# GDPR APPLICATION ANALYSIS IN A PUBLIC EDUCATIONAL INSTITUTION: A CASE STUDY

# ANÁLISE DE APLICAÇÃO DA LGPD NUMA INSTITUIÇÃO PÚBLICA DE ENSINO: UM ESTUDO DE CASO

# *ANÁLISIS DE APLICACIÓN DE LA LGPD EN UNA INSTITUCIÓN EDUCATIVA PÚBLICA: UN ESTUDIO DE CASO*

Jackson Gomes Soares SOUZA[1]
Francisco Rolfsen BELDA[2]
Carlos Hideo ARIMA[3]

**ABSTRACT**: The intensification of data collection, storage and processing by institutions calls attention to personal data protection. This basic applied research aims to verify, through a case study, the compliance between a public institution of technological education's data protection regulation instruments and the addressed by the General Data Protection Law (GDPR). The answers were collected by a structured questionnaire, being subsequently tabulated and processed. The results demonstrate the relationship between the institutional context and dimensions analyzed for the implementation of protocols, good practices and a privacy governance program that meets institutional policies.

**KEYWORDS**: General Data Protection Regulation. GDPR. Learning environments.

***RESUMO**: A intensificação na coleta, armazenamento e tratamento de dados pelas instituições traz atenção quanto à proteção de dados pessoais. Esta pesquisa básica aplicada visa verificar, por meio de um estudo de caso, a conformidade entre instrumentos normativos de proteção de dados pessoais adotados por instituição pública de ensino tecnológico e o estabelecido pela Lei Geral de Proteção de Dados Pessoais (LGPD). As respostas coletadas pelo questionário estruturado foram tabuladas e tratadas, demonstrando a relação entre contexto institucional e as dimensões analisadas para a implementação de protocolos e das boas práticas. Conforme os resultados, considera-se a necessidade de implementação de um programa de governança em privacidade que vá ao encontro das políticas institucionais.*

***PALAVRAS-CHAVE**: Lei Geral de Proteção de Dados Pessoais. LGPD. Ambientes para ensino.*

[1] Federal Institute of Education, Science and Technology of São Paulo (IFSP), Campinas – SP – Brazil. Teacher. Doctoral Student in School Education (UNESP). ORCID: https://orcid.org/0000-0003-4952-8618. E-mail: jackson@ifsp.edu.br

[2] São Paulo State University (UNESP), Bauru – SP – Brazil. Professor at the Department of Social Communication. PhD in Production Engineering (EESC-USP). ORCID: https://orcid.org/0000-0001-6350-7026. E-mail: belda@faac.unesp.br

[3] Paula Souza State Technological Education Center (CEETEPS), São Paulo – SP – Brazil. Professor of the Professional Master's Program in Management and Technology in Productive Systems and Researcher at the Graduate, Extension and Research Unit of the Paula Souza Center. Doctorate in Controllership and Accounting (USP). ORCID: https://orcid.org/0000-0001-7922-0943. E-mail: charima@uol.com.br

***RESUMEN**: La intensificación en la recolección, almacenamiento y procesamiento de datos por las instituciones llama la atención acerca de la protección de datos personales. Esta investigación básica aplicada tiene como objetivo verificar, por un estudio de caso, la conformidad entre los instrumentos normativos de protección de datos personales adoptados por una institución de educación tecnológica pública y el establecido por la Ley General de Protección de Datos (LGPD). Las respuestas obtenidas a partir de un cuestionario estructurado fueron tabuladas y procesadas, evidenciando la relación entre el contexto institucional y las dimensiones analizadas para la implementación de protocolos y buenas prácticas. De acuerdo con los resultados, se considera la necesidad de implementar un programa de gobernanza y privacidad que cumpla con las políticas institucionales.*

***PALABRAS CLAVE**: Ley General de Protección de Datos Personales. LGPD. Ambientes de enseñanza.*

## Introduction

According to Davenport (1998, p. 18), "data are simple observations about the state of the world" and have as characteristics to be: "easily structured, obtained by machines, often quantified and easily transferable", while information would be a set of "data endowed with relevance and purpose", requiring "unit of analysis, consensus in relation to the meaning and, necessarily, human mediation". Such mediation may present itself by the "interaction between humans and the systems, bringing with it concepts such as information security and privacy involved in this process" (SOUZA; ARIMA; BELDA, 2020, p. 1310).

