PRIVACY AND REGULATION: DIGITAL TRACKING ON THE INTERNET UNDER THE GENERAL LAW OF PERSONAL DATA PROTECTION

Marcelo Augusto Pedreira Xavier
Sólon Bevilacqua

Universidade Federal de Goiás (UFG), Goiânia – GO, Brazil

This article analyzes data regulation in Brazil, consolidated by the General Law for the Protection of Personal Data (LGPD). From the combination of data analysis of the Brazilian regulatory flow (RegBR) and the evaluation of practices about using cookies and other digital tracking mechanisms, we seek to identify Brazil's regulatory norms related to data privacy, and diagnosis your application. The survey also identifies who the organizations are and why they collect citizen data. The results of empirical research point out that most pages are still not sufficiently transparent with personal processing data. It is argued that the acts of the Brazilian National Data Protection Authority (ANPD) have a strong relationship with economic regulation, given the relevance of privacy in other regulatory acts and notes resulting from the normative and bibliographic review.

Keywords: privacy; regulation; internet; data; protection.

DOI: https://doi.org/10.21874/rsp.v74i3.7824 ISSN: 0034-9240 | e-ISSN: 2357-8017
Submitted: September 5, 2022. Accepted: October 13, 2022.
Original version.

PRIVACIDADE E REGULAÇÃO: RASTREAMENTO DIGITAL NA INTERNET SOB A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

O presente artigo analisa a regulação de dados no Brasil, consolidada pela Lei Geral de Proteção de Dados Pessoais (LGPD). A partir da combinação da análise de dados do fluxo regulatório brasileiro (RegBR) e da avaliação das práticas no uso de *cookies* e outros mecanismos de rastreamento digital, busca-se identificar as normas reguladoras relativas à privacidade de dados no Brasil e diagnosticar sua aplicação. O trabalho também identifica quem são as organizações e por que coletam dados dos cidadãos. Os resultados da pesquisa empírica apontam que a maioria das páginas ainda não é suficientemente transparente com o tratamento de dados pessoais. Defende-se que os atos da Autoridade Nacional de Proteção de Dados (ANPD) tem forte relação com a regulação econômica, tendo em vista a relevância da privacidade nos demais atos reguladores e apontamentos decorrentes da revisão normativa e bibliográfica.

Palavras-chave: privacidade; regulação; internet; dados; proteção.

PRIVACIDAD Y REGULACIÓN: MONITOREO DIGITAL EN INTERNET BAJO LA LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES

Este artículo analiza la regulación de datos en Brasil, consolidada por la Ley General de Protección de Datos Personales (LGPD). A partir de la combinación del análisis de datos del flujo regulatorio brasileño (RegBR) y la evaluación de prácticas en el uso de *cookies* y otros mecanismos de seguimiento digital, se busca identificar las normas regulatorias relacionadas con la privacidad de datos en Brasil, y diagnosticar su aplicación. La encuesta también identifica quiénes son las organizaciones y por qué recopilan datos de los ciudadanos. Los resultados de la investigación empírica señalan que la mayoría de las páginas aún no son lo suficientemente transparentes con el procesamiento de datos personales. Se argumenta que los actos de la Autoridad Nacional de Protección de Datos de Brasil (ANPD) tienen una fuerte relación con la regulación económica en vista de la relevancia de la privacidad en otros actos normativos y notas resultantes de la revisión normativa y bibliográfica.

Palabras clave: privacidad; regulación; internet; datos; protección.

1. INTRODUCTION

After the leakage of information scandals and the misuse of private information by companies and governments, many countries announced efforts to update or establish specific laws to protect personal data. The global backlash of cases like those revealed by Edward Snowden in 2013 and the Facebook-Cambridge Analytica in 2016 exposed the destructive potential of privacy breaches. In this context, rules such as the General Data Protection Regulation (GDPR) in the European Union forced emerging countries to create their regulations.

With Brazil, it was no different. The General Data Protection Law (LGPD) was edited in 2018 to establish instruments and guarantees so that citizens, holders of their data, could exercise their rights. Still, in 2021 the press reported that a digital security laboratory identified data leaks that exposed the personal information of 200 million Brazilians.

However, people are unaware of the privacy exploitation in daily internet access, as some companies collect personal information about habits, consumption, and search history without the user's consent. This data collected through digital tracking, primarily through cookies, is returned to users as personalized advertisements.

Good practices, such as alerting users and offering the possibility to prevent internet access monitoring, can improve the transparency of the information collection process. At the same time, several regulations from regulatory agents emerged to grant applicability to the protection of the new law.

Therefore, the research aims to answer the question: What data protection rules affect the regulatory flow, and how have internet pages treated privacy after the entry into force of the LGPD? To answer, are analyzed the 100 websites most accessed by Brazilians to identify whether these web pages offered adequate policies and resources available so that their users choose what they want to share or not. The hypothesis defended is that there is still much to improve for respecting privacy to be adequate to the law.

Also, to analyze and identify regulatory norms, data and metrics on this topic were extracted from the RegBR tool (https://infogov.enap.gov.br/regbr). The first section of the work contains a brief review of the literature, legislation, and best privacy and data protection practices.

After, we are explained how digital tracking works on the internet. The last sections exposed the methodology applied to the analysis. Finally, the results focus on improving public policies related to the research theme and are presented and discussed.

2. BACKGROUND AND LITERATURE REVIEW

The theoretical debate about the right to privacy (right to be alone) equates it to the institute of property. In this perspective, personal information is part of its owner's patrimony. The decision to disclose or not belongs to him. Warren and Brandeis (1890) say that without his

consent, it should protect against unauthorized publication with legal action of tort for damages. Additionally, it would be appropriate for an injunction in some limited cases.

If technology evolves throughout history, legal privacy protection should also be updated (Warren & Brandeis, 1890). There was great concern that not only the facts but the thoughts, feelings, and emotions that people wanted to keep private would be publicized by the press.

Another theoretical perspective on the value of privacy considers the potential for unintended consequences caused by violating it. Floridi (2017) argued about the reductionist perspective, which assesses both the personal point of view, in case of suffering, for example, and the social perception, such as other types of injustice. Under this other conceiving, privacy is still an asset, but with an instrumental feature, an essential condition to preserve human interactions.

