Okano, Marcelo Tsuguio; Sousa, Suely Dos Santos; dos Santos, Henry de Castro Lobo; Ursini, Edson Luiz

Article

How do consultants understand the privacy of personal data in brazilian financial institutions?

Contemporary Economics

Provided in Cooperation with:
VIZJA University, Warsaw

Suggested Citation: Okano, Marcelo Tsuguio; Sousa, Suely Dos Santos; dos Santos, Henry de Castro Lobo; Ursini, Edson Luiz (2025) : How do consultants understand the privacy of personal data in brazilian financial institutions?, Contemporary Economics, ISSN 2300-8814, VIZJA University, Warsaw, Vol. 19, Iss. 4, pp. 371-383, https://doi.org/10.5709/ce.1897-9254.572

This Version is available at:
https://hdl.handle.net/10419/340139

Primary submission: 15.07.2023 | Final acceptance: 04.06.2025

How do Consultants Understand the Privacy of Personal Data in Brazilian Financial Institutions?

Marcelo Tsuguio Okano[12], Suely dos Santos Sousa[1], Henry de Castro Lobo dos Santos[2], Edson Luiz Ursini[2]

ABSTRACT The General Data Protection Law (LGPD, initials of the words in Portuguese) aims to safeguard the basic right to privacy and personal freedom, as well as the formation of the personal freedom of each. The primary objective of this investigation is to examine how a group of LGPD consultants applies the theoretical framework of privacy calculation to inform privacy decisions. The investigation was intended to measure the direct relationships of the privacy calculation in the financial sector, and the survey is attempting to determine the perceived threat and expected quality of care. Hypotheses were significant, but regarding personal data, as it is considered important and personal, they are cautious and unwilling to disclose this data to any company, even if there is a benefit or an unfavorable financial situation. Respondents are reluctant to disclose their personal data to trusted companies, such as banks, to receive benefits.

KEY WORDS: privacy, LGPD, privacy by design, privacy calculation.

JEL Classification: K00.

[1]Paulista University (UNIP) , São Paulo, Brazil
[2]College of Technology of University of Campinas (UNICAMP), Limeira, Brazil

1. Introduction

The widespread adoption of digital technologies among individuals is resulting in an enormous proliferation of their data across various platforms such as social networks, social media, and other digital channels. The first important concept associated with privacy is the concept of personal data (Wiśniewski et al., 2021). The enactment of the General Data Protection Law (LGPD, acronym derived from the Portuguese language) aims to safeguard fundamental rights, including freedom, privacy, and the development of personal identity for all individuals (Government of Brazil, 2018).

The Brazilian Law No. 13.709/2018 or General Personal Data Protection Act, discusses the processing of personal data provided in physical or digital media by individuals or legal entities in accordance with public or private law, including various operations that can be conducted manually or digitally (Government of Brazil, 2018).

This legislation is new, and this work aims to help society and companies to think about adaptation strategies, as no product or action alone can guarantee the adequacy of a company to the LGPD (Muncinelli et al., 2021).

The concept of privacy is seen from two different perspectives: the first focuses on the control that the individual exercises over the access of others to himself; the second defines privacy as a condition or state of intimacy (Loch, 2009).

Understanding the value individuals assign to safeguarding their personal data is crucial to business, legislation and public decision making (Ac-

Correspondence concerning this article should be addressed to: **Marcelo Tsuguio Okano**, Paulista University (UNIP) and College of Technology of University of Campinas (UNICAMP), São Paulo, Brazil Rua Barcelar, 1212 São Paulo, Brazil E-mail: prof.okano@gmail.com

quisti et al., 2013). But for this, individuals have to understand some concepts such as data handling and privacy.

Today, personal data includes information that typically identifies persons: address, first names, last name, place of birth, parents' names, personal identification number, taxpayer identification number, as well as fingerprints, retina patterns and the aforementioned: location data and internet-based identifiers (Wiśniewski et al., 2021).

Pedersen (1997) considers privacy to be an important human need and allows people to manage both personal activities and social interactions. Privacy does not mean withdrawing from the presence of others, it involves controlling the amount of contact with others (Pedersen, 1997).

In this research, the privacy calculation theory was adopted as a theoretical lens because, according to Knijnenburg et al. (2017), "privacy calculation" has been used

extensively to describe how people make privacy-related decisions, researchers have found that decisions are not calculated, and currently, privacy calculations have been used in the service of privacy approaches. apprenticeship.

As the implementation of LGPD is still in the preliminary stages in Brazil, we intend to find out how professionals who have already received training or work with this law,

make decisions related to privacy. We selected finance professionals because they were the first to consider implementing LGPD in their organizations.

The research question of this article is "How does privacy interfere in the decision-making of professionals trained in the LGPD and other factors relevant to the decision to disclose data?".

The focus of this research is to contextualize how finance professionals who are aware of the LGPD make their decisions related to privacy and other factors relevant to the data disclosure decision through the theoretical lens of privacy calculation.

As the disclosed data gains in personal importance, the perceived risk will increase, and subjects will choose less to publish data (Malhotra et al., 2004).

