


THE INVALIDITY OF THE CONSENT GIVEN BY THE HOLDER FOR FINANCIAL CONSIDERATION - ANALYSIS OF THE TOOLS FOR HUMANITY (TFH) CASE

 <https://doi.org/10.56238/arev7n4-188>

Submitted on: 16/03/2025

Publication date: 16/04/2025

Beatriz de Andrade Vieira¹, Wellington Cardoso Silva Júnior².

ABSTRACT

The article analyzes the legal validity of the consent obtained through financial consideration for the processing of sensitive personal data, in light of the General Law for the Protection of Personal Data (Law No. 13,709/2018), focusing on the case of the company Tools for Humanity (TfH), responsible for the Worldcoin project. The research adopts a qualitative approach, based on a literature review, normative analysis and concrete case study, problematizing the ethical-legal limits of the autonomy of the will in contexts of socioeconomic vulnerability. Consent, although provided for as a legal basis by the LGPD, requires requirements of freedom, information, specificity, and clarity. However, obtaining it through financial incentives can compromise the holder's freedom of expression, especially when aimed at populations in situations of socioeconomic inequality. The collection of biometric data, such as the iris and face, in exchange for tokens convertible into cryptocurrencies, highlights risks to informational self-determination, revealing a possible imbalance in the relationship between controller and data subject. It is concluded that consent conditioned to economic advantages lacks legal validity when it compromises the decision-making freedom of the holder, and is not a legitimate basis for the processing of sensitive data.

Keywords: LGPD. Assent. Sensitive data. Financial consideration.

¹ Lawyer

Postgraduate student in Lato Sensu Specialization in New Rights at UFF
Email: beatrizandradevieira@hotmail.com

² Infrastructure and Information Security Team Leader

Graduated in Information Systems from Universidade Veiga de Almeida and postgraduate in Defensive Cyber Security from FIAP
E-mail: well.cardosojr@outlook.com

INTRODUCTION

In the face of the growing collection of personal data in the digital environment, the notion of consent has gained centrality as an expression of informational self-determination. Provided as one of the legal bases for data processing by Law No. 13,709/2018, known as the General Law for the Protection of Personal Data (LGPD), consent must be free, informed, unambiguous, and specific, reflecting the autonomy of the holder in deciding on the use of their own data.

However, in practice, the validity of consent is not always assured. In contexts marked by socioeconomic inequality, the offer of financial consideration can compromise the holder's freedom of choice, making consent only apparent. Material advantages, even if formally accepted, can act as mechanisms of induction or economic coercion, especially when directed at groups in situations of vulnerability.

According to Mecabô (2021), personal data has assumed, in contemporary times, the role of economic assets, exerting a direct influence on the free development of individuals' personalities. Although several legislations around the world, including the LGPD, attribute centrality to consent as a basis for data processing, such a mechanism, by itself, is not sufficient to ensure informational self-determination. In this scenario, important ethical-legal questions arise about the limits of the validity of consent obtained through the promise of benefits.

This problem became particularly visible in the case of the company Tools for Humanity (TfH), responsible for the operation of the Worldcoin project in Brazil. The initiative involves the collection of sensitive biometric data, especially iris, by promising cryptocurrency rewards. The performance of the National Data Protection Authority (ANPD), in determining the suspension of activities and imposing requirements aimed at transparency and informational neutrality, revealed the tensions between technological innovation, personal data protection, and the supposed voluntariness of consent.

In view of this, this article aims to analyze the legal validity of consent for the processing of personal data when conditioned to financial consideration, in the light of the case of TfH. The research adopts a qualitative approach, based on a bibliographic review and normative and factual analysis of the referred concrete case. Thus, it seeks to contribute to the debate on the limits of the autonomy of will in the sphere of data protection and the role of the State in mitigating practices that, even if based on formal consent, may constitute a violation of fundamental rights.