This perspective coincides with the conception that privacy is one of the forms of materialization of intimacy. Alonso (2005) explains that intimacy is related to a person's deep, hidden, and secret interior: It is something inaccessible, invisible that only she knows, where only she can freely elaborate or build her action, and where he processes his inner life. It is unknown even to the law, even if it protects it. While intimacy is in a pre-legal scope, privacy is under legal protection; it consists of the practice of visible, tangible human acts, which may become public or private knowledge (Alonso, 2005).

In the literature, there are at least four different types of privacy. In addition to physical privacy, which limits the ability of others to interact with or invade your personal space; mental privacy, which refers to freedom from psychological interference or intrusions into your mental life, from not being manipulated; decisional privacy, which excludes the ability to intervene in decisions in relevant fields such as education, medical treatment, career, work, marriage, faith, etc.; and, finally, informational privacy, to restrict worrisome facts about themselves (Floridi, 2017). Although these four types of privacy, while interconnected and overlapping, are not confused.

In the present analysis, personal data protection is a true expression of the right to information privacy. In this way, Facchini Neto and Demoliner (2018) summarize how the notion of privacy has evolved worldwide under many theoretical views, demonstrating that this right can be synonymous with an exclusion, limitation, and control of access to personal information.

2.1 The protection of privacy in international law

The question of privacy is present in several legal protection instruments with global value. Mazzuoli (2011) defines Public International Law as the set of principles and rules that govern the conduct of States, organizations, and individuals that form the international community, aiming at security and world peace by stabilizing diplomatic relations and establishing objectives and common goals. Thus, through conventions, treaties, and declarations, the most diverse countries find points of agreement, negotiate and submit to standard rules for themselves.

Such norms allow sovereign entities to find and dispose of ordinary limits that must not be violated. This occurs mainly in human rights, as shown in the Universal Declaration of Human Rights (UDHR). This instrument and others that came later, such as the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social, and Cultural Rights (ICESCR), have enabled advances in protecting the dignity and fundamental freedoms of people around the world. In the field of privacy, it is possible to mention sections 12 of the UDHR, 17 of the ICCPR, and 1st of the ICESCR. These provisions contain expressions related to protecting privacy and the right to self-determination.

Another instrument of international law aimed at protecting privacy, especially in the digital field, is the Convention for the Protection of Individuals about the Automatic Processing of Personal Data (Convention 108), established in 1981 by the Council of Europe. The council promotes human rights, including data protection, being the first and only international treaty to address this issue. The treaty is available for accession by European and non-European countries. The recently updated document, renamed Convention 108+, is expanding rapidly, with 55 signatory countries and at least 8 (eight) observers, including Brazil (Fachinetti & Camargo, 2021).

2.2 The protection of personal data in Brazil as a form of regulation

Recently, the list of fundamental rights presented in the Constitution of the Federative Republic of Brazil of 1988 (CRFB/1988) was expanded. Constitutional Amendment No. 115, enacted on February 10, 2022, modified the constitutional text to include the protection of personal data in this role and define the national legislative competence for the subject. As seen in article V, subsection X, the CRFB/1988 already reproduced the protection of private life and intimacy as the UDHR and other treaties. Although this previous generic constitutional protection could already be enough, the constituent raised the issue of personal data as an autonomous fundamental right, giving its protection legal superiority.

For Brazilian law, private life is part of personality rights, as shown in Article 21 of the Civil Code (Law 10,406/2002). Long before the amendment included the protection of personal information in the Constitution, the Legislative Power had already edited Law 12,965/2014 (Civil Rights Framework for the Internet), and a long time later, Law 13,709 (General Personal Data Protection Law, aka by the acronym LGPD), published on August 14, 2018, but which only came into full force in August 2021, when his sanctioning provisions finally came into force.

The LGPD created Brazil's legal bases to support personal processing data. The law lists a series of operations (Article 5, X) to define the treatment, including collecting, storing, and using information that identifies or can identify people. Individuals are defined by law as the actual holders of these data, establishing rights and guarantees. Thus, the LGPD allows public or private institutions to collect and use the personal data of Brazilian citizens if they comply with the rules established therein.

One of the grounds that allow collection is the legal institute of consent. This means that a person can authorize or oppose the processing of their data in some situations. As provided for in Article 5 (XII); Article 7, subsection I and paragraphs 4 to 7; Article 8; Article 9 and respective paragraphs. This excerpt from the law says that the organizations need to prove that the treatment consents.

Such legal provisions explain that this consent must be prior, clarified, and restricted to the respective purposes proposed initially. Consent can only be waived if the user has made the data manifestly public or in case of some limited other exceptions. Otherwise, the authorization will be considered void (Article 9, paragraph 1st, LGPD). Therefore, the LGPD promotes transparency of personal data processing, enabling people to exercise their informative self-determination.

Among other rules, the ANPD (National Data Protection Authority), a Brazilian agency for data regulation, was also created to regulate and supervise the matter. This Brazilian agency emerged in a model that distanced itself from the North American and British models, where data protection is the responsibility of antitrust authorities.

Also, the chosen format differs from the traditional regulatory model adopted in Brazil. The first Brazilian regulatory agencies were created to inspect private entities, mainly after privatizations carried out by the public authorities. The National Electric Energy Agency (ANEEL), built in 1996, inaugurated the regulatory model in that country. His creation was inspired by international experience, privileging the agencies' decision-making and financial autonomy and setting mandates for their directors not coinciding with the elections of the Executive Power (Pacheco, 2006). This autonomy represents an advance, which breaks with his protagonist's paper in defining public policies and investments. Thus, regulation in Brazil emerged to organize the sectors where the state monopoly had been broken.

However, personal information processing has never been an exclusive activity of the Government. Contrariwise, data operations are inherent to all economic activities. A comprehensive study on competition defense and data protection institutions produced by the Brazilian Administrative Council for Economic Defense points out that data regulation is interrelated with the competencies of the council itself (Conselho Administrativo de Defesa Econômica [CADE], 2021). This statement helps to understand the unique nature of this form of economic regulation.

The ANPD, in turn, was created on a modification of the LGPD and began to function effectively in November 2020. In a new recent amendment into this law, a Provisional Measure transforms the data authority into a special autarchy, the exact legal nature of other Brazilian regulatory agencies.