We are surrounded by diverse technologies, so the use of digital media for teaching and learning processes is directly related to the treatment of data stored and used by institutions, and they must adopt policies for the protection of personal data and information based on specific legislation.

The General Data Protection Law (GDPR), Law no. 13,709, of August 14, 2018 (BRAZIL, 2018):

> Provides for the processing of personal data, including in digital media, by natural persons or legal entities of public or private law, in order to protect the fundamental rights of freedom and privacy and the free development of the personality of the natural person.

With the enactment of Constitutional Amendment No. 115 (EC115), published on February 11, 2022 in Section 1, Issue 30, Page 2 of the Official Gazette of the Union, the Brazilian Federal Constitution of 1988 now contemplates the list of fundamental rights and guarantees of data protection, establishing the competence of the federative entities to legislate on the subject (BRAZIL, 2022).

Law No. 11.892, of December 29, 2008 (BRAZIL, 2008), among other provisions, establishes that:

> The Federal Institutes are multi-curricular and multi-campi institutions of higher, basic and professional education, specialized in offering professional and technological education in different modalities of education, based on the combination of technical and technological knowledge with their pedagogical practices, according to this Law.

In this sense, this research aims to study the normative instruments for personal data protection adopted in a public technological educational institution and current outcomes for the development of policies and procedures in one of its campuses.

## Theoretical Background

For Pierre Lévy (2014, p. 23), "we still do not know how to systematically transform data into knowledge", bringing the reflection regarding a "participatory digital memory, in the process of constitution, common to the whole of humanity in search of solving this problem of semantic interoperability".

In this sense, the author establishes a unity of nature founded on the notion of information, addressing a synthetic image of the informational nature and its scientific concept, conceiving the nature of information in successive layers: from quarks to atoms, from molecules to organisms, from nervous systems to phenomena, and from symbols to concepts (LÉVY, 2014). One possible interpretation would be that data would be equivalent to symbols, albeit unmodalized, but not meaningless.

On October 24, 1995, the European Parliament and the Council of the European Union published in the Official Journal No. L 281 of 23/11/1995, pages 31 to 50, the "Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data". (UNIÃO EUROPEIA, 1995).

Article 29 of Directive 95/46/EC established the creation of the advisory and independent "Working Party on the Protection of Individuals with regard to the Processing of Personal Data", the "Article 29 Working Party (WP29)". It also provides a definition of personal data, fragmenting it into 4 (four) pillars or main elements:

> [...]'any information', 'relating to', 'natural person', 'identified or identifiable'. The four pillars are closely related and support each other, together determining whether or not information will be considered personal data [...] (UNIÃO EUROPEIA, 2007, p. 6, emphasis added).

In Brazil, the GDPR besides bringing a similar definition of personal data, regulates in its 10 (ten) chapters:

> ‘General provisions'; 'processing of personal data'; 'data subject rights'; 'processing of personal data by public authorities'; 'international data transfer'; 'personal data controllers'; 'security and good practices'; 'supervision'; 'National Data Protection Authority (ANPD) and National Council for Personal Data Protection and Privacy' and 'final and transitory provisions'. (BRAZIL, 2018).

Article 6 of the GDPR establishes, among others, principles to be observed, so that the treatment policies adopted allow users to be aware of the ways in which their data will be used, making it possible to avoid or reduce the collection and use of their information by third parties. In order to apply the concepts, the main elements have been summarized in dimensions, as shown in Table 1.