CONSENT AS A LEGAL BASIS FOR THE PROCESSING OF SENSITIVE DATA

The LGPD establishes, in article 7, ten legal bases that justify the processing of personal data. These hypotheses determine under which conditions the data can be processed according to the purpose informed to the holder. Among them, consent stands out, which, at first, may seem like a simple solution to obtain the holder's authorization. However, its inappropriate use can demonstrate the complexity of its manifestation, so as to open the door to worrying precedents.

According to article 5 of the law, item XII, consent is the free, informed and unequivocal manifestation of the holder, authorizing the processing of his or her personal data for a specific purpose. This means that consent must be free, ensuring that the choice of the holder occurs without any form of imposition or pressure; informed, ensuring transparency regarding the collection, use, purpose and sharing of data; and unequivocal, requiring a clear, explicit and undoubted statement by the holder.

The data subject has the right to maintain control over their own information, enabling them to know, manage, direct and even interrupt the flow of data related to their data. In this context, the concept of informational self-determination emerges, which gives the individual the power to control the collection, possession, processing, and transmission of their personal data. As a result, attention has shifted to the consent of the data subject, evolving from implicit consent, when there is no clear manifestation, to informed consent, in which the data subject is duly informed about the use of his or her data (TEPEDINO; TEFFÉ, 2021)

There is a shift in the approach to consent, leaving aside the implicit presumption, in which the individual's behavior is interpreted as a tacit acceptance, as in the case of pop-ups with long contracts in reduced print that are signed with a simple touch, to an informed consent, in which the holder's decision is made based on clear and accessible information, that allow you to fully understand the implications of your choice. This model seeks to ensure that the data subject receives clear and detailed information about the collection, use, sharing, and storage of their data, anticipating risks of privacy violations and adopting a preventive nature (BONNA; CAÑIZO; CALZAVARA, 2024)

The LGPD establishes specific criteria for the processing of sensitive personal data, such as biometrics, raising discussions about whether or not it is necessary to obtain the consent of the data subject. An elucidative example is the collection of facial biometrics and

fingerprints from residents of a condominium, in order to control access to the premises and reinforce security. In this case, according to article 11, item II, paragraph 'g' of the LGPD, the processing of sensitive data may occur without the consent of the holder when it is indispensable for the prevention of fraud and the security of the holder, especially in identification and authentication processes in electronic systems. Therefore, the condominium is authorized to carry out such processing, as long as it respects the fundamental rights and freedoms of the holder and provides clear information about the purpose and use of the data. (HULBERT, 2023)

In contrast, the case of the company Tfh presents a different situation. The company collected biometric data from the iris of individuals, offering financial rewards in cryptocurrencies as consideration. In this case, the legal basis used was the consent of the holder. However, questions arise about the authenticity of this consent, especially considering the offer of financial benefits that can influence the holder's decision, compromising freedom of choice.

In addition, data collection in regions with greater socioeconomic vulnerability intensifies ethical and legal concerns, since financial consideration can be perceived as a form of economic coercion. Thus, while in the condominium context the processing of biometric data is justified by an objective legal basis related to security; in the case of TFH, the validity of the consent obtained is questionable, evidencing the complexity and challenges in applying the LGPD in different scenarios.

3 CONTEXTUALIZATION OF THE TFH CASE

The TFH company, with headquarters in California, USA, and Munich, Germany, defines itself as a technology company focused on development for humanity in the age of artificial intelligence. The company is responsible for manufacturing the advanced Orb camera, used to collect data from the iris, face and eyes of holders, with the aim of developing a unique human identity verification system, known as World ID. (WORLD COIN, 2024)

The initiative is part of the *Worldcoin* Project, whose goal is to create a global identity authentication system, allowing individuals to prove their identity and their real existence, in contrast to automated or bot-created records. To this end, the company manages the implementation of a digital identity called *World ID*, obtained through the automated reading of physical characteristics extracted from images of the face and iris of users. In this way,

when interacting with a digital service linked to the entity's platform, the user would be able to demonstrate that it is a human being and not an automated system simulating an individual identity.

