THE (IN)EFFICACY OF CONSENT FOR THE PROCESSING OF PERSONAL DATA

Juliana Abrusio[1]

Abstract
The article discusses the ineffectiveness of consent in the context of personal data protection. Although traditionally seen as an essential mechanism, consent faces challenges in the digital age, where privacy policies are complex and often not understood by users. Consent fatigue is common, with many individuals accepting privacy terms without prior reflection and discernment about the future. The situation is aggravated by the prevalence of algorithms and automated decisions that make both data collection and its use less transparent. The article emphasizes the need to reformulate the current consent model, proposing the use of technologies that increase transparency and an interface design that facilitates user understanding. In Brazil, the LGPD seeks to align itself with the European model, but faces similar challenges at a practical level. The article suggests that reforms are needed if consent is to truly protect the rights of individuals in a digital and economically data-driven world.

Keywords
Consent Fatigue. Data Protection. Privacy Policies. Automated Decisions. Transparency.

Summary

[1] Professor. Mackenzie University.

1.Introduction

Consent, historically considered a fundamental pillar in the protection of personal data, encounters significant challenges in today's digital environment, which tend to worsen if end-user protection measures are not adopted.

Technological advances increase the complexity levels related to data sharing, while the predominance of automated algorithms in the modern information society undermines the efficacy of effective and valid consent.

Although consent is legally defined as the free, informed and unequivocal expression of will regarding the processing of personal data, evidence shows an opposite reality in which individuals face difficulties in fully understanding and reflecting on the terms contained in the policies that are the subject of express consent, which is even criticized in the literature on the matter.

Privacy policies often feature technical and complex language that is inaccessible to the average user, resulting in a "forced" consent that is obtained from the individual without their full knowledge, and that is aggravated by the profusion of consent requests.

The terms contained in privacy policies are lengthy and come with a multitude of conditions, contributing to "consent fatigue", causing individuals to become discouraged and to choose to accept the terms of privacy policies without further thought, solely in order to consume the services or products offered.

This article will explain the limitations of the current consent model, proposing innovative approaches to improve the protection of personal data, including the use of technological methods that can increase levels of transparency, as well as achieving an interface design with the allocation of information in a common language that is accessible and easy to understand by the end user.

In the Brazilian context, the General Data Protection Law (LGPD) attempts to align itself with European standards, but still faces similar

difficulties in practical applications, as well as in guaranteeing the effectiveness and validity of obtaining consent.

Therefore, while consent remains a crucial basis for data protection, it is imperative to reassess current practices in order to fulfil the role of protecting users' individual rights in an increasingly digital and data-driven world.

2.Consent embedded in the Algorithm Culture

One of the European legislator's solutions for the processing of personal data in *profiling* practices and automated decisions by algorithms is to only allow them if there is explicit consent from the data subject[2]. This, therefore, constitutes an exception to the ban on automated decisions and *profiling*, alongside two other exceptions: when the practices are necessary to conclude or execute a contract between the data subject and a controller, or because of legitimate interest.

Here, we are interested in focusing specifically on consent. The reason for this is that *profiling* and the use of algorithms may not be transparent to the individual. Sometimes it is even based on data obtained or inferred from other data, and not on data directly provided by the data subject, as highlighted in *Recommendation CM/Rec (2010)13 and explanatory memorandum*:

[2] Article 22, GDPR: The data subject shall have the right not to be bound by any decision taken solely on the basis of automated processing, including profiling, which produces legal effects concerning themselves or similarly significantly affects them. 2. Paragraph 1 shall not apply if the decision: (a) is necessary for entering into, or the performance of, a contract between the data subject and a controller; (b) is authorized by Union or Member State law to which the controller is subject, and which also provides for appropriate measures to safeguard the rights and freedoms and legitimate interests of the data subject; or (c) is based on the explicit consent of the data subject (emphasis added.).

> Considering that profiles, when they are attributed to a data subject, make it possible to generate new personal data which are not those which the data subject has communicated to the controller or which she or he can reasonably presume to be known to the controller.[3]

The question that now arises is how much the data subject is really able to *consent to* the gathering of the algorithm, to the extent of their real understanding concerning the nature and implications of the use of artificial intelligence in an automated decision that legally affects their interests.

According to Paulo Lilla "there is therefore a real *fatigue of* consent, which ends up becoming the very refusal of the idea of control and self-management of personal information"[4].

In France, the National Commission for Information Technology and Freedoms (CNIL) fined Google 50 million euros on January 21, 2019, for failing to clearly and comprehensibly inform its users about its policy on the use of personal data, on the grounds of a lack of transparency, unsatisfactory information and the absence of valid consent on the use of its users' data.

While the CNIL recognized that the company provides information to its users, it understood that the information offered is not easily accessible and is scattered in different documents, pointing out that

---

[3] COUNCIL OF EUROPE. Recommendation CM/Rec (2010)13 and explanatory memorandum. The protection of individuals with regard to automatic processing of personal data in the context of profiling, on Nov 23, 2010. Available at: https://rm.coe.int/16807096c3. Accessed on: Nov. 09, 2018, p.6.