**Table 1 –** Personal Data Protection Dimensions

1. **Foundations (FUN):** Concern with the "protection of personal data when processed, including in digital media, in order to protect the fundamental rights of freedom, privacy and the free development of the personality of the natural person". (BRAZIL, 2018, s/p [web]).
2. **Principles (PRI):** Meeting the principles of "purpose, appropriateness, necessity, open access, data quality, transparency, security, prevention, non-discrimination, accountability, and responsibility” (BRAZIL, 2018, s/p [web]).
3. **Processing of personal data (TRA):** "Any operation performed with personal data", being indispensable the consent of the data subject "in writing or by any other means demonstrating the expression of will" "free and unequivocal". (BRAZIL, 2018, s/p [web]).
4. **4. Rights of the data subject (DIR):** The right to "withdraw consent", "update", "anonymize", "block" or "delete" personal data to the data subject (BRAZIL, 2018, s/p [web]).

Source: Adapted by the authors based on the GDPR (BRAZIL, 2018)

Chapter 4 of the GDPR regulates the treatment by the public authorities, including making direct reference in the caput of Article 23 to Law No. 12,527 of November 18, 2011, also known as the Law of Access to Information (LAI), and must "[...] be carried out for the fulfillment of its public purpose, in pursuit of the public interest, with the aim of executing the legal powers or fulfilling the legal attributions of the public service” (BRAZIL, 2018).

Additionally, article 50 makes, in its three paragraphs, direct references to principles listed in article 6, such as purpose, quality, safety, prevention and accountability.

## Methodological Procedures

According to the classification of research made by political scientist Donald Stokes, this is basic-applied research, driven by investigative curiosity about particular phenomena, not necessarily aiming at "general explanatory goals nor any practical use to which its results are destined" (STOKES, 2005, p. 119).

According to Yin (2001, p. 11 and 47), the case study is an empirical inquiry focused "on contemporary phenomena inserted in some real-life context", having as a prerequisite the systematization of procedures through protocols.

This study covers the "Campinas campus linked to the Federal Institute of Education, Science and Technology of São Paulo – IFSP" and, as it is a single case study, the data collected and its consequent analysis will not allow the generalization of the results (BRAZIL, 2018). For data collection, a structured digital questionnaire on the Google Forms platform was adopted as an instrument. It also counts on the voluntary participation of 80 teachers and managers registered in the "Unified Public Administration System" (SUAP in the Portuguese acronym) of the campus, having collected a total of 15 responses.

According to Likert (1932), surveys involving statements of opinion and attitude are considered an indirect method of gauging dispositions that are more easily signified and expressed in verbal form, and can, consequently, be grouped into patterns. Therefore, the Likert scale will be used, in which the answers obtained show the degree of agreement of the participants with the sentence, contemplating levels from 1 to 5 of the scale, classified respectively as: "I completely disagree", "I disagree", "Neutral", "Agree" and "Completely Agree".

Regarding the investigation of the normative instruments adopted by the IFSP in compliance with the requirements addressed in the GDPR, the documentary research of this study includes the institution's Statute and the most recent Ordinances, which approve the Internal Regulations of the Digital Governance Committee and update the "Information and Communication Security Policy - PoSIC", as well as the "Personal Data Protection Policy" (BRAZIL, 2020).

## Data Analysis

The interpretation of the results will initially be from the following structure: PDP - Participants' Profile and CDI - Context of the institution.

Next, personal data protection dimensions will be investigated:

- FUN – Foundations of personal data protection;
- PRI – Principles of personal data protection;
- TRA – Processing of personal data;
- DIR – Rights of the personal data subject.

The sample has 15 collected answers. The profile of the participants is characterized according to age, education, time in the institution and whether the participant currently holds a management position, according to Table 2.