One of the main requirements and materials for the use of this service is the collection of images of the retina of data subjects. According to the company's representatives, personal data processing operations under the *Worldcoin Project* would be in compliance with the LGPD.

However, the World ID Protocol has been the subject of analysis by several national personal data protection authorities, which raise questions about possible violations of users' rights to privacy and data protection. An example of this concern is Resolution No. 2024/137, issued by the National Data Protection Commission (CNPd) of Portugal, which, as part of a preliminary investigation, detailed the functioning of World ID and the procedures for processing biometric data. (CNPd, 2024)

Among the data collected, the images of the iris and eyes, obtained in the visible and near-infrared spectrums, stand out. In addition, images of the face are captured in the visible and infrared spectrums, both in near and far perspectives, including depth (3D) images. This information is used to verify the user's vitality, contributing to fraud prevention and the improvement of the algorithm for detecting fraudulent behavior. Along with iris images, such information is categorized as "Image Data."

In addition to the captured images, the system generates numerical representations called "Derivatives", through advanced algorithms and custom neural networks. These representations allow automated comparisons between the data collected, without allowing the full reconstruction of the original images. To ensure the uniqueness of users' registration on the platform, the company adopts a customized version of the Daugman Algorithm³ to calculate the so-called "Iris Code", an identifier that aims to avoid multiple records of the same individual. This code is then compared in real time with an existing database to check if the user has already been registered in the World ID system.

After the generation and insertion of the Iris Code in the database, the images captured by *the Orb* can be immediately destroyed or temporarily stored on the device until they are sent to the Worldcoin Foundation's systems, if the data subject has consented to

³ According to Souza and Pereira (2021), the algorithm for iris recognition, developed by scientist John Daugman in 1993, is structured in six steps: localization and segmentation, normalization, extraction and coding of attributes, and classification of iris patterns.

its subsequent use. Orb also has the ability to encrypt and store the data, sending it to the Worldcoin Foundation's servers hosted on Amazon Web Services (AWS).

To join the system, users must previously install the company's application called World App on their electronic devices, which also works as a digital cryptocurrency wallet. The membership process requires the creation of an account, the linking of a phone number, the confirmation of the age of majority (18 years or older), in addition to the acceptance of the privacy policy and the terms of use of the service. After these steps, the user receives a *QR Code* on their cell phone, which, when scanned by the *Orb*, authorizes the capture of biometric images and the generation of the Iris Code.

The process is completed by sending the generated code to the Worldcoin Foundation's systems and downloading the World ID to the user's mobile device. In return for the transfer of their biometric data, each adherent receives *tokens* that correspond to cryptocurrencies, which can, in some circumstances, be converted into physical currency. This financial incentive has been a determining factor for the growing adhesion to the project.

According to the Deliberation of the CNPD of Portugal, Orb operators are instructed to encourage users to consent to the conservation and use of their biometric images by Worldcoin, arguing that this practice benefits the holders themselves by avoiding the need for new captures with each update of the Iris Code generation algorithm, which occurs approximately three times a year. However, according to the document, although the algorithm developed aims to avoid duplication, failures may occur, resulting in the mistaken identification of users already registered in the system.