This study highlights the supplementary modifications implemented in the LGPD concerning data security in relation to the perceived privacy of the data. The decision to focus on perceived risk rather than actual risk stems from the fact that, in the privacy calculation, the genuine risk associated with a situation or decision is disregarded. To ensure practical decision-making, individuals typically rely on their own risk perception pertaining to existing risks (Kruthoff, 2018; Khalil & Karam, 2015).

2. Literature Review

2.1. Privacy

Understanding the value that individuals place on protecting their personal data is significant to businesses, the legal community, and policymakers. It is important for companies because, by estimating how much customers value protecting their personal data, managers can predict which privacy-enhancing initiatives could become sources of competitive advantage and which invasive initiatives could trigger adverse reactions (Acquisti et al., 2013).

Thus, privacy can be seen as a process of boundary control in which a person is aware of their rights and obligations with specific individuals. will occur, and how much and what type of interaction will occur (Pedersen, 1997).

Boundary control involves restricting and seeking interaction to achieve a desired degree of access to oneself (or the group) by others at a given time and in each set of circumstances. A person is not always successful in getting the preferred amount of interaction. Too much or too little interaction compared to the desired optimum is unsatisfactory. Too much is experienced as an invasion of privacy, and too little produces loneliness and alienation. Thus, the privacy regulation process is salient for the person (Pedersen, 1997).

Several types of personal privacy behaviors participate in order to achieve a desired degree of access to personal information or the group as a whole. Six types of privacy have been observed through empirical research - Loneliness, Isolation, Anonymity, Reserve, Intimacy with Friends, and Intimacy with Family (Pedersen, 1997).

The ideas of privacy are tied to specific situations

 DOI: 10.5709/ce.1897-9254.572

in real life. These situations are categorized as having a three-part composition: self, environmental, and interpersonal.

Combining time dynamics with developmental and socio-historical approaches, this situational analysis facilitates the understanding of individual's perceptions of privacy and the violation of privacy, it predicts the potential consequences of lack of privacy, and it describes the process of developing privacy, specific information about privacy experiences (Laufer & Wolfe, 1977).

The self-ego dimension refers to a developmental process that, in our society, focuses on individuation (autonomy) and, by implication, on personal dignity (Laufer & Wolfe, 1977).

The environmental dimension is composed of a series of elements that function as limits of meaning and experience. The elements of the environmental dimension are cultural meanings, the interaction between social arrangements and physical environments and the stage of the life cycle (Laufer & Wolfe, 1977).

The individual concept of privacy rights and rules, reflective and reflected by the environmental dimension and evolving and being fed back into the self-ego dimension,

is played out on a daily basis in the interpersonal dimension of certain situations. Although often equated with the "loneliness" of an individual or group, privacy remains an interpersonal concept. Privacy, in whatever form, presupposes the existence of others and the possibility of a relationship with them (Laufer & Wolfe, 1977).

2.2. Privacy by Design (PBD)

Cavoukian (2010) argues that there is a growing recognition that innovation, creativity and competitiveness need to be viewed from a design thinking perspective, i.e., inspired simultaneously. Data protection must also be viewed through the same design thinking lens.

Data protection must be built into network data systems and technologies by default. Data protection must become an integral part of organizational priorities, project goals, design processes, and planning procedures. Data protection must be built into all standards, protocols and processes that affect our lives. This document aims to achieve the strongest data protection in modern times by striving to create a common framework (Cavoukian, 2010).

Privacy by design guidelines define the privacy parameters followed by website and system developers (Barth et al., 2023). The implementation of the general data protection law in Brazil has changed the way software development teams implement their activities. Because of this, developers have had to get used to the present methods and tools for determining privacy requirements (Canedo et al., 2022).

PbD is supplementary to all computerized systems for information processing that have a personal data component. It should be essential to the provision of products and services to third parties and individual customers, such as social networks, search engines and Wi-Fi equipment (Schaar, 2010).

PbD consists of a set of principles that can be applied early in system development to address privacy concerns and achieve privacy compliance. However, these principles remain ambiguous, leaving questions unanswered regarding their application to systems engineering (Gürses et al.,2011).

Cavoukian (2010) presents the following guiding principles:

1. Proactive and not reactive; preventive and not corrective.
2. Privacy by default.
3. Privacy built into the design.
4. Full functionality: positive sum and non-zero sum.
5. End-to-end security: protection throughout the life cycle.
6. Visibility and transparency.
7. Respect for user privacy.

Spiekermann (2012) adds that with PbD, more challenges must be overcome:

- Privacy is a decentralized concept and thus difficult to protect. We have to agree on what we want to protect. Furthermore, data protection is often confused with security in concept and approach. We must begin to differentiate between safety and privacy in order to understand what

concerns must be addressed and how to address them.

• No agreed methodology supports systematic privacy engineering into systems. The system development life cycle rarely considers privacy issues.

• Little information is known about the practical and theoretical benefits and risks associated with companies' privacy policies.

