei Geral de Proteção de Dados Pessoais* (2d ed., Foco 2024).

⁴⁰ Lei No. 13,709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), Diário Oficial da União [D.O.U.] de 15.8.2018 (Braz.).

⁴¹ Tools for Humanity, Tools for Humanity (2025), <https://www.toolsforhumanity.com/>.

global identity authentication system enabling individuals to prove, safely and anonymously, that they are living human beings.⁴²

To achieve this purpose, TFH proposes the creation of a decentralized and anonymized identity protocol called World ID, which, according to its website, would make it possible to prove that a particular individual is a unique and real human being, and not an online robot.⁴³

The creation of this unique and anonymous identity, as explained by the technology company, occurs through the capture of images of the data subject's face and iris. This is done through an advanced camera called Orb, manufactured by TFH itself.⁴⁴

In the inspection proceeding initiated by the ANPD, the company explained:⁴⁵

If the Orb determines that the photographs are of a living human, the Orb, without any data being transferred from the device, will examine the photographs of the data subject's eyes and create an abstraction in the form of an iris code. The iris code is a binary code representing the characteristics of the eye photograph. The Orb will then ensure that the iris code is unique, that is, that a similar iris code has not previously been verified, by comparing the iris code with anonymized datasets representing previously verified humans. The comparison effectively returns the technical equivalent of a yes or no as to the existence of the iris code among previously anonymized iris codes, but does not identify or disclose the iris code, which remains anonymized.

If the iris code has not previously been presented, the process may continue. The Orb will then anonymize the data by using a Privacy Enhancing Technology known as Secure Multi-Party Computation. All personal data are deleted from the Orb as soon as the PCP is sent to the user's device. The Orb does not store personal data.

Although the development of more sophisticated technologies for capturing data is neither new nor unknown, global data protection authorities and the broader community were struck by the fact that, to implement the World ID protocol, TFH offered those willing to provide images of their irises a financial reward. The reward would be made available in cryptoassets called Worldcoin (WLD), deposited into the user's World App account, and could be converted into Brazilian currency

⁴² Autoridade Nacional de Proteção de Dados - ANPD, Procedimento de Fiscalização No. 00261.006742/2024-53, doc. 0155038 (Braz. 2024).

⁴³ Tools for Humanity, Tools for Humanity (2025), <https://www.toolsforhumanity.com/>.

⁴⁴ Autoridade Nacional de Proteção de Dados - ANPD, Procedimento de Fiscalização No. 00261.006742/2024-53, doc. 0167854 (Braz. 2024).

⁴⁵ Autoridade Nacional de Proteção de Dados - ANPD, Procedimento de Fiscalização No. 00261.006742/2024-53, doc. 0167854 (Braz. 2024).

and withdrawn after 24 hours.

In Brazil, it is estimated that at the time the project began, the 25 Worldcoin tokens made available to users represented compensation ranging from R\$ 300.00 to R\$ 700.00, depending on the token price at the time of conversion.⁴⁶

In view of these facts, and because the World ID protocol is based on the collection of users' biometric data, more specifically images of the iris and face, which are considered sensitive data under the LGPD, the ANPD initiated Inspection Proceeding No. 00261.006742/2024-53 to assess the protocol's compliance with the LGPD.⁴⁷⁻⁴⁸

Among the concerns raised by the ANPD regarding the World projects are problems related to user consent for the collection of biometric data. The offer of financial compensation could compromise the voluntariness of consent and render it invalid under the LGPD. The Authority also raised concerns about the impossibility of revocation of consent by the data subject and about difficulties in accessing and understanding the terms of use and privacy policy of the protocols, circumstances that could compromise comprehension of the project's objectives.⁴⁹

The ANPD therefore ordered, as a precautionary measure, the immediate suspension by TFH of the financial reward offered for the provision of biometric data by users of the World projects. It also required the company to identify a data protection officer on its website, with the purpose of preventing harm to citizens adhering to the protocols.⁵⁰