The authority has an extensive regulatory calendar for the 2021-2022 biennium (Portaria ANPD nº 11/2021) and has published crucial regulatory impact analysis reports, promoting studies, guidelines, and resolutions applicable to the most diverse sectors of the economy.

This way, it is noted that the LGPD has increased transparency on personal processing data, requiring government organizations and companies to promptly clarify to people about operations involving these assets of individuals. At the same time, it established data regulation as its segment, acting as an actual regulatory agency.

2.3 Internet Cookies: The big data of behavioral privacy as a raw material thus

Information privacy has become a commodity, and his political and economic misuse raises concerns. Technological evolution has reached unprecedented levels, and digital networks are an environment conducive to the espionage of intimacy. Thereby, are established a proper surveillance system is (Lemos & Di Felice, 2014).

The intense accumulation of data is one factor that allows interference in decisions, from exploring the materialization of intimacy. Many studies try to demonstrate how dependence on technology would affect human intelligence because as thousands of data are gathered, as with big data, statistical sampling loses value. It is no longer about researching trends in a population but finding small-scale patterns (Floridi, 2017).

Technological advances and the immensity of information make it possible to individualize each conduct. Thus, it is possible to foresee people's decisions by collecting their data and digital traces. It is necessary to deal with big data wisely because although it can provide relevant insights, it can cause significant options. Patterns that are invisible to the human eye that the data economy can detect bring new challenges for data scientists, including understanding which ecosystem they are evolving to present the problems they can create and possible solutions to these questions (O'Neil, 2020).

Data mining through internet digital tracking is the primary input in the economic activity of large technology networks. Google and Facebook are the most significant examples of how this market works. In resume, by collecting data in an unsupervised way, they can enable effective ads that founding "Surveillance Capitalism" (Zuboff, 2020). It is not about selling personal data but about trading behavioral surplus. These digital networks collect information that allows them to predict decisions, vending this decision-making potential as an asset when targeting online advertising.

One of the mechanisms used to monitor users is internet cookies. They are part of a network protocol created in 1994 by Netscape company to make it possible for internet pages to deposit small files on the computer of the people who access them (Oliveira & Silva, 2019). Later they would become one of the most popular digital tracking mechanisms, allowing users to monitor their behavior and trace their profiles.

These files have several functions, including directing digital advertising. They store information while browsing web pages, enabling, among others, to monitor users' audience and navigation trails. Hoofnagle, Soltani, Good, Wambach, and Ayenson (2012) explain that

"The privacy problem from cookies comes from the aggregation of this tracking across different websites into profiles and through attempts at linking this profile to the user's identity." As soon, the collected data with these technologies can be very personal.

They can reduce repetitive information traffic, promote and maintain identification or authentication, register preferences, customize the websites visited, and primarily offer products and services through personalized ads (Avelino & Silveira, 2016). Internet advertising is, as a rule, based on behavioral data produced when browsing.

The cookies can also promote malicious controls, making screens an open window into our online lives. Even after being eliminated or blocked, browser software allows for regeneration, being able to (re)activate tracking and thus monitor and record activities, making browser history one of the minor private aspects of our life (Ayenson et al., 2011; Floridi, 2017).

In the United States, internet cookies have been in public policy debate. In 1996, advertisers sought to collaborate with economic regulation, creating self-regulatory associations such as the NAI – Network Advertising Initiative. In 2000, Bill Clinton's administration even banned the use of cookies on federal government websites, and a few months later, there were at least three projects in the US Congress to regulate their use (Zuboff, 2020).

In the private market, however, self-regulation has not stopped tracking from spreading more and more. Researchers recorded that in a list of the 100 most accessed websites, over 5,600 cookies were installed, of which 4,900 belonged to third parties other than the page accessed, and 97 of these domains, including government websites, contained digital tracking associated with addresses controlled by Google (Ayenson et al., 2011).

The European Commission has established guidelines for using cookies and similar technologies, creating a mandatory model for government websites in that block (EC, 2021). Scholars say that evaluating the presence of cookie notices is an effective way to verify compliance with the law. In Europe, research of this nature pointed out that the entry into force of the GDPR caused a 16% growth in the presence of alerts about this tracking (Degeling et al., 2019; Strycharz et al., 2021).

The free collection of personal information on the internet, often without consent, fuels the algorithmic influence machine. It is a form of manipulation that works as an invisible filter, shaping how things are sighted. It is natural for human beings to make decisions in line with their interests, but what algorithms do imperceptibly is to drive an experience of filtered social existence, like psychological obesity (Pariser, 2012). Experiments demonstrate how content exposure can influence emotions, promoting large-scale contagion through digital networks (Kramer et al., 2014).

Given this scenario, the informational transparency requirements of the LGPD should shed light on such data collection practices. How organizations have warned about the existence of this treatment is one of the concerns of this work. To comply with the law and demonstrate

respect for people's privacy, pages need to be transparent about their privacy practices and obtain consent in a sufficiently informed way.

3. METHODOLOGY

Initially, we sought to understand the data available in RegBR and how they could contribute to improving the debate on data regulation. This framework allows for obtaining information about the regulatory flow and evaluating metrics of popularity, restrictiveness, complexity, and influence in sectors of the economy. The tool also provides the complete database for own evaluations.

The first step was verifying that there were rules on privacy and protection of personal data in the complete RegBR base. To this end, an extraction was provided through the textual search for acronyms, expressions, and keywords (personal data, privacy, data protection, data processing, LGPD, ANPD) to measure the regulatory relations.

In addition to this data selection, we promoted an assessment of the practical application of data regulation rules on the Internet. Among the hypotheses for processing personal data is Article 7 (I) of the LGPD. It deals with the possibility of consent. For this research, the collection of browsing data using cookies and other tracking technologies is possible.

In this context, the object of the research also included an evaluation of the 100 most accessed websites in Brazil, based on the ranking for February published by Casagrande (2022). The number of pages represents a small but robust sample to enable a punctual cut based on human observation. We sought to identify how the pages visited present the request or notice about the treatment of personal information.

The ranked pages were visited to verify the presence of alerts and policies regarding data collection using cookies and other browse navigation tracking technologies. This verification focused on the home page of each domain accessed, additionally going through the respective privacy policies.