2.3. Brazilian General Personal Data Protection

In 2018, privacy calls led to the implementation of Europe's General Data Protection Regulation (GDPR). Due to European influences, GDPR exported European data protection standards as the Brazilian Data Protection Law (LGPD) integrated in 2020 (Gadoni, 2023).

The Government of Brazil (2020) describes the process of personal data processing as occurring in two separate entities, the controller and the operator:

• The definition of the controller is derived from the law, which describes the natural or legal individual, under public or private jurisdiction, which is responsible for the processing of personal data (art. 5, VI). Within the scope of Public Administration, the Controller will be the legal entity of the public body or entity subject to the Law, represented by the authority responsible for adopting decisions regarding the treatment of such data.

• The Operator is the natural or legal individual, under civil or criminal law, this enables the processing of personal data on behalf of the controller (Article 5, VII), including public agents in the broad sense who perform such a function, as well as persons legal entities other than the one represented by the Controller, which carry out treatment activities within the scope of a contract or similar instrument.

In addition to the "treatment agents", another essential figure for the proper compliance with the LGPD is the "In charge", defined by art. 5, VIII, as the individual chosen by the controller and operator to serve as a form of information exchange between the National Data Protection Authority (ANPD), data subjects, controller and the (Government of Brazil, 2020).

Another fundamental concept is that of "data processing", which covers any activity that uses personal data in the execution of its operation, such as: production , collection, classification, receipt, access, use, transmission, archiving, reproduction, distribution, processing, storage, disposal, utilization or control, modification, communication, transmission, dissemination or extraction of information (Government of Brazil, 2020).

The LGPD also establishes, in its art. 6, that the processing of personal data must observe good faith and ten specific fundamental principles (Government of Brazil, 2020). They are:

Purpose: conducting the procedure for legal, specific, obvious and informed purposes to the owner, without the capacity to further process in a way that is in opposition to these goals.

Adequacy: the procedure is relevant and promotes the goals of the data subject, in accordance with the context of the procedure.

Need: The treatment must be confined to the minimum practical to achieve its goals, with the coverage of the relevant, proportional, and not overzealous data in relation to the objectives of the data processing.

Free access: this facilitates access to the data subjects' personal information and allows them to have free and easy access to the information regarding the treatment's duration and completeness, as well as the integrality of their personal information.

Data quality: assurance of the data subjects that the data is accurate, relevant, and up to date, as necessary, for the purpose of its treatment.

Openness: assurance to the owners that the information is clear, accurate and easily accessible regarding the execution of the treatment and the respective agents who perform it, while observing commercial and industrial secrets.

Safety: the use of technical and administrative safeguards that prevent personal data from being accessed without authorization and from being destroyed, lost, changed, or disseminated in an unlawful way.

Prevention: taking steps to prevent the damage caused by the processing of personal data.

Non-Discrimination: the inability to execute the treatment for illegal or aggressive purposes that are discriminatory; and

Accountability and the rendering of accounts, demonstrated by the agent, is the adoption of effective measures that can be proven to have been followed by the safeguarding of personal information, and the agent's effectiveness in doing so.

2.4. Privacy Calculation

Laufer & Wolfe (1977) coined the term "behavior computation" to refer to the cognitive process that underlies people's disclosure decisions.

The privacy calculation is processed as a trade-off between risk and benefit and the psychological process behind this communication is seen as a conscious and rational decision-making process (Knijnenburg et al., 2017).

Larsen & Eargle (2015) described the theory of privacy calculation, which is also known as behavior calculation, as an approach that involves individuals in considering their future actions. From an economic perspective, this implies that the associated costs and benefits are significant. In the context of privacy, the cost of specific dangers can be associated with disclosing information. As a result, individuals participate in an independent analysis of risk and benefit when faced with the transmission of personal information.

Some individuals believe that perceived privacy risks are the potential for the recipient to act opportunistically when they reveal their personal information, this can lead to a loss of control. This can be conceptualized as the secondary use of (personal) information (e.g., the sale or disclosing of personal information with other parties), illegal access and theft. The concept of Privacy Calculation is typically combined with other theories to describe the trade-off between risk and reward (Larsen & Eargle, 2015).

Figure 1 presents the diagrammatic representation of the privacy calculation theory. In this research, we use Kruthoff's (2018) model, which is based on the privacy calculation theory, Figure 2.

According to Kruthoff (2018), the underlying assumption of the represented model is that people are aware of the risk of disclosing personal data to third parties. If they are not aware of the risk, the decision is not based on privacy calculations, but on other random factors, making this research obsolete. Therefore, this model describes a positive relationship between inherent and managed risk in relation to an individual's perceived risk. Therefore, increasing manipulated and inherent risk increases the perceived risk of the subject. If the security of a system increases, the inherent risk decreases and therefore the perceived risk also decreases.

According with Kruthoff (2018), if the individual is more knowledgeable about privacy and is better at-risk management, the managed risk decreases and, consequently, the perceived risk decreases. Perceived risk is inversely proportional to the decision to disclose data, that is, a considerable risk will lead to a low propensity to relinquish personal information. The expected benefits are positively associated with the decision to release data, as it causes people to be more eager to take risk.