As a result, the CNPD, in March 2024, decided to suspend the collection of biometric data from the iris, eyes, and face of data subjects carried out by the Worldcoin Foundation, with a view to safeguarding the fundamental right to the protection of personal data, especially of minors. The authority, in this sense, ordered the controller to precautionarily suspend the processing of biometric data of users of the World Protocol, for a period of ninety days, until its investigation was completed and a final decision was also issued. (CNPD, 2024)

In the same move as the Portuguese commission, the ANPD initiated process No. 00261.006742/2024-53, a preliminary analysis for the opening of an administrative inspection procedure, under the terms of the Inspection Regulation, according to Resolution CD/ANPD No. 1, of October 28, 2021, to investigate the processing of biometric data of

users of the World ID Protocol. At the time of its establishment, more than 400 thousand Brazilians had their iris scanned by the company. In November of the previous year, when the project resumed in São Paulo after the testing phase carried out in 2023, this number was only 115 thousand. (G1, 2024)

4 WEAKNESSES OF CONSENT IN THE TFH CASE

The attribution granted to consent in the processing of personal data carries an essential character, and the importance of this element for the legitimacy of operations involving data subjects is recognized. However, it is necessary to recognize that consent, by itself, should not be considered the final word or the absolute basis to legitimize any processing, especially when there are weaknesses in obtaining or applying it. In this sense, Bioni (2019) warns of the need to move away from a view that attributes to consent the function of unrestrictedly legitimizing any and all processing of personal data, a conception that the author calls the "myth of consent".

In the context of the TFH case, the need to examine the influence of financial incentives on the decision of the data subject is highlighted, as well as the role of socioeconomic vulnerability in the process of granting consent for the processing of personal data. Such factors can compromise the freedom and authenticity of this consent, generating situations of imbalance and possible exploitation of the holder. In view of this, it is relevant to search for alternatives that promote obtaining consent in a more impartial way, minimizing biases and ensuring greater protection of the autonomy and rights of the holders.

THE ROLE OF SOCIOECONOMIC VULNERABILITY

In Brazil, according to the Brazilian Institute of Geography and Statistics (2024), the percentage of the population below the poverty line reached 27.4% in 2023. In the same year, the rate of young people between 15 and 29 years old who were neither studying nor employed reached 21.2%. This scenario, marked by the lack of basic resources and the high rate of educational and professional inactivity, generates a context of vulnerability that can directly impact autonomy in decision-making. Given this situation of socioeconomic vulnerability, the ability of individuals to critically assess the benefits and risks involved in the processing of their data may be compromised, raising questions about the authenticity and effectiveness of the consent granted.

In this sense, according to data from the Internet Steering Committee in Brazil (2024), Brazilians are more concerned about providing biometric data than about other types of sensitive information, such as sexual orientation and color or race. Despite this concern, the study reveals that, in 2023, 58% of Internet users aged 16 and over stated that they always (26%) or almost always (32%) agree to privacy policies without reading their content. Given this scenario, it is necessary to reflect on whether consent, as it has been applied, is really sufficient to ensure the protection of personal data, or whether its structure should be rethought in order to ensure greater effectiveness.

In addition, according to Mendes and Fonseca (2020), the consent paradigm faces a limitation related to the data subject and his cognitive decision-making process. From this perspective, the individual is seen as someone who seeks to maximize their interests, evaluating the costs and benefits of consenting or not to the terms presented. If you have a good understanding of the use of your personal data, you will be able to weigh the impacts on your privacy and compare them to the benefits, such as access to an online service. Thus, you will make decisions about what to consent to and what not to consent to, always based on your best interest, after reviewing the privacy terms provided.

Based on the information made available, therefore, it is assumed that the individual is able to make rational, grounded and effectively autonomous decisions. However, a dilemma arises when questioning the extent to which the data subject has the cognitive capacity necessary to make assertive decisions about consent, taking into account their cognitive limitations. It is not, obviously, a matter of "infantilizing" the holder, treating him as incapable of deciding for himself or ignoring his rational capacity. However, the excessive focus on obtaining their apparently informed consent often ignores a more complex aspect: the real ability of the personal data subject to understand and substantially assess the risks and harms that may arise from their consent, especially in the online environment.