The technology company filed an administrative appeal, arguing in summary that it did not retain users' personal data because iris codes were immediately anonymized through decomposition into numerical fragments, making a consent revocation policy unnecessary. It also argued that users' manifestation of will was free, informed, and unambiguous, since they were fully informed of the protocol's purpose and of the control they had over their data. Finally, regarding financial compensation, it argued that data collection was not directly connected to obtaining the reward, because users were merely offered the possibility of requesting a small amount of Worldcoin after providing biometric data, and that Worldcoin was not money but a token with cultural and technological meaning.⁵¹

⁴⁶ Autoridade Nacional de Proteção de Dados - ANPD, Procedimento de Fiscalização No. 00261.006742/2024-53, doc. 0165222 (Braz. 2024).

⁴⁷ Autoridade Nacional de Proteção de Dados - ANPD, Procedimento de Fiscalização No. 00261.006742/2024-53, doc. 0155038 (Braz. 2024).

⁴⁸ Lei No. 13,709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), Diário Oficial da União [D.O.U.] de 15.8.2018 (Braz.).

⁴⁹ Autoridade Nacional de Proteção de Dados - ANPD, Procedimento de Fiscalização No. 00261.006742/2024-53, doc. 0165222 (Braz. 2024).

⁵⁰ Autoridade Nacional de Proteção de Dados - ANPD, Procedimento de Fiscalização No. 00261.006742/2024-53, doc. 0165222 (Braz. 2024).

⁵¹ Autoridade Nacional de Proteção de Dados - ANPD, Procedimento de

The administrative appeal was denied. The main ground used by the data protection authority to maintain the suspension measure was the possibility of defects in the consent obtained by the company. The Authority held that it was necessary to assess whether the offer of financial consideration complied with Article 11(I) of the LGPD, which requires consent to be free. According to the rapporteur, following the ANPD's prior understanding, consent is free only when there is no external interference, including by the controller, capable of directly or indirectly vitiating or impairing the consent granted.⁵²⁻⁵³

The Authority therefore understood that the offer of financial compensation could be considered a form of undue interference in the autonomy of the data subject, especially in cases involving greater vulnerability and economic insufficiency. For that reason, maintenance of the suspension measure remained necessary until further investigation of the case.⁵⁴

The administrative proceeding is still pending. Civil society entities, such as the Brazilian Institute for Consumer Protection (IDEC) and the Institute for Studies on Technology and Law, Aqualtune Lab, have recently entered the proceeding, arguing that the investigations should continue and that sanctions should be imposed if unlawful conduct is proven.⁵⁵

It is also important to note that countries such as Portugal, Spain, and Argentina have already adopted measures to limit or suspend TFH's operations, revealing global concern not only with the company's activities, but also with personal data protection.

IV. THE WORLD ID PROTOCOL, FINANCIAL COMPENSATION FOR OBTAINING BIOMETRIC DATA, AND DEFECTIVE CONSENT

Having set out these considerations, it is necessary to analyze whether the offer of a financial reward for making sensitive personal data available may in fact impair the consent given by the data subject and therefore violate Article 11(I) of the LGPD.⁵⁶

As argued above, because sensitive personal data are involved, the LGPD establishes stricter rules for processing and requires qualified consent from the data subject or legal representative, that is, consent

Fiscalização No. 00261.006742/2024-53, doc. 0167684 (Braz. 2024).

⁵² Autoridade Nacional de Proteção de Dados - ANPD, Procedimento de Fiscalização No. 00261.006742/2024-53, doc. 0167633 (Braz. 2024).

⁵³ Lei No. 13,709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), Diário Oficial da União [D.O.U.] de 15.8.2018 (Braz.).

⁵⁴ Autoridade Nacional de Proteção de Dados - ANPD, Procedimento de Fiscalização No. 00261.006742/2024-53, doc. 0167633 (Braz. 2024).

⁵⁵ Autoridade Nacional de Proteção de Dados - ANPD, Procedimento de Fiscalização No. 00261.006742/2024-53, doc. 0171437 (Braz. 2024).