2.5. Hypotheses

The considerations have led the authors to propose six hypotheses that will be empirically tested in the remainder of the study. Each of the hypotheses presented is directly derived from the individual hypotheses that were formulated.

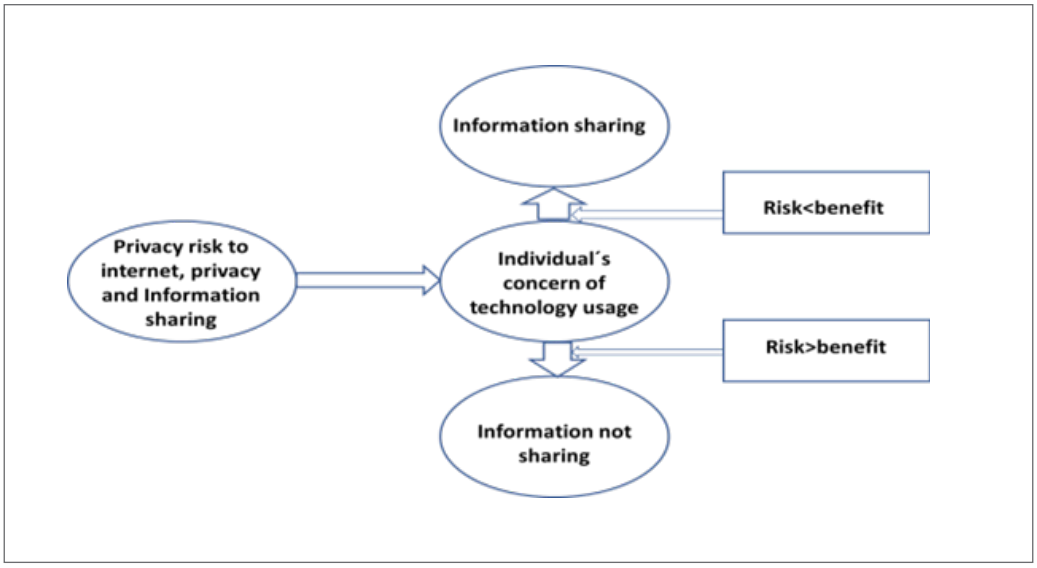
H1: People realize that their personal data is important.

This hypothesis stems from the basic requirement for people to perceive their data as important or valuable in order to make an informed decision about the privacy calculation (Kruthoff', 2018).

Privacy is equally important in regard to data security and data protection is primarily comprised of various laws, regulations and procedures that are intended to preserve the data and reduce the intrusion into personal privacy (Srivastava & Geethakumari, 2013).

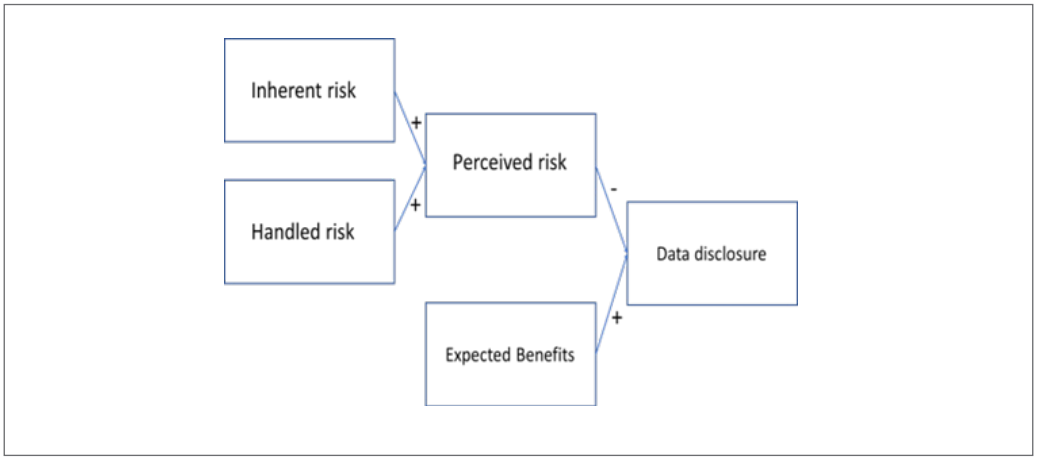
If they do not perceive their data as important, they would not associate any risk to the disclosure of personal data, making the application of the privacy calculation theory obsolete. This is used as a baseline to recognize outliers and see if the privacy calculation theory applies to the number of respondents. If this condition is not met, survey

Figure 1
Theory of Privacy Calculation



Source: Larsen & Eargle (2015)

Figure 2
Correlation Between Privacy Calculation Factors



Source: Kruthoff (2018)

 DOI: 10.5709/ce.1897-9254.572

responses are not based on privacy calculation (Kruthoff', 2018).

H2: People trust financial institutions more than commercial companies.

Institutional trust plays a prominent role as a mitigating factor in risk perception, which from a financial perspective (Kruthoff', 2018), this implies that the associated costs and benefits are significant. In the context of privacy, the expense of specific dangers can be connected to releasing information. As such, individuals participate in an independent assessment of the risk and benefit associated with personal information transmission (Larsen & Eargle, 2015) .