For consent to validate data processing, it is assumed that the individual decides in a rational, reasoned and autonomous manner. However, by offering a benefit, there is a risk of coercing the user to authorize the use of their data without their full conviction. This was evident in an action carried out by the British company Purple, which offers free Wi-Fi and *hotspots* for stores and public areas. The company has demonstrated that many people do not read the terms of the contract, accepting any information that is written in the document. During the action, one of the clauses to access the *company's hotspots* required the user to accept to perform a thousand hours of community service, with activities such as

cleaning public bathrooms, sewer pipes and scraping gum from public roads. (BONFIM, 2017)

The company announced that, in the two weeks of the campaign, about 22 thousand people accessed the *hotspots*, but only one noticed the abusive terms in the form. This raises serious questions about the extent to which the holders have the time to read the terms and, if they do, whether they really understand what is described.

4.2 THE INFLUENCE OF THE PAYMENT ON THE DECISION OF THE HOLDER

In the case of TFH, financial compensation to the holder occurs through the provision of the requested personal data, enabling him to request WLD tokens. For the conversion of these tokens into local currency, a minimum interval of 24 hours is required. In Brazil, this compensation varies between R\$ 300.00 and R\$ 470.00, depending on the price of the 25 WLD tokens made available to holders at the time of registration. (ANPD, 2025)

This practice generates a significant risk: the reduction of consent to the role of a simple mechanism for legitimizing practices that, in other circumstances, could be considered abusive. The data subject now has his fundamental rights of freedom and privacy placed in the background, in the face of the urgency of satisfying basic economic needs. However, from the financial consideration, the fact is extracted that, many times, consent to the use of data is not free and genuine, because there is an unequal relationship of power. The data subject ends up being forced to accept, as there are no viable alternatives, which violates the principle of freedom of choice in consent. In the same sense, Doneda (2019) explains:

The disparity of means and power between the person who is required to consent to the use of personal data in contemplation of the execution of a contract and the person who asks for them means that the real option left to him is, so often, that of "all or nothing", "take it or leave it".

From this, it is possible to infer that when there is asymmetry of information and power between those who collect the data (companies or platforms) and those who provide it (holders), this requirement is severely compromised.

According to interviews conducted by G1 (2025), data subjects reported that the information provided by TfH was limited and difficult to understand for most users. Due to this limitation, many did not have effective knowledge about the specific purpose of the processing of their biometric data, which, due to their sensitive and irreversible nature, required explicit and informed consent. In addition, there was a lack of clear information

regarding the potential risks of leakage or misuse of this data, which could lead to serious violations of the privacy and security of the holders.

Likewise, no clarifications were made available about the storage period of the information collected, nor about the policies for disposing or eliminating the data, nor about any sharing with third parties or uses for commercial and technological purposes that would go beyond the initial proposal presented to the participants. Such information would be crucial for the manifestation of free consent.

The absence of clear and accessible information places the holder of personal data in a position of evident disadvantage in relation to the company responsible for collecting and processing the information. While the organization has specialized technical knowledge, financial resources, and control over the data lifecycle, individuals remain oblivious to the processes involved, basing their decisions on superficial information and persuasive marketing strategies. In most cases, the prevailing perception is that the financial compensation received mitigates any losses, even though there are no guarantees as to the security and proper use of your data. This imbalance is intensified by the technological complexity inherent in the processing of biometric data, whose understanding is limited for most data subjects, especially those without specific technical training.

In this regard, the use of consent as a bargaining chip impacts the dynamics of consumer relations and the governance of personal data. By offering direct benefits in exchange for consent, a market logic is created that encourages exploitative practices, in which sensitive data is treated as tradable goods, to the detriment of the fundamental rights to protect the intimacy and dignity of the human person. The LGPD, in article 8, paragraph 3, expressly prohibits the processing of personal data through a defect of consent, precisely to prevent such practices from being consolidated in the Brazilian legal system. Such reasoning was also demonstrated by the ANPD in the administrative proceeding:

The asymmetry that may result in the invalidation of consent, however, should not be analyzed only in the context of the existence of a subordinate relationship between the processing agent and the data subject, so that the latter feels coerced to submit to the processing of personal data because he is unable to autonomously express his will without suffering unfair negative consequences due to his decision. Any analysis of the free manifestation of consent that only evaluates the existence of subordination or the conditioning of access to a certain service, in fact, would limit the exercise of the holder's self-determination, as it would fail to evaluate substantial elements related to the context in which the processing is carried out, such as, for example, elements related to the informational asymmetry with regard to the processing performed and socioeconomic issues that may influence the decision of the holder in a disproportionate manner. The analysis of possible asymmetry of power to assess whether a certain manifestation of the holder is in fact "free", under

the terms of the LGPD, therefore, cannot be done in a restrictive way, since it could result in the reduction of the scope of the fundamental guarantee provided for in the Federal Constitution. (ANPD, 2025)

By establishing a parallel with the analysis of free and informed consent in the context of clinical research, as discussed by Castro, Mapelli, and Gozzo (2023), significant challenges related to the clarity of the information provided and the effective autonomy of the participants are evident, especially when the complexities of their socioeconomic and educational conditions are not considered. The study reveals that the low readability of the Informed Consent Forms (ICF), combined with inequality in access to information, compromises the full understanding of the risks and benefits involved in participating in research.

An analogous situation is observed in the context of the collection of biometric data in programs such as the one promoted by TfH, in which there is a marked informational asymmetry. In these cases, data subjects in situations of social vulnerability are led to make decisions without access to adequate and understandable information. Thus, both in clinical research and in the provision of sensitive data through economic incentives, consent is weakened, lacking guarantees regarding the effective freedom and autonomy in the manifestation of the will of the holders.

In addition, the aforementioned study by Castro, Mapelli and Gozzo highlights the influence of social, economic and cultural factors in the decision-making process, showing that participants with low education and limited income are more susceptible to consent without adequate understanding of the ethical and legal implications of the act. This phenomenon is directly applicable to the analysis of consent required by TfH, in which the offer of financial rewards in exchange for biometric data intensifies structural inequality and converts consent into a mere formality, vitiated by economic necessity.

ALTERNATIVES TO ENSURE FREEDOM OF CONSENT

Despite the particularities of the TfH case, not every financial consideration automatically invalidates consent. However, some aspects must be taken into consideration. There should be full transparency about the value and what will be done with the data. Although the analysis of consent is at the heart of the matter, this was not the only problem pointed out by the ANPD, which understood that there was a lack of transparency regarding data processing.

It was identified that the informative materials about the service and data processing were, by default, written in English, which compromises the right to clear, adequate and accessible information, as provided for in Brazilian legislation. In view of this, the authority determined the dissemination of such information also in Portuguese, as well as the launch of a new application aimed exclusively at Brazilian holders, which must contain complete information and presented in a clear and intuitive way, in parallel with the Terms of Use and the existing Privacy Notices.

In addition, new instructions were imposed on attendants at physical collection points, with the aim of restricting any form of guidance, assistance or discussion about the incentive in Worldcoin. This measure aims to avoid inducing or inducing undue influence on the decision-making process of the holder regarding the authorization for the processing of their biometric data, especially with regard to iris collection. The authority made it clear that informational neutrality at the time of collection is essential for the validity of consent.

Another approach to ensure the voluntariness of consent is to calibrate the value of the financial consideration to the socioeconomic profile of the holder, so that the value does not become so high as to eliminate the real possibility of refusal. In addition, offer alternative participation modalities, other than monetary incentives, that allow the holder to freely choose between different forms of engagement. This dual strategy not only mitigates the risk of economic coercion, but also reinforces the principles of autonomy and self-determination, which are essential for the legal validity of consent in personal data collection environments. It is necessary to offer reasonable alternatives, as shown in the examples below.