**Table 2 –** Participant Profile

| Professors | Age | Education | How long in the institution | Manager |
|---|---|---|---|---|
| **D1** | 30 - 39 | Master's | between 4 and 10 years | No |
| **D2** | 50 - 59 | Doctorate | between 4 and 10 years | No |
| **D3** | 30 - 39 | Master's | between 4 and 10 years | No |
| **D4** | 30 - 39 | Doctorate | between 10 and 20 years | No |
| **D5** | 50 - 59 | Doctorate | More than 20 years | Yes |
| **D6** | 40 - 49 | Doctorate | between 4 and 10 years | Yes |
| **D7** | 60 - 69 | Doctorate | between 4 and 10 years | No |
| **D8** | 50 - 59 | Master's | between 4 and 10 years | No |
| **D9** | 30 - 39 | Doctorate | between 4 and 10 years | Yes |
| **D10** | 40 - 49 | Doctorate | between 4 and 10 years | Yes |
| **D11** | 50 - 59 | Doctorate | between 4 and 10 years | No |
| **D12** | 50 - 59 | Doctorate | between 4 and 10 years | No |
| **D13** | 40 - 49 | Master's | between 4 and 10 years | No |
| **D14** | 30 - 39 | Master's | between 4 and 10 years | No |
| **D15** | 18 - 29 | Master's | between 4 and 10 years | No |

Source: Research results

The participant's profile changes according to their education, and it is observed that only two age brackets encompass 64% of the teachers, these being 30 to 39 years old and 50 to 59 years old; while in the first bracket the highest concentration is of master's degrees, in the second, most have doctorates.

The analysis of the context of the institution (CDI) covers the investigation of:

- CDI1 – Adoption of a sufficiently clarifying Information and Communications Security Policy (PoSIC) by the institution;
- CDI2 – Technical protection controls for stored personal data;
- CDI3 – Transparency and free access to stored personal data and information;

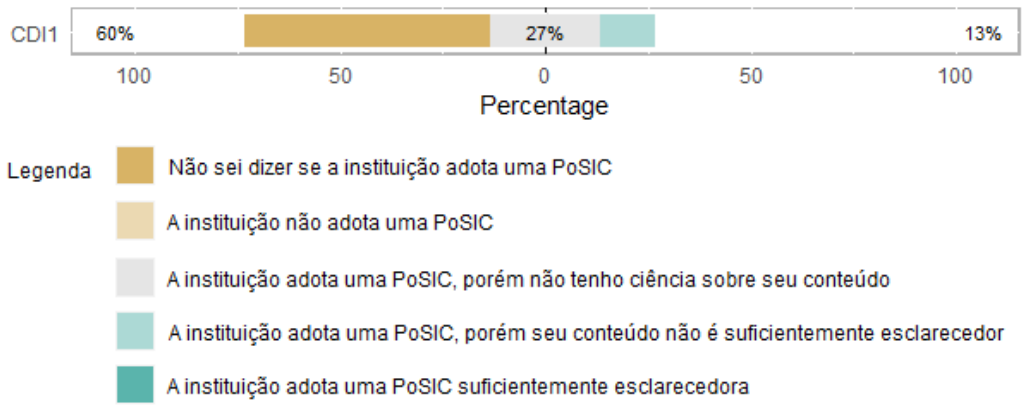
- CDI4 – Training or events that address privacy and protection of personal and operational data;
- CDI5 – Adoption of different authentication methods;
- CDI6 – Communication, via notices, about privacy and personal data protection;
- CDI7 – Information Security Awareness;
- CDI8 – Awareness about protection of confidential information in electronic format.

Initially, the awareness of the results regarding the adoption of a sufficiently clarifying Information and Communication Security Policy (PoSIC) by the institution, addressed by the element CDI1, will bring us evidence of possible neutral answers in the statements about the context of the institution.

As can also be seen in Figure 1, 40% of the participants agree that the institution adopts a PoSIC; however, 26.67% say they are not aware of its content, and 13.33%, that its content is not enlightening enough.

Despite 60% of the participants not being able to say whether the institution adopts a PoSIC, a premature inference of this phenomenon could call into question their level of familiarity with the topic in question. However, the participants add in their answers that 'in the institution the employees know little about the GDPR, and there are no institutional measures adopted for data protection, leaving it up to the good sense of the employee to protect the data', and also 'not having any knowledge about data protection in our institution'.