A questionnaire was previously prepared to be answered at each visit. In the list of questions, we sought to identify the presence of alerts about the collection of personal data and whether the information was sufficiently detailed to enable a decision (consent) to accept or not the collection of information. Also, the available options were evaluated regarding the possibility of refusing to track or customize information collection.

The accesses to the searched sites were carried out between April 4th and May 5th, 2022, using the most up-to-date 64-bit version of the Google Chrome browser available at the time, always from the same home computer directly connected to the internet network and with all advertising inhibition or cookie rejection functions disabled.

During each visit, tools were used to identify trackers and collect the list of installed cookies, to catalog the URL and the origin entity of these files. The analyzes refer to trackers from external

domains, also known as third-party cookies or third-cookies. Primary trackers were not analyzed in this article due to limitations of the collection tools and because they tend to have less impact on privacy, as they are not as extensively used in digital marketing as third parties.

To identify the trackers, extensions available on the Chrome Web Store were used: Get Cookies.txt, Awesome Cookie Manager, and DuckDuckGo Privacy Essentials. The tools were adjusted to allow a complete listing of the tracking mechanisms in each access. The extractions and analyses of both RegBR data and tracking research were carried out with computational tools for data integration, such as Qlik Sense, Orange DataMining, and Python.

4. DISCUSSION AND RESULTS

From the complete RegBR database, at least 197 regulatory acts have been located that mention in whole or in part privacy and the protection of personal data, including 103 decrees, 31 resolutions, and 26 laws. Of this total, 43 rules are no longer in force. The Regulatory Agencies that most dealt with the matter were ANATEL (National Telecommunications Agency), with 20 acts, and ANS (National Supplementary Health Agency), with 14 acts.

The regulatory impact on personal data was also analyzed in terms of temporal flow and impact on economic sectors. The Administrative Activities sector stands out with 40 standards. Then appear: Health and Social Services; Information and Communication; and, Financial and Insurance Services, with 28, 27, and 21 regulations, respectively. In the timeline, the most significant growth of regulatory norms occurred in 2018, when 14 acts were edited, which also appeared in 2019. The peak occurred in the last two years, adding 49 regulations, 23 in 2020 and 26 in 2021.

RegBR points out the most sought-after laws among the subject's regulations regarding popularity. The measurement uses information from Google Trends and the DOU (Diário Oficial da União). Data updated in May 2022 indicated that Law 13,982/2020 (Covid-19 Emergency Aid) had the highest average in Google searches, while Law 8,666/1993 (Bids and Contracts) was the one with the highest frequency in the DOU.

Although it is not possible to make direct comparisons, a verification of the search frequency of terms on Google Trends shows that interest in "LGPD" over time in the last five years has an average of 22 points, against 6 (six) for "Lei de Licitações" (references to Brazilian bidding's law). Compared to the search for the emergency aid law, the search for the data protection law was only surpassed once, in May 2020, when the first added 20 points against 18 for the second. In the DOU, Law 13,709/2018 (LGPD) mentions a significant number, totaling more than 3,000 results. Therefore, it is demonstrated that data regulation would be widespread if included in metrics.

To assess restrictiveness, the complete RegBR database was used to locate the words[1] used to evaluate this measure in the previously selected acts. We've found 3820 occurrences of restrictive terms. The highest incidence was in the Administrative Activities sector with 815 restrictive expressions, whose 215 only in 2020 when it reached its peak. Other sectors with a significant amount of restriction terms were: Information and Communication (671), Health and Social Services (607), and Financial and Insurance Services (369).

The overview of the RegBR database showed that data regulation had been an object of concern not only to the ANPD (responsible for the theme) but also to other regulatory agencies on various topics, especially health how, as described. The COVID-19 pandemic may justify this scenery cause, in this period, episodes about vaccine transparency or monitoring population displacement have many privacy implications. According to the LGPD (Article 5. II), medical data are sensitive data whose treatment requires compliance with stricter rules, following Articles 11 to 13 of that law.

The impact on economic sectors highlights how the market revolves around data. However, in some segments, personal information is even more relevant, so care for protecting this data requires more extensive regulatory intervention. Thus, restrictive measures are justified by the need to preserve people's privacy. Finally, the increase in norms observed in the last five years coincides with the edition of the LGPD, demonstrating that the law sought to regulate by imposing general rules and boosting the issuance of regulatory acts.

However, only the analysis of the regulatory framework cannot diagnose the actual situation of personal data protection in Brazil. For this, it is necessary to look at practical problems, where the law and other applicable rules must be observed. In this way, the present analysis also sought to assess one situation that raises concerns about protecting individual information.

To this end, the study analyzed how cookies and similar mechanisms have observed the regulation of the use of personal data. This way, we analyzed websites on 100 position ranking to Brazil internet addresses. Only 07 did not contain any tracking technology on the homepage, but 04 of these domains don't have visible content because they are addresses used exclusively for internet navigation tracking; that is, tracking networks whose data traffic comes from being embedded in other pages.

Among those identified that contain trackers, 45 sites did not show any forms of notice of data collection. This means that less than half (49.4%) of the pages have warned or asked for users' consent for operations to process their information using cookies. The percentage is lower than that observed in Europe, whose rate jumped from 46.1% in 2018, when GDPR came into force, to 62.1% shortly after (Degeling et al., 2019).