[4] LILLA, Paulo. Proteção de Dados Pessoais e os Requisitos de Validade do Consentimento. Uma análise comparada das disposições da LGPD e do GDPR [Personal Data Protection and the Requirements for the Validity of Consent. A comparative analysis of the provisions of the LGPD and the GDPR]. 2023, Monograph in lato sensu specialization, p. 23.

sometimes it takes five clicks to access the necessary information, and that this demand is not accompanied by a legitimate justification for the access to personal data[5].

Data controllers who rely on consent as the basis for *profiling* practices and automated decisions will have to demonstrate that data subjects understand exactly what they are consenting to, which means that data subjects must be given sufficient and relevant information about the use and intended consequences of the use of the data processing, in order to ensure that any consent given by the data subject represents an informed choice. However, this imposition is a major challenge for everyone (companies and data subjects).

3.The dogmatic formula of consent

In Brazil, the General Data Protection Law (Law No. 13,709/2018), aligned with the European model, includes consent as one of the legal bases for data processing (art. 7, I), and defines it as the "free, informed and unequivocal expression by which the data subject agrees to the processing of their personal data for a specific purpose" (art. 5, XII).

It is worth remembering that consent, in Brazilian legislation, was already provided for even before the General Data Protection Law (LGPD), as an authorizing foundation for the processing of personal data, by virtue of the Brazilian Civil Rights Framework for the Internet (Law No. 12.965/2014), which provides for consent as a legal basis in its art. 7, IX.

Consent, as a manifestation of the individual's will, anchored in private autonomy and freedom to contract, reflects the principle of informational self-determination of data subjects, given that the individual

[5] NETTESHEIM, Martin. Data Protection in Contractual Relationships (Art. 6(1)(b) GDPR), p. 2.

is the absolute holder of control over their own personal information. This can be considered the main legal basis for legitimizing data processing[6].

However, this dogmatic legal formula of consent carries with it significant obstacles to truly fulfilling the rights of data subjects in today's information society, guided by the algorithm data collection. In the face of so many obscurities, it has become a challenge to find a way of providing data subjects with knowledge and control over the circulation of their personal data. There is a considerable risk that the individual will be expropriated of the right to construct and control their own social image. It follows that consent is losing the importance and trust it was once afforded.

Consent comes from *co-sentire*. There is an involvement to know and agree to the bases to which consent is given, as stipulated in article 4(11) of the GDPR[7]. However, in today's fast-paced life, with its immediacy and scarce time, there doesn't seem to be any space or availability of time and mind to reflect on and consent to the countless instruments that need to be consented to. It is important to remember that time is a finite resource on the virtually limitless stage of computational and algorithmic ubiquity. Accordingly, in most cases, users want to get through all the screens that ask for their "agreement" in order to reach their destination as quickly as possible, regardless of *what* they are consenting to.

People are fast, in a hurry, and lack patience. In this context, there are those who preach the death of privacy policies (of *websites* and apps), because they understand that they are useless, since hardly anyone reads them. Moreover, individuals have limited rationality when it comes to the decisions they make on a routine basis, so the *trade-off* between access to

---

[6] LILLA, Paulo. Proteção de Dados Pessoais e os Requisitos de Validade do Consentimento. Uma análise comparada das disposições da LGPD e do GDPR [Personal Data Protection and the Requirements for the Validity of Consent. A comparative analysis of the provisions of the LGPD and the GDPR]. 2023, Monograph in lato sensu specialization, p. 4.

[7] TREHAN, Kriti. Is Consent Really Dead?, p. 6.

their personal data and the use of the service they are being offered does not involve an in-depth cost-benefit analysis, as it is difficult to measure future impacts in view of the uncertainty of the event[8].

The report of the survey carried out by the *Annenberg School for Communication at the University of Pennsylvania* concluded that the majority of Americans are resigned to giving up their personal data because they see the task of consent as a burden[9]. Renunciation occurs when a person believes that an undesirable outcome is inevitable and feels powerless to prevent it, emphasizing the cognitive problems of individuals in the self-management of privacy, rebutting the premise of rationality and full information regarding the performed acts[10].

Consequently, according to the report, instead of feeling able to choose, Americans believe that it is pointless to manage what companies can acquire about them, given that companies offer incentives that capture individuals' attention in exchange for obtaining consent to access their data[11]. According to the study, more than half of the 1,506 Americans interviewed (all over the age of 18) do not want to lose control over their information, but at the same time believe that this loss of control has already happened[12].

---

[8] SOLOVE, Daniel J. Murky Consent: An Approach to the Fictions of Consent in Privacy Law, p. 620.

[9] SCHERMER, Bart W.; CUSTERS, Bart; HOF, Simone van der. The Crisis of Consent: How Stronger
Legal Protection may lead to Weaker Consent in Data Protection, p. 4.

[10] SOLOVE, Daniel J. Privacy Self-Management and the Consent Dilemma, p. 1883.

[11] SOLOVE, Daniel J. Murky Consent: An Approach to the Fictions of Consent in Privacy Law, p. 612.