**Figure 1 –** Graphical representation of ICD1 responses[4]




Source: Research results

[4] Não sei dizer se a instituição adota uma PoSIC = I can't tell if the institution adopts a PoSIC; A instituição não adota uma PoSIC = The institution does not adopt a PoSIC; A instituição adota uma PoSIC, porém não tenho ciência sobre seu conteúdo = The institution adopts a PoSIC, but I am not aware of its content; A instituição adota uma PoSIC, porém seu conteúdo não é suficientemente esclarecedor = The institution adopts a PoSIC, but its content is not sufficiently clarifying; A instituição adota uma PoSIC suficientemente esclarecedora = The institution adopts a PoSIC that is sufficiently clear

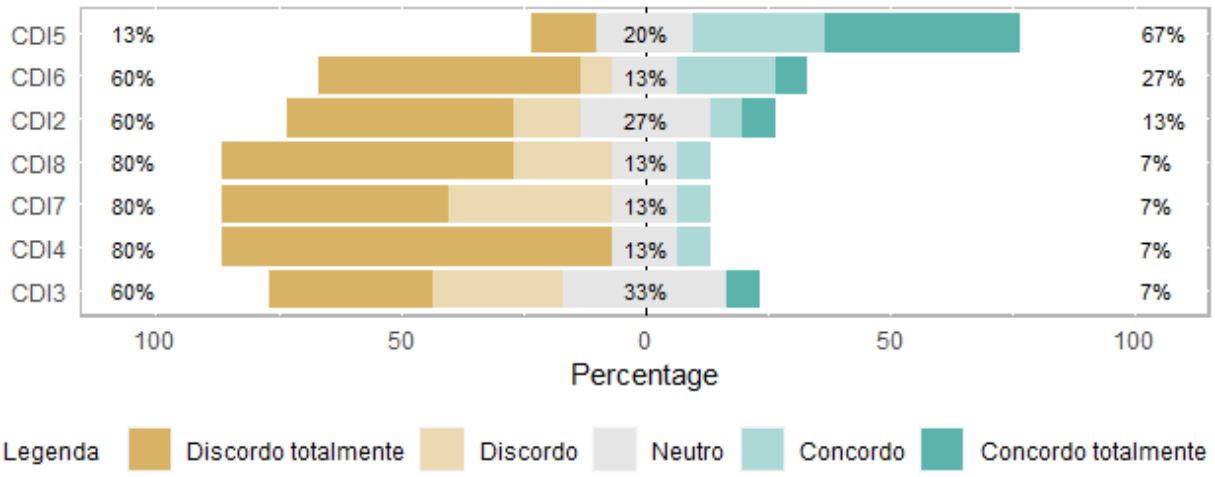
For a proper analysis, the factors related to this point are investigated in greater depth both in the next ICD elements and then in the analyses of the personal data protection dimensions.

Next, it can be seen from Figure 2 that the only aspect that showed a high degree of agreement (67%) was ICD5, which refers to the fact that the institution adopts, for user access to the systems, different authentication methods, such as user and password, biometrics, tokens by applications.

The other answers show a high degree of disagreement, and can be divided into two groups, one with 80% disagreement and the other with 60% disagreement. CDI4, CDI7 and CDI8 have 80% disagreement, when they talk about aspects related to conducting training or events that deal with privacy and protection of personal data; awareness of the context of information security; and how to protect confidential information in electronic format.

Next, with 60% of disagreement, are CDI2, CDI3, and CDI6, when addressing institutional aspects regarding the implementation of technical controls to protect personal data stored in its systems; whether it offers data subjects transparency and free access to the information and personal data stored in its systems; and the communication of issues that are related to privacy and data protection.