CONTEXT	CALIBRATED CONSIDERATION	ALTERNATIVE WITHOUT PAYMENT	MITIGATED RISK
OPINION RESEARCH IN LOW-INCOME COMMUNITIES	Proportional value to cover comfortable commuting	Certificate of participation for curriculum or complementary hours in social projects	Excessive economic coercion
HEALTH APP TESTING ON BASIC PLAN USERS	R\$ 10 credit in pharmacy voucher	Online course on cardiovascular care with certificate	Undue influence by monetary value and feeling of "not being able to refuse"
SURVEY OF CONSUMER HABITS IN RETAIL STORES	5% Discount Coupon On Next Purchase	Loyalty program with accrual points (no immediate value)	Biases in the future purchase decision

Thus, the effectiveness of free and informed consent requires the adoption of measures that ensure the autonomy of the personal data subject, especially in scenarios marked by socioeconomic vulnerability. As demonstrated above, the alternatives consist of the possibility of offering forms of participation that are not conditioned by direct financial incentives. By decoupling the granting of consent from economic counterparts, the risks of economic coercion and vitiated consent are minimized, allowing the decision of the holder to be based on the understanding of the risks and benefits involved in the processing of their data, and not on the immediate need to obtain material advantages.

FINAL CONSIDERATIONS

The analysis of the case of Tools for Humanity (TfH), responsible for the Worldcoin project, reveals substantial weaknesses in the way the consent of the holders of sensitive personal data has been obtained. Although consent represents one of the legal grounds provided for by the General Law for the Protection of Personal Data (Law No. 13,709/2018), its validity depends on the effective freedom, information, and understanding on the part of the data subject, which has been compromised in the face of several factors observed in the specific case.

The context of socioeconomic vulnerability of a significant part of the Brazilian population, associated with the offer of financial incentives for the provision of biometric data, compromises the authenticity of consent. The absence of clear, accessible information in Portuguese, added to the asymmetry of power and the technical complexity involved in data processing, aggravates this scenario, giving consent a merely formal character, devoid of substance.

The ANPD, when analyzing the conduct of TfH, recognized the insufficiency of the informational practices adopted and imposed corrective measures, such as the requirement of clear communication in Portuguese, the neutrality of the attendants at the time of collection and the reformulation of the information channels. Such measures aim to restore the holder's informational self-determination, ensuring that consent is given based on a free, informed and conscious decision.

In addition, the need for structural alternatives that guarantee freedom of consent in contexts of vulnerability is highlighted. Strategies such as the calibration of the value of the financial consideration, the offer of non-monetary modalities of participation, and informational neutrality are mechanisms capable of mitigating the risk of economic coercion

and strengthening the rights of data subjects. These solutions reinforce the constitutional principles of human dignity, freedom, and equality, in addition to achieving the protective objectives of the LGPD.

It is therefore concluded that the validity of consent in the processing of sensitive personal data requires not only formal compliance with legal requirements, but also a contextualized approach, which takes into account socioeconomic, informational, and structural factors that influence the data subject's decision.

Only through the implementation of strategies and practices that consider these variables will it be possible to ensure the effective protection of the fundamental rights to privacy and informational self-determination in the contemporary digital environment.