In Kruthoff's theory (2018), if the security of a system increases, the inherent risk decreases and, therefore, the perceived risk also decreases. The most significant trust is also measured at the baseline, comparing trust in companies and banks.

H3: People facing a more serious condition are more likely to disclose personal data than people facing a lesser condition.

The theory suggests that individuals' intentions to disclose information are based on behavioral calculations that weigh potential competing factors against possible outcomes (Li, 2012).

A popular form of behavioral accounting is risk-return analysis, which considers the trade-offs between expected risks and expected benefits in the context of a particular disclosure (Li, 2012).

To evaluate the hypothesis, we use the comparison of t-test results between heavy and light quality in each different scenario.

H4: When presenting the LGPD, people are more likely to disclose personal data.

The introduction of the LGPD lessens the level of risk inherent in the system itself by introducing privacy by design. Reducing inherent risk would lead to a less risky perception of another party who owns the data, resulting in less concern when disclosing the data.

LGPD talks about the processing of personal data in physical or digital media that is provided by individuals or legal entities in accordance with public or private law, this includes various actions that can be undertaken manually or digitally (Government of Brazil, 2018).

According with Kruthoff (2018), if the individual is more knowledgeable about privacy and is better at-risk management, the managed risk decreases and, consequently, the perceived risk decreases

To say whether we support this hypothesis, pairing the light financial needs in the baseline and LGPD scenario and pairing the financial needs in the same way. If we notice a significant disparity between the samples, we recognize the hypothesis as true.

H5: When providing a choice of whether or not to participate in a decision, people are more likely to disclose personal data.

The LGPD provides that personal data will be deleted after the end of its treatment, within the scope and technical limits of activities (Government of Brazil, 2018).

Deletion represents a decrease in risk administered in the context of the privacy calculation decision. By giving a chance to withdraw from data storage, people will feel that the decision made is less risky and should subsequently lead to higher disclosure behavior (Kruthoff, 2018).

As done in the previous hypothesis, the method consists of pairing the light financial needs in each scenario and separately and then looking at the results if we can find a significant difference in the two distributions.

H6: When it is suggested that disclosing more data with the bank will lead to a higher level of service, people are more likely to disclose the data.

Suggesting that disclosing more data with the bank will result in better care increases the benefits of taking that risk. For this increase, people should be more inclined to release data.

Some individuals believe that the potential for perceived privacy risks is the recipient to act opportunistically when they disclose their personal information, this can lead to a loss of control (Larsen & Earle, 2015).

Again, we evaluated this hypothesis by separately comparing light and heavy financial needs in each scenario.

3. Methodology

The scientific methods used in the research include data collection through questionnaires and

statistical analysis using paired t-tests to evaluate differences in levels of perceived risk and quality of care in different financial scenarios.

The research was designed to measure the causal relationships of the privacy calculation applied to the financial field; the survey is measuring the perceived risk and the expected quality of care. Perceived risk is divided into inherent risk and system managed risk. On the other hand, the expected quality of care is measured. First, a baseline of intent to disclose data is made, which means that, under no external conditions, what kind of data would be disclosed by the respondent.

The dependent variable is the actual decision to reveal an amount of data and is measured at 4 distinct levels. These levels range from not disclosing any data to disclosing data only to the finance team responsible for financial services. The next level would be to grant the financial team complete authority to act on the client's behalf., passing the information on to other finance experts. The fourth level is not only giving the finance team full authority over personal data, but also providing consent to store the data so that it can be used in longitudinal studies to improve financial services. The four levels represent distinct levels of difficulty of data disclosure on an ordinal scale and function as a slider, where each additional step is granted more access to the data.

Research data were collected from July 14 to July 22, 2021, through google forms, 17 questions were prepared. The database used is composed of 103 respondents who are part of the team that implements LGPD in their organizations. First, a baseline of perceived risk is measured in relation to data handling by companies and personal assessment of data. The baseline is measured on a 5-scale Likert that ranges from "strongly disagree" to "strongly agree". In further analysis, a score of 1 corresponds to the "strongly disagree" answer and a score of 5 corresponds to the "strongly agree" answer. The six concepts we measure are perception, whether personal data is private or essential to the data subject.

Next, we asked about trust in companies in general. Subsequently, we ask for trust in financial institutions specifically and if there is trust in banks not to take advantage of personal data. It then asks whether financial incentives could persuade them to disclose their data. The seventh question is an inverted variable, meaning it is a question to see if the basic questions have been answered consistently.

This baseline is essential for measuring, for explaining the possible variation between subjects' responses. Furthermore, it is important in privacy calculus theory to realize the level of risk involved in order to make an informed decision about data disclosure. If people do not see the risk in disclosing the data, as mentioned earlier, they do not make a privacy calculation decision and as a result, the aforementioned hypotheses are not pertinent to this investigation. To make relevant assumptions about the correlation and relationships between, we need more than 100 respondents (Blumberg et al., 2014).