**Figure 2 –** Graphical representation of responses from CDI2 to CDI8[5]




Source: Research results

It is also noteworthy that ICD2, ICD3 and ICD5 present a certain degree of neutrality in relation to the other aspects analyzed, with emphasis on the 33% of ICD3, when dealing

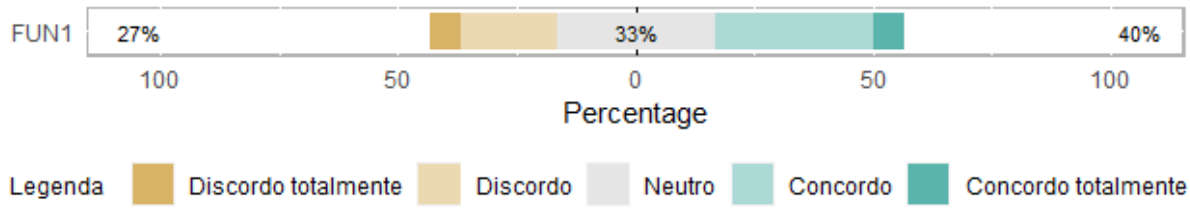
[5] Discordo totalmente = Completely disagree; Discordo = Disagree; Neutro = Neutral; Concordo = Agree; Concordo totalmente = Completely agree

with transparency and free access to information, which indicates a possible relationship of the indexes analyzed here with the phenomenon observed in ICD1.

The analysis of the personal data protection dimensions will contemplate the Fundamentals (FUN), Principles (PRI), Treatment (TRA) and Rights of the Data Subject (DIR).

With regard to the fundamentals of personal data protection (FUN), the pillar is the provision in the first sentence of Article 1 of the GDPR when it establishes that the institution, in its various activities, must be concerned with the "protection of personal data when processing", "including in digital media, in order to protect the fundamental rights of freedom, privacy and the free development of the personality of the natural person". (BRAZIL, 2018).

**Figure 3 –** Graphic representation of FUN1 responses



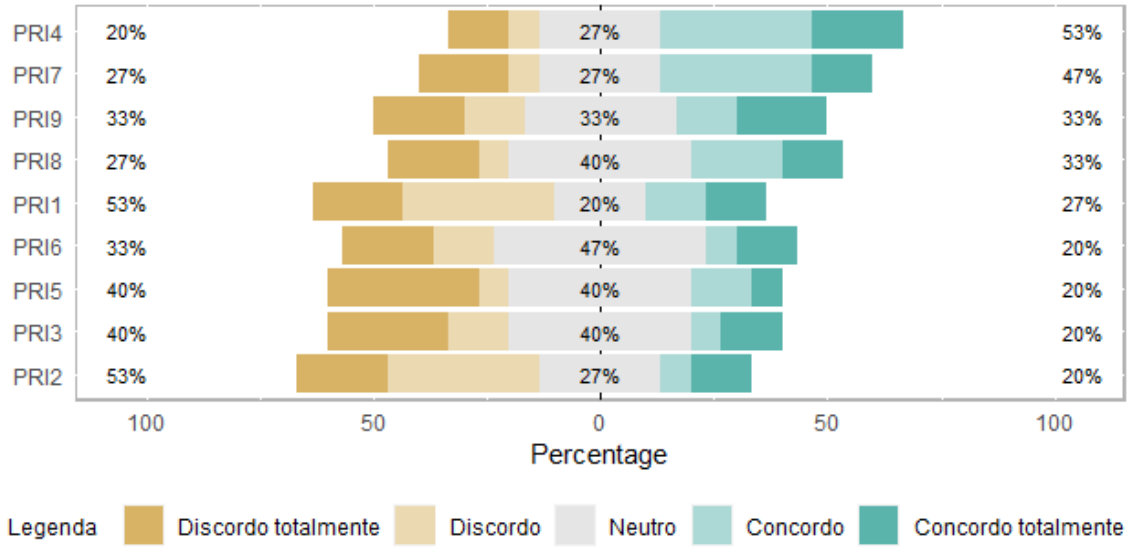

Source: Research results

- According to Figure 3, it can be observed that, despite 40% of respondents agreeing, there is a high degree (33%) of neutrality if compared to the total, and, in addition, approximately 27% of disagreement, thus bringing divergent and inconclusive results.
- The analysis of personal data protection principles (PRI) covers the investigation of whether, during the process of collecting and processing personal data, the institution informs its data subjects:
- PRI1 - "The specific purpose(s) of the use of such data" (BRAZIL, 2018);
- PRI2 - "The level of commitment to meet the informed purpose(s)" (BRAZIL, 2018);
- PRI3 - "Whether it allows free and facilitated consultation about the form and duration of the treatment, as well as the completeness of its personal data" (BRAZIL, 2018);
- PRI4 - "Whether it allows the updating of its data" (BRAZIL, 2018);
- PRI5 - "Whether it provides accessibility and clarity of information about the performance of treatment" (BRAZIL, 2018);