⁵⁶ Lei No. 13,709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), Diário Oficial da União [D.O.U.] de 15.8.2018 (Braz.).

granted in a specific, highlighted, and informed manner.⁵⁷

The specific study of the World ID protocol in Brazil raises serious questions about the way in which users of the World project have granted consent, especially because press interviews show that the offer of a financial reward has been the main factor leading people to authorize the capture of images of their irises and, consequently, of their biometric data.

According to media reports, approximately 500,000 Brazilians had already made their biometric data available to TFH. It is noteworthy that, although the company's action was initially concentrated in wealthy neighborhoods of São Paulo, it quickly expanded to peripheral areas where residents' income is evidently lower.⁵⁸

In interviews with people at the iris-capture locations, journalists found that many did not know what the World ID protocol was, what to do with the application, or whether there would be risks in providing the photographs. One person interviewed confirmed that he had heard through friends that there was an application giving away money: "I asked, free like that? And they confirmed, free. I came for the money. I'm broke."⁵⁹

In other statements, individuals confirmed that they did not know the reason for the iris scan or how to use the World App, while also indicating that the main incentive for providing the data was the amount offered by the company. It was a matter of doing something different in exchange for an attractive sum.⁶⁰

Considering the economic model prevailing in Brazilian society and the fact that much of the population works informally and survives on approximately one minimum wage, it is a logical consequence that initiatives offering money quickly and easily will attract broad adherence, particularly when campaigns such as World ID are directed at low-income populations.

In this scenario, citizens' vulnerability in relation to new technologies becomes an even greater concern, since such vulnerability is often exploited by companies, placing individuals in situations of extreme exposure and risk.

As noted in Technical Note No. 4/2025/FIS/CGF/ANPD, the offer of financial compensation for obtaining information may interfere with users' free manifestation of will, especially where economically

⁵⁷ Lei No. 13,709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), Diário Oficial da União [D.O.U.] de 15.8.2018 (Braz.).

⁵⁸ Victor Hugo Silva & Darlan Helder, Pagamento por foto da íris atraiu meio milhão de brasileiros, com foco na periferia de SP, até ser barrado pelo governo, G1 Tecnologia (Jan. 25, 2025).

⁵⁹ Victor Hugo Silva & Darlan Helder, Pagamento por foto da íris atraiu meio milhão de brasileiros, com foco na periferia de SP, até ser barrado pelo governo, G1 Tecnologia (Jan. 25, 2025).

⁶⁰ Forbes Brasil, Brasileiros que venderam a íris falam sobre o serviço; empresa entra na mira do governo brasileiro, Forbes (Jan. 16, 2025).

vulnerable individuals are involved.⁶¹

There is no doubt that, in such cases, payment of consideration, even in cryptoassets, may be a determining factor in deciding whether to provide data, since the individual is informed that the token may later be converted into Brazilian reais.

Depending on the Worldcoin exchange rate, a user of the World ID protocol may obtain an amount close to R\$ 700.00, almost half of the Brazilian minimum wage. This creates a potential risk that the will expressed was not free, but conditioned by the offer of reward.⁶²

The issue raised here concerns precisely the manner in which the will of these individuals is formed. For the requirement of freedom to be observed, clear and precise information about which data will be collected, including the nature of the data and the risks in case of leakage, how processing will occur, why collection is being carried out, and how consent may be withdrawn must serve as the starting point.

In the case of the World ID protocol, this point already appears deficient, since information is conveyed in a way that is not very intelligible for users. The World Foundation Biometric Data Consent Form is long and full of details that seem more likely to raise doubts than to provide answers.⁶³

It seems implausible that users who are little accustomed to reading the privacy policies of websites they use daily would devote time to reading the twelve pages of that form. Considering the nature of the data captured by TFH, it would be reasonable to adopt measures for personal clarification of users on the date the Orb captures the photographs, allowing the user to withdraw from the protocol at that moment. Based on the information available so far, such precautionary measures do not appear to have been adopted.