[12] TUROW, Joseph; HENNESSY, Michael; DRAPER, Nora. The trade off fallacy. How marketers are misrepresenting american consumers and opening them up to exploitation. Annenberg School for Communication University of Pennsylvania, June 2015. Available at: https://www.asc.upenn.edu. Accessed on: Aug. 02, 2024.

In fact, it is on the consent of the data subject that lies the foundation for exercising this freedom to control the individual's data, so as to make it possible, in theory, to determine the level of protection of the data concerning them[13].

The protection of personal data has an *ex ante* regulatory rationale, while the contractual protection of the consumer has, par excellence, an *ex post* control, through the declaration of nullity of abusive contractual clauses, except in cases of action in the sphere of diffuse and collective interests, in which other consumers can benefit from the modifications made to the contractual bases[14].

This model of informed consent was effective two decades ago[15], but today it could very well prove to be a fantasy. In a constant stream of *online* interactions, especially on the small screens of cell phones, which now account for most of the usage, it is neither realistic nor feasible to trust that

[13] LILLA, Paulo. Proteção de Dados Pessoais e os Requisitos de Validade do Consentimento. Uma análise comparada das disposições da LGPD e do GDPR [Personal Data Protection and the Requirements for the Validity of Consent. A comparative analysis of the provisions of the LGPD and the GDPR]. 2023, Monograph in lato sensu specialization, p. 3.

[14] BIONI, Bruno Ricardo. Proteção de dados pessoais. A função e os limites do consentimento [Protection of personal data. The role and limits of consent]. Rio de Janeiro: Forense, 2019, p.173.

[15] LILLA, Paulo. Proteção de Dados Pessoais e os Requisitos de Validade do Consentimento. Uma análise comparada das disposições da LGPD e do GDPR [Personal Data Protection and the Requirements for the Validity of Consent. A comparative analysis of the provisions of the LGPD and the GDPR]. 2023, Monograph in lato sensu specialization, p. 4: "Given its importance, consent as a legal basis for the processing of personal data has already been included in the US Fair Information Practice Principles (FIPPs) since the early 1970s , which established a normative guideline for the protection of personal data in order to give citizens greater control over their data."

people are reading the privacy policies[16]. Alessandro Acquisti *et al* summarize the idea that we are trying to convey here: "in the current state of the digital economy, consent is ubiquitous, and its consequences are rarely understood"[17]. Blume also considers that

> even when consent is founded upon information and furthermore is specific, most data subjects are not able to understand the kinds of processing that take place in the modern complex information society[18].

For Katherine Strandburg, consent has emerged as a panacea because it presents ways of "having it all". For the author, consent in the universe of *big data* may seem attractive as a way of solving the use of data, but in practical terms it proves to be elusive[19].

Along the same lines, Solon Barocas and Helen Nissenbaum have stated their opinion on the ineffectiveness of consent:

> In the case of consent, too, commonly perceived operational challenges have distracted from the ultimate inefficacy of consent as a matter of individual choice and the absurdity of believing

[16] SABLICH, Elizabeth. Why protecting privacy is a losing game today – and how to change the game. In: Brooking. Available at: https://www.brookings.edu. Accessed on: Aug. 02, 2024.

[17] ACQUISTI, Alessandro; TAYLOR, Curtis; WAGMAN, Liad. The Economics of Privacy. Journal of Economic Literature, vol 54, June 2016, p.442 e 477-478.

[18] BLUME, P. The inherent contradictions in data protection law. International Data Privacy Law 26, 2012, p.29.

[19] STRANDBURG, Katherine J. Monitoring, datafication, and consent: legal approaches to privacy in the big data context. *In*: LANE, Julia; STODDEN, Victoria; BENDER, Stefan; NISSENBAUM, Helen (Coords.). Privacy, big data, and public good: frameworks for engagement. Cambridge: Cambridge University Press, 2014, p.2.

> that notice and consent can fully specify the terms of interaction between data collector and data subject[20].

An experimental study conducted in 2016 by two professors, Jonathan Obar of York University in Toronto and Anne Oeldorf-Hirsch of the University of Connecticut, confirms the obvious: almost nobody reads the terms of use or *online* contracts to which they give consent. The professors created a new social network, called NameDrop, and advertised it to several students. Hundreds of university students clicked on the "by clicking *join* you agree to abide by our terms of service" button to become members of the new social network, but according to paragraph 2.3.1 of the terms of service, they agreed to give NameDrop their future first-born children[21].

The result showed that only a quarter of the 543 students bothered to look at the fine print, and spent a longer time on the text. The average "longer time" was one minute, which did not prevent all 543 from agreeing to the terms of use.

The fact that the counterpayment is not monetary makes it easier for internet users to disregard a more detailed analysis of the *online* contract . Furthermore, many internet users don't bother to read the terms they agree to, since they know that Google, Facebook, Amazon and others are not in a position to negotiate their own separate agreement, and so won't spend time on a contract that can't be modified.

---

[20] BAROCAS, Solon; NISSENBAUM, Helen. Big data's end run around anonymity and consent. *In*: LANE, Julia; STODDEN, Victoria; BENDER, Stefan; NISSENBAUM, Helen (Coords.). Privacy, big data, and public good: frameworks for engagement. Cambridge: Cambridge University Press, 2014, p.2.