- PRI6 - "If uses technical and administrative measures suitable to protect personal data from unauthorized access and accidental or unlawful situations of destruction, loss, alteration, communication" (BRAZIL, 2018);
- PRI7 - "They use measures to prevent the occurrence of damage due to the processing of personal data," such as restrictions on access and authentication, adoption of encryption (BRAZIL, 2018);
- PRI8 - "It will be impossible to carry out treatment for discriminatory, illicit or abusive purposes", from the collection to its use, modification, dissemination and elimination of the data (BRAZIL, 2018);
- PRI9 - "It will adopt measures of compliance with the standards of protection of personal data, being responsible for the effectiveness of these measures" (BRAZIL, 2018).

Figure 4 shows that the answers presented a range between 20% and 46.67% of neutrality, which may indicate the need for attention to the principles listed by the GDPR, especially PRI6 - the security principle, provided for in Article 6, item VII, which deals with the use, by the institution, of "technical and administrative measures to protect personal data" (BRAZIL, 2018).

**Figure 4 –** Graphical Representation of PRI Responses




Source: Research results

Still analyzing the answers with a high rate of neutrality when compared to the rates of agreement and disagreement, PRI8 - "principle of non-discrimination", foreseen by article 6, item IX, despite the 33.33% of agreement, presents an even higher degree (40%) of neutrality,

a fact that is associated with the 26.67% of disagreement when dealing with the adoption of measures by the institution that make it impossible to "perform treatment for discriminatory, illicit or abusive purposes" from the collection to its use, modification, dissemination and elimination of the data (BRAZIL, 2018).

In this same range of 40% of neutrality, PRI5 - "transparency principle", provided for by Article 6, item VI, still shows 40% of disagreement and draws attention to possible adjustments by the institution regarding the guarantee, to the holders, of accessibility and clarity of information about the "conduct of processing and respective agents responsible" for data processing (BRAZIL, 2018).

An analogous situation occurs with PRI3 - "principle of free access", provided by Article 6, item IV, which provides that the institution must guarantee that data subjects are consulted "easily and free of charge on the form and duration of the processing, as well as on the completeness of their personal data" (BRAZIL, 2018).

The principle PRI9 - "principle of accountability and responsibility", listed by Article 6, item X, presents equal rates of 33.33% for disagreement, neutrality and agreement when addressing the adoption of measures of "observance and compliance with the standards of personal data protection, taking responsibility for the effectiveness of these measures" (BRAZIL, 2018).

The highest degree of disagreement is found in PRI1 and PRI2, with the index of 53.33%. PRI1 - "principle of purpose", provided by Article 6, item I, provides that the "performance of the processing is for legitimate, specific, explicit purposes and informed to the data subject, without the possibility of further processing in a manner incompatible with these purposes" (BRAZIL, 2018).

In the same context, PRI2 - "principles of adequacy and necessity", provided by Article 6, items II and III, address the "level of commitment to meet the purposes of data processing informed to the data subject, limiting the processing to the minimum necessary" (BRAZIL, 2018).

PRI4 and PRI7 were the only elements that presented a higher degree of agreement than the others. With 53.33% of agreement, PRI4 - "principle of quality", provided by Article 6, item V, provides that "the holder is guaranteed the possibility of updating, accuracy, clarity and relevance of their data, according to the need and for the fulfillment of the purpose of their treatment" (BRAZIL, 2018).