When this informational deficit is combined with the offer of financial compensation, the consideration offered clearly emerges as a determining element in the decision to provide data. Nor can it be argued that the offer lacks financial content, since cryptoassets can be converted into reais and withdrawn.

The issue of reward offers and defects in consent is not new. It has long been addressed in bioethics in connection with payment to volunteers for participation in clinical studies.

Authors such as Aline Albuquerque and Heloisa Barboza argue that, despite existing regulation on the subject, financial reward is incompatible with informed consent because it is capable of annihilating the participant's voluntariness. It interferes with the participant's ability to

⁶¹ Autoridade Nacional de Proteção de Dados - ANPD, Procedimento de Fiscalização No. 00261.006742/2024-53, doc. 0165222 (Braz. 2024).

⁶² Decreto No. 12,342, de 30 de dezembro de 2024, Diário Oficial da União [D.O.U.] de 31.12.2024 (Braz.), establishing the 2025 Brazilian minimum wage at R\$ 1,518.00.

⁶³ Autoridade Nacional de Proteção de Dados - ANPD, Procedimento de Fiscalização No. 00261.006742/2024-53, doc. 0155038 (Braz. 2024).

absorb and analyze information regarding the harms that the clinical research may cause.⁶⁴

Drawing a parallel, without disregarding the differences between the objects of analysis, it seems reasonable to affirm that the offer of financial reward to citizens, especially low-income citizens, constitutes external interference, even if indirect, in the psychological formation of the individual's will. That person may become inclined to provide biometric data without understanding the repercussions that this may have in the individual sphere of rights.

In view of these considerations, it is not unreasonable to state that, as implemented, the World ID protocol has the potential to violate Article 11(I) of Law No. 13,709/2018, since the offer of financial reward is capable of influencing the formation of the data subject's will and thus removing the voluntariness required for validity.⁶⁵

V. COMPLIANCE AND DATA GOVERNANCE AS INSTRUMENTS OF GOOD PRACTICES AND MITIGATION OF THE UNDUE USE OF DATA SUBJECTS' VULNERABILITIES

The analysis carried out so far shows that the issue is not limited to identifying the vulnerability and economic insufficiency of data subjects. It also concerns the improper manipulation of those individuals, which leads to reflection on the responsibility - not only civil, but also ethical - of those who process data.

It is therefore necessary to consider instruments capable of eliminating or at least mitigating the risks arising from activities carried out in technological environments, as well as bringing ethical, loyal, and good-faith standards to the conduct of data processing agents toward users of new technologies.

At this point, data governance and digital compliance emerge as important mechanisms enabling data agents both to respect the rights of data subjects and to pursue their own purposes, which are technological development and, often, profitability.

Digital compliance may be understood as a set of practices, policies, and controls adopted by an organization to ensure that its activities in the digital environment comply with applicable laws, regulations, and ethical standards.⁶⁶

In this technological and globalized environment, in which data have acquired significant monetary importance, it is essential to adopt means

⁶⁴ Aline Albuquerque & Heloisa Helena Barboza, *Remuneração dos participantes de pesquisas clínicas: considerações à luz da Constituição*, 24 *Revista Bioética* 29, 31 (2016), <https://doi.org/10.1590/1983-80422016241103>.

⁶⁵ Lei No. 13,709, de 14 de agosto de 2018, *Lei Geral de Proteção de Dados Pessoais (LGPD)*, *Diário Oficial da União [D.O.U.]* de 15.8.2018 (Braz.).

⁶⁶ José Luiz de Moura Faleiros Júnior, *Compliance digital y gobernanza: el diálogo interdisciplinario en la era digital*, 1 *Juris Studia* 145, 146 (2024), <https://doi.org/10.52428/30074320.v1i2.940>.

that enable technology companies to build a culture of integrity aimed not only at legal compliance, but also at ethical conduct coordinated with the values prevailing in each society.