REFERENCES

1. BONFIM, Isabella. Without reading the terms of use, more than 20,000 people sign up for community service. *Estadão*, São Paulo, 6 Apr. 2024. Available at: <https://www.estadao.com.br/emails/comportamento/sem-ler-os-termos-de-uso-mais-de-20-mil-pessoas-se-inscrevem-em-servicos-comunitarios/>. Accessed on: 12 Apr. 2025.
2. BONNA, Alexandre Pereira; CAÑIZO, Amanda de Moura; CALZAVARA, Giovana Ferreira. Consent and LGPD: challenges in the face of consumer hypervulnerability. *Journal of Administrative Law and Public Management*, Brasília, v. 10, n. 3, p. 250–270, Sept./Dec. 2024. Available at: <https://www.portaldeperiodicos.idp.edu.br/rda/article/view/6231/2527>. Accessed on: 12 Apr. 2025.
3. BRAZIL. National Data Protection Authority. Technical Note No. 4/2025/FIS/CGF/ANPD. Brasília, 23 Jan. 2025. Available at: https://anpd-super.mj.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?yPDszXhdoNcWQHJaQIHJmJlqCNXRK_Sh2SMdn1U-tzNecesYdd_tZp-0w7M55fZJpoHOzEMG_PdSXLtjMpJTrCwyUvB0ZP8nCbud-aECp3wS48Cc6UYN8co-Z_cSDs6h#item_Y9pFFEzbgAsQKROG. Accessed on: 22 mar. 2025.
4. CASTRO, Talita Garcia do Nascimento de; MAPELLI, Lina Domênica; GOZZO, Thais de Oliveira. Informed consent in clinical research participants. *Journal Health NPEPS*, v. 8, n. 1, e10760, Jan./Jun. 2023. Available at: <https://repositorio.usp.br/directbitstream/8bd39c21-d28a-405a-9e5d-cb27608c783b/003173771.pdf>. Accessed on: 22 mar. 2025.
5. NATIONAL DATA PROTECTION COMMISSION (CNPd). CNPD suspends collection of biometric data. Available at: <https://www.cnpd.pt/comunicacao-publica/noticias/cnpd-suspende-recolha-de-dados-biometricos/>. Accessed on: 20 Feb. 2025.
6. NATIONAL DATA PROTECTION COMMISSION (CNPd). RESOLUTION/2024/137. Lisbon, 25 mar. 2024. Available at: https://www.cnpd.pt/media/imub4o4i/pt-sa-decision-worldcoin_temporary-limitation-of-processing_20240325.pdf. Accessed on: 1 mar. 2025.
7. G1. Payment for iris photo attracted half a million Brazilians with a focus on the outskirts of São Paulo until it was barred by the government. *G1*, 25 Jan. 2025. Available at: <https://g1.globo.com/tecnologia/noticia/2025/01/25/pagamento-por-foto-da-iris-atraiu-meio-milhao-de-brasileiros-com-foco-na-periferia-de-sp-ate-ser-barrado-pelo-governo.ghtml>. Accessed on: 22 mar. 2025.
8. HULBERT, Herik. LGPD in condominiums: collection of biometric data. *Sokolowski Advogados*, 24 Jan. 2023. Available at: <https://sokolowski.adv.br/2023/01/24/lgpd-em-condominios-coleta-de-dados-biometricos/>. Accessed on: 12 Apr. 2025.

9. IBGE. In 2023, poverty in the country falls to the lowest level since 2012. *IBGE News Agency*, 22 mar. 2024. Available at: <https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/42043-em-2023-pobreza-no-pais-cai-ao-menor-nivel-desde-2012>. Accessed on: 05 mar. 2025.
10. MECABÔ, Alex. Personal data protection: the function and limits of consent, by Bruno Bioni. *Journal of Contemporary Civil Law*, v. 28, year 8, p. 421-424. São Paulo: Ed. RT, jul./set. 2021.
11. MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Data protection beyond consent: contemporary trends of materialization. *Journal of Institutional Studies*, Rio de Janeiro, 2020. Available at: <https://www.estudosinstitucionais.com/REI/article/view/521/510>. Accessed on: 1 mar. 2025.
12. TEFFÉ, Chiara Antonia Spadaccini; TEPEDINO, Gustavo. Consent to the circulation of personal data. *Brazilian Journal of Civil Law*, v. 25, n. 3, p. 83-116, 2020. Available at: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/521/389>. Accessed on: 1 mar. 2025.
13. WORLD COIN. The Orb FAQs. Worldcoin, 2024. Available at: <https://world.org/pt-br/blog/worldcoin/orb-faqs>. Accessed on: 21 Feb. 2025.