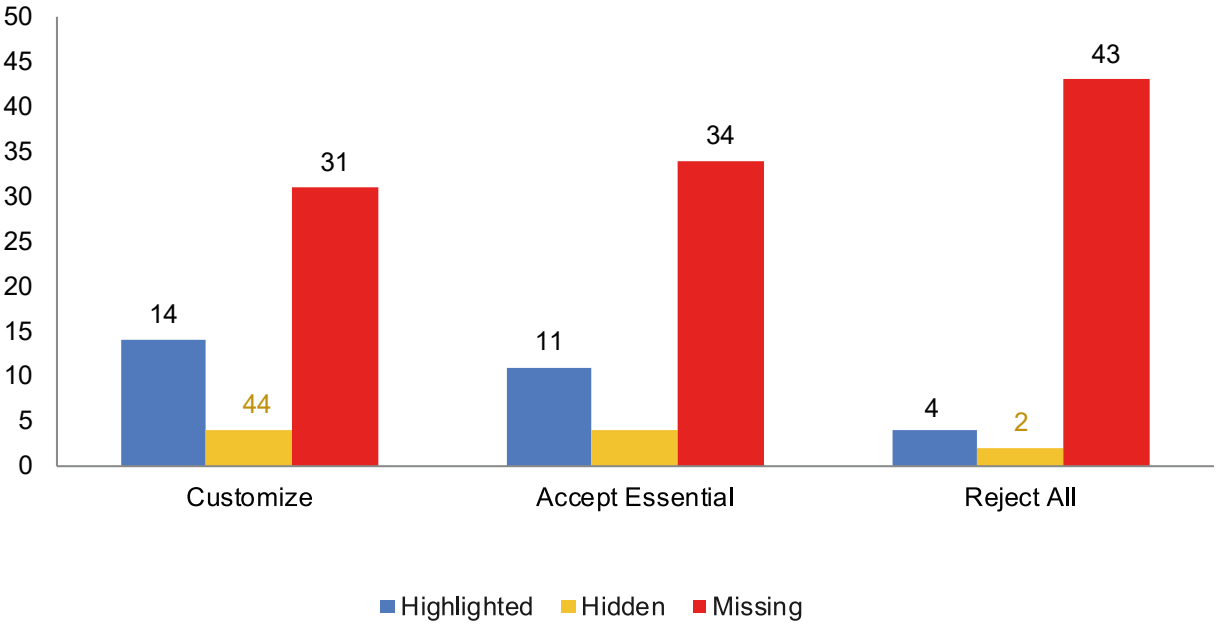
[1] RegBR assesses restrictiveness by measuring the frequency of restrictive terms that means: vetoed, prohibited, closed, prohibited, denied, determines, obliges, orders, imposes, limits, delimits, demarcates, restricts, confines, reduces, defines, must, shall, precisely and need; how as described at: <https://infogov.enap.gov.br/regbr/metricas/restritividade>.

On these pages that warned about data collection, the way to obtain consent was evaluated. A total of 34 domains (equivalent to 69.4% of sites that contained some cookie notice) were observed; there was only one option: fully and unrestrictedly accept tracking. In addition, when accessing the website, the browser automatically installs cookies and other technologies. In other words, even if the user disagreed with the data processing and left the page, the tracking mechanisms were installed and activated automatically on the first access. Only 02 of the visited pages transferred third cookies only after due authorization.

To evaluate consent practices, it was also verified whether the user could choose between the following options: Customize (when the website has any option to personalize consent to install cookies or similar tracking), Accept Essential (if the site has a specific option to allow just tracking that is required to page works), and Reject All (when visited domain allows that user prevents all browse tracking).

Common consent management frameworks have adopted these practices as an appropriate standard (Cooper, 2022). They allow the user to have greater control over data collection from their browsing. The consent options were evaluated at three different levels regarding their form of presentation: if they received similar prominence to the choice to accept everything (Highlighted); whether personalization was made difficult (Hidden); and if there was no option (Missing). The following graph demonstrates the research result:

Figure 1 - Consent Practices



Note: It only includes websites that have cookie warns.
Source: elaborated by the authors.

It is possible to prove that most sites do not allow any customization. This means that, in general, even when advising about data collection, the user doesn't have mechanisms to choose the purposes with agreeing or not. The situation is worse of the possibility of rejecting

tracking, absent in 43 of the 49 pages that warned of the treatment. The lack of autonomy offered demonstrates that there is little interest in making continuous browse tracking difficult.

The assessment also covered the terms of use and privacy policies published by the pages visited. The data presented below evaluated the presence of specific sections on operations using cookies and similar technologies in these documents. We also sought to verify the quality of the information delivered. Similarly, policy verification was carried out at three levels as to how they were given, whether there was enough detail for informed consent (Detailed); if the information was shallow (Insufficient); or if there was no information (Missing).

It was noted that 61% of the pages had some information about data collection, but with little or no detail; in general, they were limited to synthetically reproducing generic expressions without specifying the purpose and types of tracking. Also, 22% did not even include a specific section on this subject in their policies. Only 17% provided full details. The data are represented in Table 1 below:

Table 1 - Cookies Policy

Situation	Percentage
Insufficient	61%
Missing	22%
Detailed	17%

Source: elaborated by the authors.

The transparency of the pages was also evaluated regarding the details of the technologies and partners that collect behavioral information from navigation. We sought to verify whether information such as the nominal listing of cookies, their duration, domain of origin, identification of third parties that promote data collection with their respective objectives, and links to these partners' policies were present. In this sense, the study showed that 48% do not publish such details, as shown in Table 2:

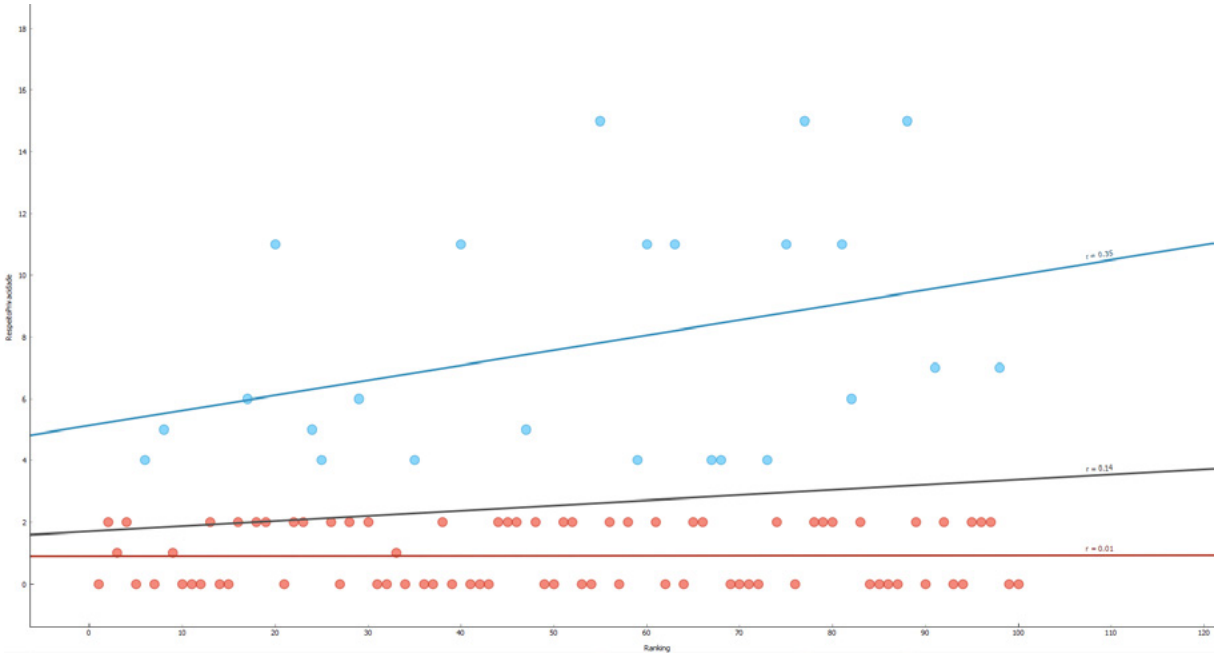
Table 2 - Tracking Details

Situation	Percentage
Missing	48%
Insufficient	35%
Detailed	17%

Source: elaborated by the authors.

In addition, we try to determine whether there was any relationship between the audience of the pages and respect for privacy based on the analysis described above. It was noted that there is a noticeable weak correlation between ranking position and transparency. Good practices for personal data protection decline when they rise in the rankings. In this way, the study pointed out a tendency to disrespect the regulation in more visible sites. Figure 2 below shows, in Linear Regression, how this situation can be observed.

Figure 2 - Dispersion of Privacy Respect



Note: The X-axis represents the ranking position (where 1 is the site with the highest audience, and 100 is the lowest). In turn, the Y axis is respect for privacy, composed of the sum of good practices observed. The group in blue gathers the sites that warned about cookies, and the red color represents pages that did not contain this type of warning.
Source: elaborated by the authors.

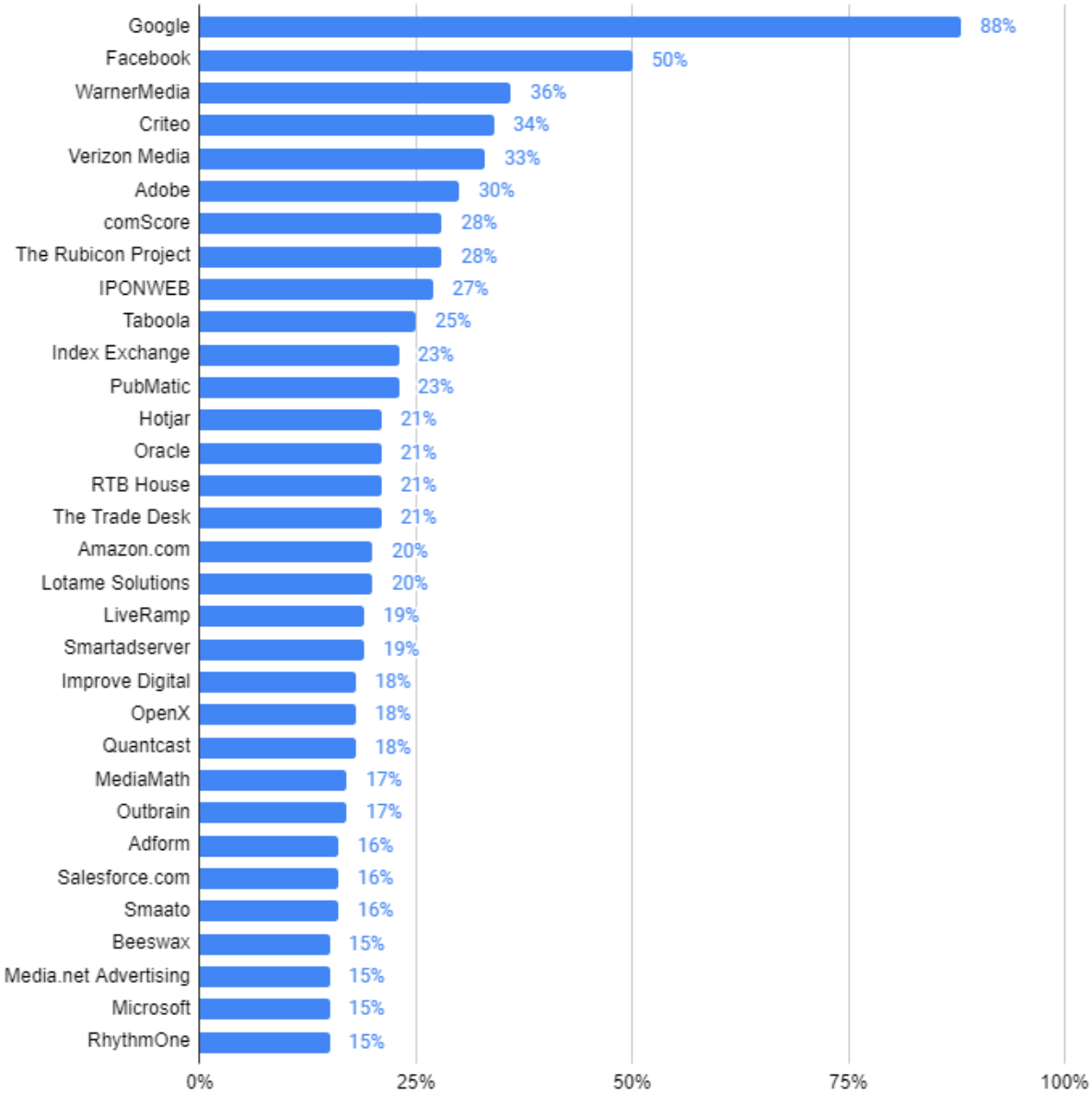
The analysis showed that in the group of pages that contain cookie notices, the practical set of actions that privilege privacy is more significant in the lower positions of the ranking. However, some respect and violate personal data protection throughout the sites. The sample of only 100 sites is tiny compared to the immensity of the internet, so it cannot accurately point out reality. Thus, it cannot be generalized.

It should be noted that the list of domains analyzed contains pages hosted in different locations. In this way, many observed practices stem from applying external regulations such as the GDPR. In any case, the possible conclusion is that there are gaps in improving compliance with Brazilian law.