Otherwise, tests like the t test do not give us any meaningful answers about the difference between two variables, because the means and ranges would be too imprecise. After that, we expose the participants to situations they might encounter. These situations include a change in only one perceived risk or expected quality of care, since, in the event of a change in more than one variable, it is not possible to identify the cause of the alteration of the dependent variable to one of the independent variables exactly. In the first situation, participants are presented with a small financial problem, needing a small amount of money.

In this situation, it is measured by what types of the information they are prepared to disclose. The second situation involves a larger and more important financial amount, for example borrowing a large amount of money, and again, the level of disclosure is measured. Basic conditions are changed to check for differences in data disclosure with respect to different financial scenarios.

Risk is divided into inherent risk and managed risk. Participants will be presented with the situation to choose or not to disclose the data, representing the ability to deal with risk. In the following question, participants are informed about the new LGPD regulation and the following improvements for data security within the system. Then again, the

Table 1
Means of Baseline Measure

	n	mean	median	Standard deviation	Minimum	maximum
importance data	103	4.98	5	0.14	4	5
private data	103	4.88	5	0.43	2	5
trust in companies	103	2.19	2	0.97	1	5
trust in banks	103	2.87	3	1.2	1	5
trust in professionals	103	2.24	2	1.04	1	5
trust more in banks	103	3.11	3	1.21	1	5
financial incentives	103	2.69	3	1.43	1	5
light financial scenario	103	2.95	3	1.26	1	5
heavy financial scenario	103	3.26	3	1.32	1	5

Table 2
Descriptive Statistics

	n	mean	median	Standard deviation	Minimum	maximum	skewness
Basic_light	103	2.95	5	1.26	1	5	0.12
basic_heavy	103	3.26	5	1.32	1	5	-0.24
LGPD_light	103	3.29	2	1.18	1	5	-0.29
LGPD_heavy	103	3.34	3	1.2	1	5	-0.34
OPT_light	103	3.31	2	1.2	1	5	-0.24
OPT_heavy	103	3.4	3	1.17	1	5	-0.41
Quality_light	103	2.95	3	1.21	1	5	-0.18
Quality_heavy	103	3.12	3	1.22	1	5	-0.23

Table 3
Paired Sample T-Test for Basic-Heavy Conditions

	Paired Differences			*t*	*df*	*sig*
	mean	95% Confidential Interval				
		Lower	Higher			
Pair 1 Basic_light Basic_heavy	-0.3106796	-0.54773095	-0.07362827	-2.59	103	0.01072
Pair 2 LGPD_light - LGPD_heavy	-0.04854369	-0.199382	0.1022946	-0.64	103	0.5247
Pair 3 OPT_light - OPT_heavy	-0.08737864	-0.21605251	0.04129523	-1.35	103	0.181
Par 4 Quality_light - Quality_heavy	-0.1650485	-0.29657287	-0.03352422	-2.49	103	0.01443

Table 4
Paired Sample T-Test for Basic-Scenario Conditions

	Paired Differences			*t*	*df*	*sig*
	mean	95% Confidential Interval				
		Lower	Higher			
Pair 1 Basic_light Basic_heavy	-0.3398058	-0.61423220	-0.06537945	-2,456	103	0.01574
Pair 2 LGPD_light - LGPD_heavy	-0.3592233	-0.65757948	-0.06086712	-2.3881	103	0.01877
Pair 3 OPT_light - OPT_heavy	0	-0.2581799	0.2581799	0	103	1
Par 4 Quality_light - Quality_heavy	-0.0776699	-0.3495407	-0.3495407	-0.5666	103	0.5722
Pair 5 Basic_heavy – OPT_heavy	-0.1359223	-0.4407282	0.1688835	-0.8845	103	0.3785
Pair 6 Basic_heavy – Quality_heavy	0.1456311	-0.09977001	0.39103215	1.1771	103	0.2419

kind of data they are willing to release is measured.

Improving data security through the LGPD represents the inherent risk of the system. Both factors are expected to increase willingness to disclose information about themselves. The third situation presented to the respondents is the quality of service that is projected to be funded by the financial institution, which means that disclosing data means better service. Again, more data is expected to be released in the event of a more financially critical scenario.

As all questions are measured on an ordinal scale, the data will be analyzed using paired t tests. With a t test, you can verify that the pairs of responses are significantly different from one another. A t test does this by comparing the null hypothesis that there is no association between these two populations. The significance level chosen in this study was 5% two-tailed to reject the null hypothesis, which implies that there is a relationship between the samples and that this difference can be explained by changes in the correlated variables (Kruthoff', 2018).

4. Results and Analysis

A total of 103 responses were gathered from professionals engaged in the field of LGPD, including consultants, lawyers, IT specialists, and others. The majority of the respondents (96.11%) hold a higher education degree, while 75% possess a postgraduate qualification. In terms of age distribution, a considerable proportion (92.23%) falls within the range of 31 to 60 years old, 6.8% are aged between 21 and 30, and 0.97% have a mean age of 61 years, or older. Table 1 presents the statistics of the first part of the survey.