[21] BERREBY, David. Click to agree with what? No one reads terms of service, studies confirm. In: The Guardian, Mar 3, 2017. Available at: https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print. Accessed on Aug. 18, 2024.

In another investigation, carried out as part of the CLAUDETTE project[22], which resulted in the publication of a report[23] containing the preliminary results of the study, the problem of consent algorithm culture was brought into focus. The scope of the research was to assess, from a legal point of view, based on the GDPR[24], and using artificial intelligence and *machine learning*, whether the available privacy policies comply with the GDPR. Thus, the researchers described the requirements that a privacy policy must meet under the GDPR (comprehensive information, clear language, fair processing), as well as the ways in which these documents could be considered unlawful (if the mandatory information is insufficient, the language is unclear, or the processing is potentially unfair). The content of the privacy policies of Google, Meta, Amazon, Apple, Microsoft, X (formerly Twitter), Uber, AirBnB, Booking.com, Skyscanner, Netflix, Steam and Epic Games were analyzed. The results of the first experiments conducted show that it is possible to use machine learning techniques for the desired purpose. It is therefore worth devoting time and effort to initiatives of this kind, with the aim of forming an instrument in defense of the data subject and the consumer. The study indicated that none of the information analyzed regarding the privacy policies contained in the

[22] Automated CLAUse DETeCTER. Available at: http://claudette.eui.eu. Accessed on: July 24, 2024.

[23] CONTISSA, Giuseppe Contissa; DOCTER, Koen; LAGIOIA, Francesca; LIPPI, Marco; Micklitz, Hans-W; PALKA, Przemyslaw; SARTOR, Giovanni; TORRONI, Paolo. CLAUDETTE meets GDPR. Automating the evaluation of privacy policies using artificial intelligence. Study Report, Jul 02, 2018. Available at: https://goo.gl/irpAaz. Accessed on: Aug. 18, 2024.

[24] NETTESHEIM, Martin. Data Protection in Contractual Relationships (Art. 6(1)(b) GDPR), p. 13: "The GDPR has two intertwined regulatory objectives.26 Art. 1 (1) GDPR, which in this respect implements Art. 16 (2) TFEU, indicates that the subject matter and objective of the Regulation is not only 'the protection of natural persons with regard to the processing of personal data'. The equally important second objective of the Regulation is to establish rules 'on the free flow of such data'."

material met the requirements of the GDPR. There were 3658 sentences (80,398 words), of which 401 (11.0%) were classified as unclear language and 1240 (33.9%) were classified as potentially unlawful clauses, i.e. "problematic processing" or "insufficient information" clauses, according to the rules of articles 13 and 14 of the GDPR.

According to David Hoffman, a professor at the University of Pennsylvania who researches the law and psychology of contracts, this condition and this situation are, however, not new, given the cognitive problems that prevent the full exercise of consent. They have existed since printed contracts of adhesion. Furthermore, according to him, there is a real concern that data protection rules are being swallowed up by *online* agreement clauses[25]. It has been estimated that reading digital contracts would take an American almost 250 hours of their time per year[26].

Regarding the wording of the law, in the LGPD the legislator chose to require unambiguous consent (more pragmatic), while the Brazilian Civil Rights Framework for the Internet requires express consent (more formal). The LGPD therefore favors certainty over formality. In any case, some formality is imposed on consent, without tacitly adopting it. It is well known that the general rule is that the form is not a requirement for a contract to be valid. Therefore, since the end of the Roman Empire[27], the law has

---

[25] HOFFMAN, David A.; WILKINSON-RYAN, Tess.The psychology of contract precautions. University of Chicago Law Review, v.80, p.395, 2013.

[26] HOFFMAN, David A.; WILKINSON-RYAN, Tess.The psychology of contract precautions. University of Chicago Law Review, v.80, p.395, 2013.

[27] By the rule instituted by the constitution of Emperor Leon of 472 AD, the requirement for the validity of the use of solemn words in the execution of the *stipulatio* was expressly abolished. The words of this constitution left room for much interpretation. At first, one tends to consider that this emperor dismissed the old Roman oral formality, consisting of that ritual involving a question and an answer, a procedure which at that time should have been considered quite antiquated. (ZIMMERMANN, Reinhard. The law of obligations. Oxford, New York, 1996, p.80). The compilers commented on this rule in the Institutions (I.3.15.1.1.) to the effect that Leon's constitution suppressed the

incorporated the principle of *solus consensus obligat*. As a result, although there is practically nothing left of the formalism laid down in ancient law[28], today's formalism should be seen as an attempt to guarantee people's fundamental rights.

By allowing dubious or non-existent consent to be understood as valid, a precedent is created which legitimizes the improper collection of data with its subsequent disclosure[29].

In the context of data protection, it is clear that the law, in its sovereign will, considers it to be essential for the data subject to have a synchronized understanding regarding the communication (contract) of collection and processing of their information. This is, in fact, ancient legal

---

solemnity of words. However, against this view, it is argued that Leon did not abolish *sollemnitas verborum*, as the text says, but admitted that the *stipulatio* could be perfected *quibuscumque verbis*, considered by *consensus* (BIONDI, Biondo. Contratto e stipulatio. Milano, 1953, p.289).