Regarding the purpose of tracking navigation, it was found that 52% of the mechanisms are used for advertising. Most information collection displays personalized advertisements based on the user's interest and behavior. Another 39% are in analytics; they monitor activities to measure the audience and support other decision-making. Still, the remaining 9% of trackers have different goals that could not be classified.

A total of 3,445 tracking domains controlled by third parties were identified, totaling 246 different entities present in the 100 pages visited. Google is present in 88% of the sites, followed by Facebook, detected in 50% of the addresses. WarnerMedia completes the podium with 36% prevalence. Compared with other studies mentioned in the theoretical framework, there is alignment. The exploitation of behavioral data mining also includes big companies like Oracle and Amazon. Figure 3 lists organizations with prevalence in 15% or more visited sites.

Figure 3 - Tracking Entities with the Most Prevalence



Source: elaborated by the authors.

People's privacy is being exposed more than ever. The diagnosis showed that most of the most popular pages in Brazil do not fully comply with the LGPD, as they process personal data without proper consent. Either they do not inform the data collection or collect forced and artificial consent.

The law requires the user to have enough information to decide whether to accept that their personal information is collected. But in most cases, there is little information about the actual purposes of collecting personal information. Zuboff (2020) explains that large organizations that collect data benefit from the absence of regulation precisely because of the inability to regulate the Internet effectively.

Geographic barriers are practically unknown or non-existent in the digital network environment (Castells, 1999, 2009; Lemos & Di Felice, 2014; Floridi, 2017). This absence of borders seems to work as an escape mechanism from regulation.

Digital trackers, materialized through cookies and similar technologies, were present on practically all websites surveyed, but consent was only collected to some extent in half of them. Even where there were privacy notices, the policies were not detailed enough. Many organizations worldwide continue to collect browsing information, primarily for advertising revenue.

The simple lack of transparency demonstrates a violation of data protection rules. The law and current regulations seem insufficient to enforce respect for the self-determination of individuals' information.

Oliveira and Resende (2020), when proposing an instrument for evaluating institutional governance for the public sector, point out the types of isomorphisms of Institutional Theory as ways to shape the behavior of organizations, attributing LGPD as one of the normative forms of this drive. Thus, data inspection and regulation should be public policies capable of improving citizens' privacy to improve the scenario pointed out in this study.

5. CONCLUSIONS

The present work intends to identify which regulatory acts are related to the data protection rules of the LGPD and to diagnose how the internet pages have applied this law to practices regarding the tracking of internet browsing through cookies and other similar technologies.

The background and literature review included the national and international rules for protecting personal data. It was possible to observe that privacy preservation stems from relevant legal instruments dealing with human rights. It has been argued that people are often unaware of how much their privacy can be violated when sensitive information is leaked while browsing the internet.

It was explained that companies from different locations always collect information about browsing, consumption, and search habits. For this reason, it is understood that it is necessary to improve the transparency of this information collection through practices that include alerting the user, obtaining consent, and offering the possibility to customize or prevent such monitoring.

These practices are closely linked with regulatory instruments, which the RegBR database demonstrates. The data and metrics proposed there proved relevant to understanding data regulation as a subject to be viewed as a public policy whose debate can use this critical tool to measure and monitor the Brazilian regulatory flow.

Finally, the data collected according to the described methodology showed that more than half of the visited pages promoted data collection via digital tracking but not adequately, in disagreement with the privacy protection norms. Therefore, confirming the hypothesis that there is still much to be done in line with the law to improve respect for privacy.

The research was limited to a small sample of one hundred sites with the highest audience in Brazil. In this way, the conclusions obtained, although they cannot represent the vastness of the internet. However, this study can diagnose a portion that affects millions of citizens who use their devices to access those addresses.

Thus, this article demonstrates your need and importance. Other studies like this can contribute to the improvement of privacy regulation and data protection. Thereby, it is intended to expand and deepen this research in the future to understand the relationship between the protection of personal information and human rights, mainly those who are promoted by public policies.

REFERENCES

Alonso, F. R. (2005). Pessoa, intimidade e o direito à privacidade. In: Martins, I. G. S., & Junior, A. J. P. (coords). *Direito à Privacidade*. Aparecida: Ideias & Letras; São Paulo: Centro de Extensão Universitária.

Avelino, R. S., & Silveira, S. A. (2016). A dependência do rastreamento comportamental online para a economia globalizada. *Simpósio Internacional LAVITS. ¿Nuevos paradigmas de la Vigilancia?,* Buenos Aires, IV. Retrieved from https://www.rodolfoavelino.com.br/a-dependencia-do-rastreamento-comportamental-online-para-a-economia-globalizada/

Ayenson, M. D., Wambach, D. J., Soltani, A., Good, N., & Hoofnagle, C. J. (2011). *Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning*. Social Science Research Network. https://doi.org/10.2139/ssrn.1898390

Cadwallader, C. & Graham-Harrison, E. (2018). *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in a major data breach*. The Guardian. Retrieved from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Casagrande, E. (2022). *Top 100 sites mais acessados no Brasil [Edição 2022]. Principais sites do Brasil classificados por tráfego em fevereiro de 2022.* Semrush Blog. Retrieved from https://pt.semrush.com/blog/top-100-sites-mais-visitados/

Castells, M. (1999). *Sociedade em rede* (R. V. Majer, Trans.). São Paulo: Paz e Terra, 1999.

Castells, M. (2009). *Comunicación y Poder* (M. Hernández, Trans.). Madrid: Alianza Editorial.