According to Claudio Joel Brito Lóssio, conduct aligned with digital compliance can modify internal processes and operational controls within companies, producing a behavioral change that goes beyond formal legal compliance.⁶⁷

Data governance policies and digital compliance should perform a preventive role: not only to avoid harm related to cybersecurity, but also to ensure genuine respect for users and for the personal data they entrust to processing agents.

Accordingly, actions such as those carried out by TFH and the World ID protocol, involving financial compensation for the provision of sensitive data, must be assessed not only in light of the formal validity of consent, but also from the broader standpoint of fairness, transparency, accountability, and the prohibition of abusive exploitation of vulnerability.

The LGPD, attentive to the need for preventive instruments in relation to personal data, included in Articles 50 and 51 the possibility for controllers and processors to formulate rules of good practice and governance establishing conditions of organization, operating regimes, procedures, safety standards, technical rules, specific obligations, and educational measures, among other aspects.⁶⁸

A consistent governance program must include mapping of processing activities, risk assessment, definition of legal bases, adoption of security measures, documentation of decisions, review of consent mechanisms, and measures to ensure that information is provided in accessible and intelligible language.

Where sensitive data and vulnerable populations are involved, governance and compliance must be even more demanding. The legality of processing cannot depend solely on formal consent, but must be supported by evidence that the consent was genuinely free, informed, specific, and capable of being revoked.

In this sense, the World ID case illustrates the need for a substantive understanding of data protection compliance. Compliance cannot be reduced to forms, checkboxes, or long privacy policies that users are unlikely to understand. It must require a concrete institutional effort to prevent the exploitation of asymmetries, especially informational and socioeconomic asymmetries.

⁶⁷ Claudio Joel B. Lóssio, *Proteção de dados e compliance digital* 121 (2d ed., Almedina 2023).

⁶⁸ Lei No. 13,709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), Diário Oficial da União [D.O.U.] de 15.8.2018 (Braz.).

CONCLUSION

In light of the foregoing, the advances of the internet over recent decades have brought not only technological changes, but also a profound transformation of social dynamics. They have made communication easier, shortened distances, accelerated transactions, and created new possibilities for individuals, companies, and governments.

Society is increasingly connected and dependent on technologies. Although this has facilitated the routine of citizens, companies, and public authorities, it has also created new risks to personality rights, privacy, intimacy, and informational self-determination.

In this context, the processing of citizens' personal data emerges as one of the central concerns of contemporary society, whether because of technological processes that create detailed profiles of individuals or because of the economic value acquired by personal data in digital markets.

In Brazil, the entry into force of the LGPD represented an important milestone in the attempt to create a regulatory framework for data protection and to prevent the improper use of personal information. The statute established principles, rights, obligations, and rules designed to protect data subjects and to guide the conduct of processing agents.⁶⁹

However, the mere existence of laws does not necessarily lead to conduct consistent with them. Violations of legal rules by those who should observe them remain frequent, especially in environments marked by technical opacity, informational asymmetry, and economic incentives that favor data extraction.

It is in this context that the study of the World ID protocol launched by TFH, in light of the LGPD, becomes relevant. It requires reflection on the legality and legitimacy of collecting sensitive biometric data through the offer of a financial reward.⁷⁰

As argued throughout this article, the offer of financial compensation so that World App users provide biometric data through the World ID protocol is capable of vitiating consent, especially when directed at socioeconomically vulnerable individuals.

Biometric data extracted from the iris constitute sensitive data that, if improperly processed or leaked, may cause serious harm to individuals, since they are linked to unique and permanent characteristics of the person. Unlike passwords or ordinary identifiers, biometric attributes cannot simply be replaced.

For this reason, Article 11(I) of the LGPD requires qualified consent for the processing of such data. This requirement entails not only a duty to inform, but also respect for the voluntariness, specificity, and clarity of

⁶⁹ Lei No. 13,709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), Diário Oficial da União [D.O.U.] de 15.8.2018 (Braz.).