[28] In Roman law, especially in the older period, the form of legal transactions, unlike today, was the very substance of the legal act. If the prescribed form, solemnity and gestures were not complied with, the contract would not be perfected, even if the will of the parties was clear in the desired effects. In fact, at the origins of Roman law, there was a rigid business formality, which was preserved with a certain degree of moderation throughout the classical age and only seems to have been overcome in the post-classical age. The distinction between formal and non-formal contracts was proposed by more recent Romanists; the *ius civile* knew nothing but formal contracts, the solemnity of which not only covered the wills of the parties, but was in itself fully effective. Form was the most important element, and if it were defective, no legal result would be produced. (OURLIAC, Paul; DE MALAFOSSE, Jehan. Derecho romano y francês histórico. Tradução ao espanhol e anotações de Manuel Fairén, t. I [Roman law and historical French. Spanish translation and annotations by Manuel Fairén, v. I], 1960, p. 80).

[29] SOLOVE, Daniel J. Murky Consent: An Approach to the Fictions of Consent in Privacy Law, p. 596-604.

intelligence, formulated by the Romans [30]. However, as it turns out, the consent tool alone seems to be ineffective in today's reality.

Recital 42 of the GDPR states that for consent to be informed "the data subject must know at least the identity of the controller and the purposes for which the processing is intended". According to Daniel J. Solove, the legislation has still not solved the consent dilemma because it is an arduous task to regulate the privacy of individuals[31].

From another perspective, one of the problems with the old-fashioned model of prior notification and individual choice is that this format transfers the burden of protecting privacy and data protection onto the data subjects, resulting in an unequal bargain. It is up to the data subject to read, understand and consent.

4.Granularity of Consent

[30] The requirement of congruence between question and answer can also be identified as a concern with substance, since the necessary congruence does not simply lie in the formal aspect of the words used, but in the concern to establish the meaning of the promisor's statement in relation to the meaning of the *stipulator*'s request. This is why Gaius (Gai. 3.102) considered that a *stipulatio* was invalid if the question had not been answered, as in the case of one stipulating the amount of ten and the other promising five (The problem would then become one of interpretation (CANNATA, Carlo Augusto. Corso di Istituzioni di Diritto Romano [Course in Institutions of Roman Law], II, 1, Torino, 2003, p.91-92). As a result, the *stipulatio*, as a formal contract, has both a simple and free form as well as a strict form. If the *stipulatio* is the means of realizing an *obligatio verbis*, and this means that the obligation is perfected by the effects of the words pronounced, it is therefore the fact of pronouncing the words that produces the obligations: this is born precisely when the promissor has made his affirmative response to the *stipulator*'s question.

[31] SOLOVE, Daniel J. Murky Consent: An Approach to the Fictions of Consent in Privacy Law, p. 599.

The all or nothing attitude is in line with the "take it or leave it" approach[32]. When it comes to consent, there is also mention of the *granularity* of user authorizations, i.e. allowing authorizations to be given in a fragmented manner. Intelligence in this way overcomes the problem of "all" or "nothing". The 2013 Opinion of the Article 29 Data Protection Working Party (now EDPB) points out accordingly that:

> In some cases users are able to give a granular consent, where consent is sought for each type of data the app intends to access. Such an approach achieves two important legal requirements, firstly of adequately informing the user about important elements of the service and secondly asking for specific consent for each[33].

The US Federal Trade Commission (FTC) has taken a position with respect to consent in *online* activities for advertising segments, in a report[34]

---

[32] Hours after the GDPR came into force, the Austrian lawyer filed a lawsuit to challenge Facebook's policies. Accordingly: Within hours of the General Data Protection Regulation (GDPR) going into effect today, a privacy group accused Facebook (FB), Alphabet (GOOGL)'s Google, WhatsApp, and Instagram of violating Europe's strict new data-protection law.Austrian lawyer Max Schrems, a frequent critic of Facebook's privacy policies, on Friday filed complaints that claim the companies forced members to consent to terms of service with a "take it or leave it" threat. (SWARTZ, Jon. It's day one of GDPR, and facebook, google are accused of breaking new rules, May 25, 2018. Available at: https://www.barrons.com/articles/its-day-one-of-gdpr-and-facebook-google-are-accused-of-breaking-new-rules-1527284532. Accessed on: July 24, 2024).

[33] ARTICLE 29 Data protection working party. Opinion 02/2013 on apps on smart devices. Adopted on Feb. 27, 2013. Available at: https://www.pdpjournals.com/docs/88097.pdf. Accessed on: Aug. 10, 2024.

[34] FTC. Developing the Administration's Approach to Consumer Privacy, Aug. 9, 2024. Available at: https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-

sent to the *National Telecommunications and Information Administration* (an agency of the US Department of Commerce that advises the President on telecommunications policies). While throughout the report it recognizes the importance of data privacy, there is an emphasis placed on data-driven innovation[35].

This overflow of recurring requests for individuals to provide their consent makes it impossible to consider the effective applicability of express

staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf. Accessed on: Aug. 20, 2024.