Respondents considered that their data is important and should be kept private, with a mean of 4.98 and 4.88. They also expressed that they trust banks more (mean of 2.87) than companies in general (mean of 2.19) for handling personal data and the question directly asked to respondents if they trust banks more for storage data (mean of 3.11) than in companies supports the claim that people answered the questions consistently and not randomly, but the degree of confidence drops in relation to banking professionals (mean of 2.24). Respondents are unwilling to disclose personal data due to financial incentives (mean of 2.69), but when the financial scenario becomes more complicated, requiring greater financial resources, respondents considered providing more personal data, a mean of 3.26 in heavy financial scenarios versus 2.95 in light financial scenarios.

 DOI: 10.5709/ce.1897-9254.572

It was found that we can use the t test, because in Table 2, the asymmetry values are within the chosen range of 1 and -1, verifying the normality of the variables. Thus, we can assume that the data are normally distributed, and we can utilize the t test to assess the significance of the discrepancy in variables.

Paired t tests were applied in different scenarios to see if responses to different conditions vary according to the type of financial problem. The t test evaluates the difference of means clustered around the variance of a distribution and shows whether the assumption that two distributions are not equal is correct.

The results in Table 3 showed that, in the comparison of light and heavy financial scenarios, there is a negative and significant difference at the level of 5%, this explains that respondents tend to disclose more data when they face a more serious financial scenario. This phenomenon is repeated in pair 4, when we emphasize the seriousness of the financial problem, that is, the interviewee needs more money in the heavy scenario than in the light one.

In these two cases the p-values (0.01072 and 0.01443) are less than the significance level alpha = 0.05, and we can then reject the null hypothesis in each situation and conclude that the distribution of responses is not the same. In the other situations (pairs 2 and 3), the p-values are greater than 0.05, so we do not reject the null hypothesis, that is, the difference between the light and heavy scenarios is not significant.

Table 4 shows the results of the paired t test for alternative scenarios, there are two pairs with significance of distributions compared between the light and heavy financial scenarios and the disclosure of personal data. The first scenario is when the financial scenario is light and the LGPD is in force and banks are required to improve security and personal data processing procedures and the second scenario occurs when the financial scenario is light and there is an option to withdraw from the decision to disclose data. The remaining tests fail to reject the null hypothesis at the chosen 5% significance level.

Regarding the hypotheses:

H1: People realize that their personal data is important.

In the answers of the interviewees, it can be seen that they agree with the statement that their data are private and important, where we obtained the highest means of the answers. In this way, the answers to the remaining questions can be based on the underlying assumptions made to decide whether or not to disclose the data is based on the privacy calculation framework.

H2: People trust financial institutions more than commercial companies.

Respondents pointed out that they trust banks more than companies in general, the mean of trust in banks was higher than trust in companies (Mean of Trust in banks: 2.87; mean of Trust in Companies: 2.19). The question asked directly to respondents whether they trust banks more for data storage (mean of 3.11) than companies support the claim that people answered the questions consistently and not randomly.

H3: People facing a more serious condition are more likely to disclose personal data than people facing a lesser condition.

In the comparison of light and heavy financial scenarios, there is a negative and significant difference at the level of 5%, this explains that respondents tend to disclose more data when facing a more serious financial scenario. This phenomenon is repeated in pair 4, when we emphasize the seriousness of the financial problem, that is, the interviewee needs more money in the heavy scenario than in the light one.

H4: When presenting the LGPD, people are more likely to disclose personal data. Based on the t-tests made in the analysis, we were unable to confirm the hypothesis,

as only the par when the financial scenario is light and the LGPD is in place and banks are required to improve security and personal data processing procedures can be proven to be significant at the 5% level, but also within the 95% confidence interval. So, based on the research, we can conclude that the LGPD and later the inherent risk has a significant impact on people's disclosure behavior.

H5: When someone gives you the option of choosing between two options, the likelihood that

you will disclose personal information increases.

The t test when comparing the baseline scenario and given the opt-out gives us the conclusion that the choice to opt-out has a considerable influence on the decision to disclose the information. This means that the risk addressed has a considerable influence in the context of privacy calculation and data disclosure.

H6: When it is suggested that disclosing more data with the bank will lead to a higher level of service, people are more likely to disclose the data.

The paired t test shows that the differences in distributions in the light and heavy financial scenarios are not significant at a 5% level. This shows that there would be no risky behavior.

Hypotheses proved to be true to a significant degree, but in relation to personal data, as they consider it important and private, they are cautious and are not willing to trust and disclose their data with all types of companies, even if there is LGPD, which has a financial benefit or a financially unfavorable situation. Respondents are not willing to exchange their private data to obtain advantages in trusted companies such as banks.

5. Conclusions

According to the results and discussions presented, the objective of the article was achieved as several significant contributions to the theory of privacy calculation and its application in the implementation of the LGPD in the Brazilian financial sector were highlighted.

The results demonstrate that individuals believe that their personal data is meaningful and personal. This understanding is in line with the theory of Malhotra et al. (2004), who state that as the personal value of data increases, the perceived risk also increases, as a result, individuals become more hesitant to disclose their data.

Respondents demonstrated a greater degree of trust in financial institutions than in other companies. This trust reduces the perceived risk which is discussed by Kruthoff (2018), system security reduces the inherent risk and, consequently, the perceived risk.