⁷⁰ Lei No. 13,709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), Diário Oficial da União [D.O.U.] de 15.8.2018 (Braz.).

the manifestation of will.⁷¹

By offering financial compensation for the collection of biometric data, especially when the offer is directed at low-income individuals, as occurred in the World ID case when the initiative expanded to peripheral regions, the company creates a strong incentive capable of interfering with the formation of consent.

The expectation of receiving money in exchange for what may appear to be mere photographs of the eyes and face is, in fact, a factor capable of guiding the decision to be made. Where there are doubts, informational deficits, or lack of understanding about the risks involved, the apparent freedom of consent becomes fragile.

The matter addressed here therefore concerns not only the need for technology companies to adopt measures ensuring proper compliance with the LGPD, but also the indispensable requirement that such companies act ethically, responsibly, and in good faith when dealing with individuals whose vulnerabilities may be intensified in digital environments.

From this perspective, data governance and digital compliance appear as valuable instruments for preventive action. They make it possible to ensure that companies act not only in formal conformity with the law, but also in a way that effectively protects data subjects and prevents the undue exploitation of their vulnerabilities.

REFERENCES

- Albuquerque, Aline & Barboza, Heloisa Helena. Remuneração dos participantes de pesquisas clínicas: considerações à luz da Constituição, 24 Revista Bioética 29 (2016), <https://doi.org/10.1590/1983-80422016241103>.
- Autoridade Nacional de Proteção de Dados - ANPD. Procedimento de Fiscalização No. 00261.006742/2024-53 (Braz. 2024).
- Azevedo, Júlio Camargo de. Tutela jurisdicional adequada às pessoas em situação de vulnerabilidade (2019) (Master's dissertation, Universidade de São Paulo), <https://doi.org/10.11606/D.2.2019.tde-24072020-003648>.
- Azevedo, Júlio Camargo de. Delimitando o conceito de vulnerabilidade digital - Parte I, Jota (Dec. 9, 2021).
- Bioni, Bruno R. Proteção de dados pessoais: a função e os limites do consentimento (3d ed., Forense 2021).
- Brasil. Lei No. 8,078, de 11 de setembro de 1990, Diário Oficial da União [D.O.U.] de 12.9.1990.
- Brasil. Lei No. 13,709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), Diário Oficial da União [D.O.U.] de 15.8.2018.

⁷¹ Lei No. 13,709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), Diário Oficial da União [D.O.U.] de 15.8.2018 (Braz.).

- Brasil. Decreto No. 12,342, de 30 de dezembro de 2024, Diário Oficial da União [D.O.U.] de 31.12.2024.
- Doneda, Danilo. Da privacidade à proteção de dados pessoais (2d ed., Thomson Reuters Brasil 2021).
- Fagundes, Priscila Basto; Macedo, Douglas Dyllon Jeronimo de & Freund, Gislaine Parra. A produção científica sobre qualidade de dados em big data: um estudo na base de dados Web of Science, 16 RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação 194 (2017).
- Faleiros Júnior, José Luiz de Moura. Compliance digital y gobernanza: el diálogo interdisciplinario en la era digital, 1 *Juris Studia* 145 (2024), <https://doi.org/10.52428/30074320.v1i2.940>.
- Forbes Brasil. Brasileiros que venderam a íris falam sobre o serviço; empresa entra na mira do governo brasileiro, *Forbes* (Jan. 16, 2025).
- Instituto Brasileiro de Geografia e Estatística - IBGE. Acesso à Internet e à televisão e posse de telefone móvel celular para uso pessoal 2023, PNAD Contínua (2024).
- Leal, Mônia Clarissa Hennig & Paulo, Lucas Moreschi. A Lei Geral de Proteção de Dados, a vulnerabilidade dos usuários da internet e a tutela dos direitos, 12 *Civilistica.com* 1 (2023).
- Lóssio, Claudio Joel B. Proteção de dados e compliance digital (2d ed., Almedina 2023).
- Marques, Claudia Lima & Mucelin, Guilherme. Vulnerabilidade na era digital: um estudo sobre os fatores de vulnerabilidade da pessoa natural nas plataformas, a partir da dogmática do Direito do Consumidor, 11 *Civilistica.com* 1 (2022).
- Martins, Guilherme Magalhães; Longhi, João Victor Rozatti & Faleiros Júnior, José Luiz de Moura, eds. Comentários à Lei Geral de Proteção de Dados Pessoais (2d ed., Foco 2024).
- Massola, Silze Cristina & Pinto, Giuliano Scombatti. O uso da internet das coisas (IoT) a favor da saúde, 15 *Revista Interface Tecnológica* 124 (2018), <https://doi.org/10.31510/infa.v15i2.515>.
- Micklitz, Hans-W.; Helberger, Natali; Strycharz, Joanna et al. EU Consumer Protection 2.0: Structural Asymmetries in Digital Consumer Markets (BEUC 2021).
- Miragem, Bruno. Princípio da vulnerabilidade: perspectiva atual e funções no direito do consumidor contemporâneo, in *Direito do Consumidor - 30 anos de CDC* 248 (Claudia Lima Marques ed., Forense 2020).
- Monteiro, Renato Leite. [complete bibliographic data unavailable] (2021).
- Mulholland, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais, Migalhas (June 22, 2020).
- Piaia, Thami Covatti; Costa, Bárbara Silva & Willers, Miriane Maria. Quarta Revolução Industrial e a proteção do indivíduo na sociedade digital: desafios para o direito, 28 *Revista Paradigma* 122 (2019).