[35] FTC. Developing the Administration's Approach to Consumer Privacy, Nov. 09, 2018. Available at: https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf. Accessed on: Nov. 20, 2018: "The FTC supports a balanced approach to privacy that weighs the risks of data misuse with the benefits of data to innovation and competition. Striking this balance correctly is essential to protecting consumers and promoting competition and innovation [...]. The digital economy has benefitted consumers in many ways, saving individuals' time and money, creating new opportunities, and conferring broad social and environmental benefits. [...] Privacy standards that give short shrift to the benefits of data-driven practices may negatively affect innovation and competition. Moreover, regulation can unreasonably impede market entry or expansion by existing companies; the benefits of privacy regulation should be weighed against these potential costs to competition. [...] Transparency is another longstanding privacy tenet championed by the FTC. The challenge is *how* and *when* to be transparent—how and when to provide important information about data collection and use in a way that it is accessible and meaningful to consumers. [...] The FTC has long encouraged a balanced approach to control. Giving consumers the ability to exercise meaningful control over the collection and use of data about them is beneficial in some cases. However, certain controls can be costly to implement and may have unintended consequences. For example, if consumers were opted out of online advertisements by default (with the choice of opting in), the likely result would include the loss of advertising-funded online content."

consent, as it does not allow us to scale and monitor the array of terms that individuals are exposed to on a daily basis[36].

It is interesting to note that this complexity also stems from the language used by companies in their privacy policies, which are often written by lawyers who use technical expressions that are not common knowledge to the end user[37].

5.Interface Design

Considering the aforementioned scenario, there are growing concerns about "interface *design* problems", which should be the subject of legal provision by the legislator when establishing technical design, as well as certification mechanisms and codes of conduct that ensure the effectiveness of consent[38].

In other words, without proper design there will be no resolution of the central problem concerning the effectiveness of consent, and issues such as non-readability will persist, as will certain design adjustments to the interface with the data subject, rendering doubts as to whether the individual's decision in fact emanated from a voluntary act[39]. As such, best practices in this sector point out that in order to make privacy notices

[36] SOLOVE, Daniel J. Murky Consent: An Approach to the Fictions of Consent in Privacy Law, p. 595-597.
[37] SCHERMER, Bart W.; CUSTERS, Bart; HOF, Simone van der. The Crisis of Consent: How Stronger Legal Protection may lead to Weaker Consent in Data Protection, p. 5.
[38] GRAFENSTEIN, Max von; HEUMÜLLER, Julie; BELGACEM, Elias; JAKOBI, Timo; SMIESKOL, Patrick. Effective regulation through design: Aligning the ePrivacy Regulation with the EU General Data Protection Regulation (GDPR), p. 6.
[39] SOLOVE, Daniel J. Murky Consent: An Approach to the Fictions of Consent in Privacy Law, p. 610-612.

effective and usable, they should be integrated into the design of the system[40].

A minimum parameter that contributes to greater awareness of the individual's information and greater control of their data should be imposed, in which the information is in accessible language in an interface that simplifies the assimilation process[41]. In this sense, broadly speaking, the space given to *design* linked to notifications relating to personal data must meet the following dimensions: notification time (when it is provided); channel (how it is delivered); modality (which interaction models are used) and control (how options are provided). These dimensions can be considered in parallel, to the detriment of the sequential mode[42].

Several studies have already been carried out and others are still underway to investigate ways of improving the effectiveness of privacy terms and policies. However, it appears that there is still little guidance for *designers* and developers on *design* aspects that can impact or contribute to the effectiveness of privacy notices. In the words of Elizabeth Sablich, "some forms of notice are necessary and attention to user experience can help, but the problem will persist no matter how well designed disclosures are"[43].

---

[40] SCHAUB, Florian; BALEBAKO, Rebecca; DURITY, Adam L.; CRANOR, Lorrie Faith. A design space for effective privacy notices. Symposium on Usable Privacy and Security (SOUPS), July 22–24, 2015, Ottawa, Canada. Available at: https://www.usenix.org. Accessed on: Aug. 12, 2024.

[41] SCHERMER, Bart W.; CUSTERS, Bart; HOF, Simone van der. The Crisis of Consent: How Stronger Legal Protection may lead to Weaker Consent in Data Protection, p. 8.

[42] SCHAUB, Florian; BALEBAKO, Rebecca; DURITY, Adam L.; CRANOR, Lorrie Faith. A design space for effective privacy notices. Symposium on Usable Privacy and Security (SOUPS), 22 a 24 de de 2015, Ottawa, Canada. Available at: https://www.usenix.org. Accessed on: Aug. 12, 2024, p.6.

[43] SABLICH, Elizabeth. Why protecting privacy is a losing game today – and how to change the game. In: Brooking. Available at: https://www.brookings.edu/research/why-

For data protection clauses to be more effective, it is essential to work on the issue of interface *design*, and especially to empower users with privacy controls in order to increase transparency, as well as trust and power of control over their personal data.

New technologies and integrated devices, such as *wearables* and the internet of things, pose challenges for the use of different means of *design* for privacy notifications and controls. In today's world, information collection is continuous. Therefore, public policies, laws and technological approaches need to be applied together in order to allow users to better manage their personal data[44].