Conselho Administrativo de Defesa Econômica. (2021). *Benchmarking internacional sobre as instituições de Defesa da Concorrência e de Proteção de Dados.* Ministério da Justiça e Segurança Pública. Retrieved from https://cdn.cade.gov.br/Portal/centrais-de-conteudo/publicacoes/estudos-economicos/documentos-de-trabalho/2021/Documento%20de%20Trabalho%20-%20Benchmarking-internacional-Defesa-da-Concorrecia-e-Proteacao-de-dados.pdf

Constituição da República Federativa do Brasil de 1988. Retrieved from http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.Htm

Convention for the Protection of Individuals about Automatic Processing of Personal Data 1981, ETS 108. Retrieved from https://edps.europa.eu/data-protection/our-work/publications/legislation/council-europe-convention-no-108-data-protection_en

Cooper, S. (2022). *6 Best Cookie Consent Tools for 2022*. Comparitech. Retrieved from https://www.comparitech.com/data-privacy-management/best-cookie-consent-tools/

Declaração Universal dos Direitos Humanos de 1948. Retrieved from https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por

Decreto nº 591, de 6 de julho de 1992. Pacto Internacional sobre Direitos Econômicos, Sociais e Culturais. Promulgação. Retrieved from http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0591.htm

Decreto nº 592, de 6 de julho de 1992. Pacto Internacional sobre Direitos Civis e Políticos. Retrieved from http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2019). *We value your privacy ... Now take some cookies: Measuring the GDPR's impact on web privacy.* NDSS. Retrieved from https://arxiv.org/pdf/1808.05096.pdf

Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm

Escola Nacional de Administração Pública. (2022). *RegBR. Dados Atualizados em Maio/2022 com foco em normativos regulatórios*. ENAP. Retrieved from https://infogov.enap.gov.br/regbr

European Commission. (2021). *The Europa Web Guide. 04. Cookies and similar technologies – WEB GUIDE - EC Public Wiki.* Retrieved from https://wikis.ec.europa.eu/display/WEBGUIDE/04.+Cookies+and+similar+technologies

Facchini Neto, E., & Demoliner, K. S. (2018). Direito à Privacidade e Novas Tecnologias Breves Considerações Acerca da Proteção de Dados Pessoais no Brasil e na Europa. *Revista Internacional Consinter de Direito. IV* (VII). http://doi.org/10.19135/revista.consinter.0007.01

Fachinetti, A. F., & Camargo, G. (2021). Convenção 108+: o tratado de proteção de dados e a relevância do tema para o Brasil. *Revista Consultor Jurídico (Conjur)*. Retrieved from https://www.conjur.com.br/2021-jul-04/opiniao-convencao-108-relevancia-protecao-dados

Floridi, L. (2017). *La quarta rivoluzione - Come l'infosfera sta trasformando il mondo* (M. Durante, Trans). Milano: Raffaello Cortina.

General Data Protection Regulation (GDPR). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

Greenwald, G., & Macaskill, E. (2013). *NSA Prism Program Taps in to User Data of Apple, Google, and Others.* The Guardian. Retrieved from http://www.guardian.co.uk/world/2013/jun/06/ustech-giants-nsa-data

Hoofnagle, C. J., Soltani, A., Good, N., Wambach, D. J., & Ayenson, M. D. (2012). *Behavioral Advertising: The Offer You Cannot Refuse*. Harvard Law & Policy Review, *6* (2012), 274-296, Retrieved from https://ssrn.com/abstract=2137601

Kramer, A. D. I., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. https://doi.org/doi:10.1073/pnas.1320040111

Lei nº 10.406, de 17 de julho de 2002. Institui o Código Civil. Retrieved from http://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406.htm

Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Retrieved from http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Retrieved from http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Lemos, R., & Di Felice, M. (2014). *A vida em rede*. Campinas: Papirus 7 mares.

Mazzuoli, V. O. (2011). *Curso de direito internacional público* (5th ed). São Paulo: Editora Revista dos Tribunais.

Medida Provisória nº 1.124, de 13 de junho de 2022. Altera a Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais, transforma a Autoridade Nacional de Proteção de Dados em autarquia de natureza especial e transforma cargos em comissão. Retrieved from https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Mpv/mpv1124.htm

O'Neil, C. (2020). *Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia* (R. Abraham, Trans.). Santo André, SP: Editora Rua do Sabão.

Oliveira, J. V, & Silva, L. A. (2019). "É de Comer?" Cookies de Navegador e os Desafios à Privacidade na Rede. *Revista Tecnologia e Sociedade, 15* (37), 297-310. Retrieved from https://periodicos.utfpr.edu.br/rts/article/view/8419

Oliveira, N. P., & Resende, P. C. J. (2020). Proposta de instrumento para avaliação da governança organizacional em uma instituição do setor público. *Revista do Serviço Público – RSP 71* (2), 397-426. Retrieved from http://repositorio.enap.gov.br/handle/1/5523.

Pacheco, R. S. (2006). Regulação no Brasil: Desenho das Agências e Formas de Controle. *Revista Administração* Pública (RAP). 40 (4). 523-543. https://doi.org/10.1590/S0034-76122006000400002

Pariser, E. (2011). *O filtro invisível: O que a internet está escondendo de você* (D. Alfaro, Trans.) Rio de Janeiro: Zahar.

Portaria ANPD nº 11, de 27 de janeiro de 2021. Torna pública a agenda regulatória para o biênio 2021-2022. *Autoridade Nacional de Proteção de Dados*. Retrieved from https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313

Rosenberg, M., Confessore, N., & Cadwallader, C. (2018). How Trump Consultants Exploited the Facebook Data of Millions. *The New York Times*. Retrieved from https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

Strycharz, J., Smit, E., Helberger, N., & Noort, G. (2021) No to cookies Empowering impact of technical and legal knowledge on rejecting tracking cookies. *Computers in Human Behavior. 120* (2021). https://doi.org/10.1016/j.chb.2021.106750

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review, IV* (5). https://doi.org/10.2307/1321160

Zuboff, S. (2020). *A Era do Capitalismo de Vigilância: A luta por um futuro humano na nova fronteira do poder* (G. Schlesinger, Trans.). Rio de Janeiro: Intrínseca.

Marcelo Augusto Pedreira Xavier
https://orcid.org/0000-0001-5974-9364
Master's student in Human Rights (PPGIDH), Universidade Federal de Goiás (UFG). Sspecialist in External Control and Public Governance, Instituto Brasiliense de Direito Público (IDP). Bachelor of Laws, Centro Universitário Cambury (UNICAMBURY). Graduated in Information Technology Management, Centro Universitário de Goiás (UNIGOIÁS).
marceloaugustoweb1@gmail.com

Sólon Bevilacqua
https://orcid.org/0000-0002-0050-3527
Post-Doctorate, Universidade Federal de Uberlândia (UFU). Doctor in Psychology from the Pontifícia Universidade Católica de Goiás (PUC/GO). Master's in Business Administration, Universidade Federal de Uberlândia (UFU). Graduated in Business Administration, Universidade Federal do Rio Grande do Sul (UFRGS).
solon@ufg.br