Studies have shown that individuals are more inclined to share personal information when financial situations are more serious. This conduct is in line with the calculus theory of privacy, which involves carrying out a separate risk and benefit analysis (Larsen and Eargle, 2015).

Despite the introduction of the LGPD which decreased inherent risk while increasing perceived security, the results were not definitive with regards to the assertion that people are more inclined to share personal information just because of the presence of the LGPD. This finding implies that, in addition to legislation, other environmental and individual components of the environment also influence privacy decisions.

The ability to opt out of storing data had a significant impact on the decision to disclose personal information. This finding is in line with research suggesting that having control over data can reduce perceived disease risk and increase desire to share (Kruthoff, 2018).

The theory that betters quality service leads to greater willingness to share information has not been significantly disregarded. This result implies that, despite the obvious benefits, individuals still have a certain degree of caution when disclosing personal information, which is attributed to a complexity in privacy decisions that goes beyond the simple risk-benefit comparison.

These findings reinforce the importance of understanding individual risk perception and trust in institutions when formulating privacy policies and LGPD compliance strategies. The study contributes to the literature by applying privacy calculus theory in a new and relevant context, providing practical insights for companies and policymakers in Brazil.

References

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth? *The Journal of Legal Studies, 42*(2), 249–274. https://doi.org/10.1086/671754

Barth, S., Ionita, D., & Hartel, P. (2023). Understanding online privacy—A systematic review of privacy visualizations and privacy by design guidelines. *ACM Computing Surveys, 55*(3), 1–37. https://doi.org/10.1145/3502288

Blumberg, B., Cooper, D., & Schindler, P. (2014). *EBOOK: business research methods*. McGraw Hill.

Government of Brazil. (2018). *Brazilian general data protection law (LGPD).* https://www.gov.br/cidada-

nia/pt-br/acesso-a-informacao/lgpd

Government of Brazil. (2020). *Good practices guide – Brazilian general data protection law (LGPD)*. https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guia-boas-praticas-lgpd

Canedo, E. D., Calazans, A. T. S., Bandeira, I. N., Costa, P. H. T., & Masson, E. T. S. (2022). Guidelines adopted by agile teams in privacy requirements elicitation after the Brazilian general data protection law (LGPD) implementation. *Requirements Engineering*. https://doi.org/10.1007/s00766-022-00391-7

Cavoukian, A. (2010). *The 7 foundational principles: Implementation and mapping of fair information practices*. https://gpsbydesign.org/the-7-foundational-princides-implementation-and-ma-pping-of-fair-information-practices

Gadoni C., R. (2023). The effects on local innovation arising from replicating the GDPR into the Brazilian General Data Protection Law. *Internet Policy Review, 12*(1). https://doi.org/10.14763/2023.1.1686

Gürses, S., Troncoso, C., & Diaz, C. (2011). Engineering privacy by design. *Computers, Privacy & Data Protection, 14*(3), 25.

Khalil, L., & Karam, N. A. (2015). Security management: real versus perceived risk of commercial exploitation of social media personal data. *Procedia Computer Science, 65*, 304–313. https://doi.org/10.1016/j.procs.2015.09.087

Knijnenburg, B., Raybourn, E., Cherry, D., Wilkinson, D., Sivakumar, S., & Sloan, H. (2017). Death to the privacy calculus? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2923806

Kruthoff, S. (2018). *Privacy calculus in the context of the general data protection regulation and healthcare: a quantitative study* (Bachelor's thesis). University of Twente.

Larsen, K. R., Allen, G., Vance, A., & Eargle, D. (2015). *Theories used in IS research wiki*. Retrieved September 22, 2025.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues, 33*(3), 22–42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems, 54*(1), 471–481. https://doi.org/10.1016/j.dss.2012.06.010

Loch, J. de A. (2003). Confidentiality: Nature, Characteristics, and Limitations in the Context of the Clinical Relationship. *Revista Bioética, 11*(1).

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Muncinelli, G., de Lima, E. P., Cestari, J. M. A., Deschamps, F., & da Costa, S. E. G. (2021). Developing a conceptual model for process capability in the Brazilian data protection regulation context. *Journal of Industrial Integration and Management, 6*(04), 407–427. https://doi.org/10.1142/S2424862221400017

Pedersen, D. M. (1997). Psychological functions of privacy. *Journal of Environmental Psychology, 17*(2), 147–156. https://doi.org/10.1006/jevp.1997.0049

Schaar, P. (2010). Privacy by design. *Identity in the information society, 3*(2), 267–274. https://doi.org/10.1007/s12394-010-0055-x

Spiekermann, S. (2012). The challenges of privacy by design. *Communications of the ACM, 55*(7), 38–40. https://doi.org/10.1145/2209249.2209263

Wiśniewski, R., Oleksiuk, I., & Iwanowska, B. (2021). Privacy of European citizens in the face of the development of new data-driven business models. *Contemporary Economics, 15*(4), 442–456. https://doi.org/10.5709/ce.1897-9254.459