Faced with the powerlessness presented, it is necessary to add other means than the traditional ones. It is no longer possible to think and act with the means inherited from the old orders, so Daniel J. Solove proposes an innovative approach called "ambiguous consent", in which the fictitious nature of consent is recognized, moving away from the binary aspects (consented or not), making it possible to analyze the existence or not of different levels of consent[45].

The law on its own is limited to provide support for current needs, meaning that it is also necessary to resort to technology itself, so that there is accountability with the data processed, as well as ensuring efficient methods for the individual's consent[46]. The goal is to understand a

protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/. Accessed on: Aug. 02, 2024.

[44] SCHAUB, Florian; BALEBAKO, Rebecca; DURITY, Adam L.; CRANOR, Lorrie Faith. A design space for effective privacy notices. Symposium on Usable Privacy and Security (SOUPS), 22 a 24 de de 2015, Ottawa, Canada. Available at: https://www.usenix.org. Accessed on: July 12, 2024, p.12.

[45] SOLOVE, Daniel J. Murky Consent: An Approach to the Fictions of Consent in Privacy Law, p. 598.

[46] LILLA, Paulo. [Personal Data Protection and the Requirements for the Validity of Consent. A comparative analysis of the provisions of the LGPD and the GDPR]. 2023, Monograph in lato sensu specialization, p. 14.

legislation based on evidence and objective criteria grounded in the empirical method[47].

The reason for this is that with the aggregate collection of user data, it is up to legislation to provide normative instruments that are capable of generating a layer of protection for individuals who are vulnerable when deciding to consume products/services, in view of the fact that companies that collect data can carry out countless analyses and forecasts[48], that could have an impact on an entire community.

However, it should be mentioned that technology and the legislative system have completely different speeds of advancement, given that the law is endowed with a lengthy process that demands greater reflection on representatives of the population, also conferring a layer of interaction with the community and experts in the sector, while technology advances at exponential levels, making it difficult to make normative provisions that adequately reflect the current methods used to obtain consent, thus resulting in inefficient data protection[49].

6.Conclusion

This article discusses the inefficiency of consent in the context of personal data protection, highlighting the difficulties and limitations associated with the current model of obtaining consent from users. Consent, traditionally seen as an essential mechanism for data protection, is losing its effectiveness in the modern information society, marked by the complexity of data and the ubiquity of algorithms.

---

[47] GRAFENSTEIN, Max von; HEUMÜLLER, Julie; BELGACEM, Elias; JAKOBI, Timo; SMIESKOL, Patrick. Effective regulation through design: Aligning the ePrivacy Regulation with the EU General Data Protection Regulation (GDPR), p. 27-28.
[48] SOLOVE, Daniel J. Privacy Self-Management and the Consent Dilemma, p. 1890.
[49] SCHERMER, Bart W.; CUSTERS, Bart; HOF, Simone van der. The Crisis of Consent: How Stronger Legal Protection may lead to Weaker Consent in Data Protection, p. 6.

Consent is legally defined as the individual's free, informed and unequivocal expression of will for the processing of their personal data, but in reality this definition faces several challenges. Privacy policies are often complex and difficult for the average person to understand, which leads to consent being "forced" or obtained without real understanding.

In addition, the article presents the results of surveys that were applied to analyze individuals' levels of awareness in terms of reading, knowledge and awareness of potential future effects, reaching a conclusion that leads us to believe that, in fact, individuals do not adequately read the policies, which emphasizes the lack of validity of the consent expressed by the individual.

There is consent fatigue due to the successive requests to accept policies on various platforms, where individuals' decisions are based on their desire to consume a particular product or service offered, so the trade-off between the service offered and the acceptance of sharing personal data is not weighed up, something that is emphasized by the literature pointing out the limited rationality of individuals.

Added to this is the absence of a clear and legitimate justification by companies for the purpose of collecting individuals' personal data, as well as the use of profiles and automated decisions that make it unclear and non-transparent to users, imposing on individuals a great burden of self-management over the decision of whether or not to share personal data with third parties in a complex virtual environment, according to the understanding of traditional consent.

In response to these problems, this article highlights the need for improvements in consent and methods that guarantee data protection, as well as providing mechanisms that can contribute to the individual's decision as to when to authorize the sharing of data.

In this step, the article proposes the use of technology that increases levels of transparency, as well as the understanding and adoption of an interface design that simplifies the decision-making process for users. The balance between innovation and data protection must always be present, providing incentives for companies to be increasingly transparent,

so that they can repay the sharing of collected data with rewards for their end users.

On the Brazilian scenario, the General Data Protection Law (LGPD) seeks to align itself with the European model, highlighting consent as a legal basis, but it still faces similar challenges in terms of practical application and effectiveness. Thus, while consent remains an important basis for data protection, there is a clear need for changes to ensure that it can truly fulfill its role of protecting the rights of individuals in an increasingly digital and data-driven world.

REFERENCES

ACQUISTI, Alessandro; BRANDIMARTE, Laura; LOEWENSTEIN, George. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. **ACM Computing Surveys**, v. 50, n. 3, 2017. Available at: https://dl.acm.org/doi/10.1145/3054926. Accessed on: July 27, 2024.

ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 15/2011 on the definition of consent, 2011. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf. Accessed on: July 27, 2024.

BAROCAS, Solon; NISSENBAUM, Helen. On Notice: The Trouble with Privacy Policies and What to Do About It. **Journal of Privacy and Confidentiality**, v. 7, n. 1, 2014. Available at: https://journalprivacyconfidentiality.org/index.php/jpc/article/view/419. Accessed on: July 27, 2024.

BIONI, Bruno Ricardo. **Proteção de Dados e a Autodeterminação Informacional no Brasil Data** [Protection and Informational Self-Determination in Brazil]. Graduation monograph, 2024.

CLAUDETTE PROJECT. Automated Analysis of Terms of Service and Privacy Policies with CLAUDETTE, 2018. Available at: https://www.claudette.eu/publications/claudette_report.pdf. Accessed on: July 27, 2024.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL). Délibération n° SAN-2019-001 du 21 janvier 2019 mettant en demeure la société GOOGLE LLC, 2019. Available at: https://www.cnil.fr/en/deliberation-no-san-2019-001. Accessed on: July 27, 2024.

GRAFENSTEIN, Max von; HEUMÜLLER, Julie; BELGACEM, Elias; JAKOBI, Timo; SMIESKOL, Patrick. Effective regulation through design: Aligning the ePrivacy Regulation with the EU General Data Protection Regulation (GDPR). 2021. Available at: https://www.cnil.fr/en/deliberation-no-san-2019-001. Accessed on: July 27, 2024.

HOFFMAN, David. Consent and the Illusion of Privacy: Contract Law and the Failure of Notice. **University of Pennsylvania Law Review**, v. 167, n. 4, 2019. Available at: https://www.pennlawreview.com/print/2019. Accessed on: July 27, 2024.

KOOPS, Bert-Jaap. The Trouble with European Data Protection Law. **International Data Privacy Law**, v. 4, n. 4, 2014. Available at: https://academic.oup.com/idpl/article/4/4/250/757362. Accessed on: July 27, 2024.

LILLA, Paulo Eduardo. **Proteção de Dados Pessoais e os Requisitos de Validade do Consentimento: Uma Análise Comparada das Disposições da LGPD e do GDPR.** [Personal Data Protection and the Requirements for the Validity of Consent. A comparative analysis of the provisions of the LGPD and the GDPR]. 2023, Monograph in lato sensu specialization. Accessed on: July 27, 2024.

NETTESHEIM, Martin. Data Protection in Contractual Relationships (Art. 6(1)(b) GDPR). 2023. Available at: https://ssrn.com/abstract=4427134. Accessed on: July 27, 2024.

OBAR, Jonathan; OELDORF-HIRSCH, Anne. The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. **Information, Communication & Society**, v. 21, n. 4, 2018. Available at:

https://www.tandfonline.com/doi/abs/10.1080/1369118X.2018.1486870. Accessed on: July 27, 2024.

SABLICH, Elizabeth. Designing for Privacy. **Yale Journal of Law & Technology**, v. 19, 2022. Available at: https://yjolt.org/designing-privacy. Accessed on: July 27, 2024.

SCHERMER, Bart W.; CUSTERS, Bart; HOF, Simone van der. The Crisis of Consent: How Stronger Legal Protection may lead to Weaker Consent in Data Protection. Ethics and Information Technology, 2014. Available at: https://ssrn.com/abstract=2412418. Accessed on: July 27, 2024.

SOLOVE, Daniel J. Murky Consent: An Approach to the Fictions of Consent in Privacy Law. **Boston University Law Review**, v. 104, n. 593, 2024. Available at: https://ssrn.com/abstract=4333743. Accessed on: July 27, 2024;

SOLOVE, Daniel J. Privacy Self-Management and the Consent Dilemma. **Harvard Law Review**, v. 126, n. 7, p. 1880-1903, 2013. Available at: https://ssrn.com/abstract=2171018. Accessed on: July 27, 2024.

STERN, Joanna. How GDPR Has Transformed the World of Privacy Emails. **Wall Street Journal**, 2018. Available at: https://www.wsj.com/articles/how-gdpr-has-transformed-the-world-of-privacy-emails-1528722601. Accessed on: July 27, 2024.

STRANDBURG, Katherine. Privacy, Big Data, and the Public Good: Frameworks for Engagement. **Cambridge University Press**, 2014. Available at: https://www.cambridge.org/core/books/privacy-big-data-and-the-public-good/59C9CBE8F9E4D4628D3EAB1C1B9C7E9A. Accessed on: July 27, 2024.

TENE, Omer; POLONETSKY, Jules. Big Data for All: Privacy and User Control in the Age of Analytics. **Northwestern Journal of Technology and Intellectual Property**, v. 11, n. 5, 2013. Available at: https://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1. Accessed on: July 27, 2024.

TREHAN, Kriti. Is Consent Really Dead? **Amsterdam Privacy Conference**, 2018. Available at: https://ssrn.com/abstract=3247015. Accessed on: July 27, 2024.