- Pini, Indyanara Cristina. O consentimento, os dados sensíveis e a responsabilidade civil na LGPD: uma análise à luz dos contratos de seguro, 94 Revista Acadêmica da Faculdade de Direito do Recife 230 (2022), <https://doi.org/10.51359/2448-2307.2022.251044>.
- Santos, Romualdo Baptista dos. Responsabilidade civil do Estado na sociedade de vigilância: análise à luz da Lei Geral de Proteção de Dados, in Direito público e tecnologia 397 (Daniela Cravo, Eduardo Jobim & José Luiz de Moura Faleiros Júnior eds., Foco 2022).
- Sarlet, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal Brasileira de 1988, 14 Revista Brasileira de Direitos Fundamentais & Justiça 179 (2020).
- Schwab, Klaus. A quarta revolução industrial (Edipro 2016).
- Silva, Victor Hugo & Helder, Darlan. Pagamento por foto da íris atraiu meio milhão de brasileiros, com foco na periferia de SP, até ser barrado pelo governo, G1 Tecnologia (Jan. 25, 2025).
- Teffé, Chiara Antonia Spadaccini de & Tepedino, Gustavo. O consentimento na circulação de dados pessoais, 25 Revista Brasileira de Direito Civil 83 (2020), <https://doi.org/10.33242/rbdc.2020.03.005>.
- Tools for Humanity. Tools for Humanity (2025), <https://www.toolsforhumanity.com/>.
- Tribunal Superior Eleitoral & Autoridade Nacional de Proteção de Dados. Guia orientativo: aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) por agentes de tratamento no contexto eleitoral (2021).

* * *

Patricia F. Macedo Possamai

Master of Laws in Economic and Social Relations, Milton Campos Law Faculty (2025). LL.B., Centro Universitário Curitiba - UNICURITIBA (2011). Specialist in Applied Law, Escola de Magistratura do Paraná - EMAP (2014); Specialist in Social Security Law - Social Security and Social Security Practice, Faculdade Legale (2022); and Specialist in Public Procurement and Contracts, Escola Mineira de Direito - EMD (2024). Former Legal Advisor at the Office of the Prosecutor General of the Public Prosecutor's Office of the State of Paraná - MPPR (2011-2020), working in judicial proceedings in Administrative, Constitutional, Civil, and Criminal Law. Attorney practicing in Social Security, Administrative, and Civil Law, and Professor of Law at Faculdade Mais de Ituiutaba (FacMais Ituiutaba).

Email: patricia.possamai@facmais.edu.br

ORCID iD: <https://orcid.org/0009-0007-9256-8523>