While with 46.66% agreement, PRI7 - "prevention principle", provided by Article 6, item VIII, deals with the "adoption of measures to prevent the occurrence of damage due to

the processing of personal data", such as access restrictions and authentications and adoption of encryptions (BRAZIL, 2018).

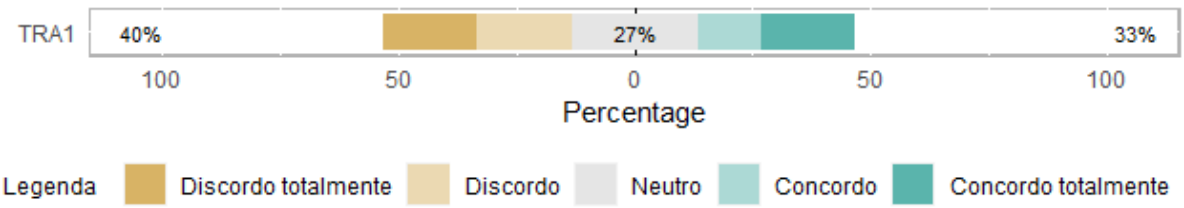
The analysis of the "processing of personal data" (TRA) covers the investigation of whether the institution:

● TRA 1 - asks the data subjects or legal guardians for their "consent in writing or by some other means that demonstrates manifestation of will" if there is interest in data processing (BRAZIL, 2018).

It can be observed that the answers present some degree of neutrality (26.67%) when compared to the other indexes and, as can also be visualized in Figure 5, the total index of disagreement is 40%, while the total of agreement is 33.33%.

With respect to the 40% of disagreement, it is observed the need on the part of the institution to ask the holders or legal guardians for their consent if there is interest in data processing, meeting the provisions of Article 7 of the GPDR, item I (BRAZIL, 2018). In addition, there are nine other items containing the hypotheses that must be met in order to carry out the processing of personal data (BRAZIL, 2018).

**Figure 5 –** Graphical Representation of TRA Responses

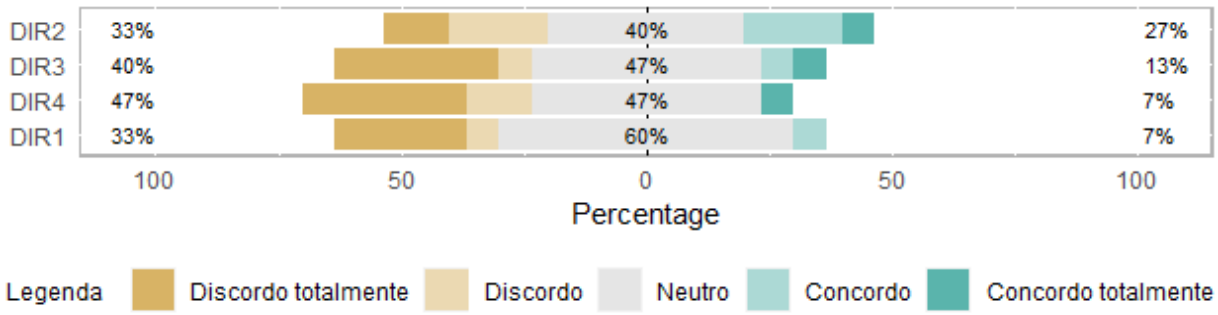



Source: Research results

The analysis of the "rights of the data subject" (DIR) covers the investigation of whether, upon the termination of the specific purpose of the processing, the institution guarantees data subjects the right to: DIR1 - "Revocation of consent"; DIR2 - "Anonymization of personal data"; DIR3 - "Blocking of personal data"; DIR4 - "Deletion of personal data" (BRAZIL, 2018).

It can be observed from Figure 6 that the responses presented a range between 40% and 60.00% of neutrality, which may indicate the need for attention to the "rights of the data subject" listed by the GPDR, especially to DIR1 - "right of the data subject to revoke his or her consent" provided by Article 18, item IX (BRAZIL, 2018).

**Figure 6 –** Graphical representation of DIR's responses




Source: Research results

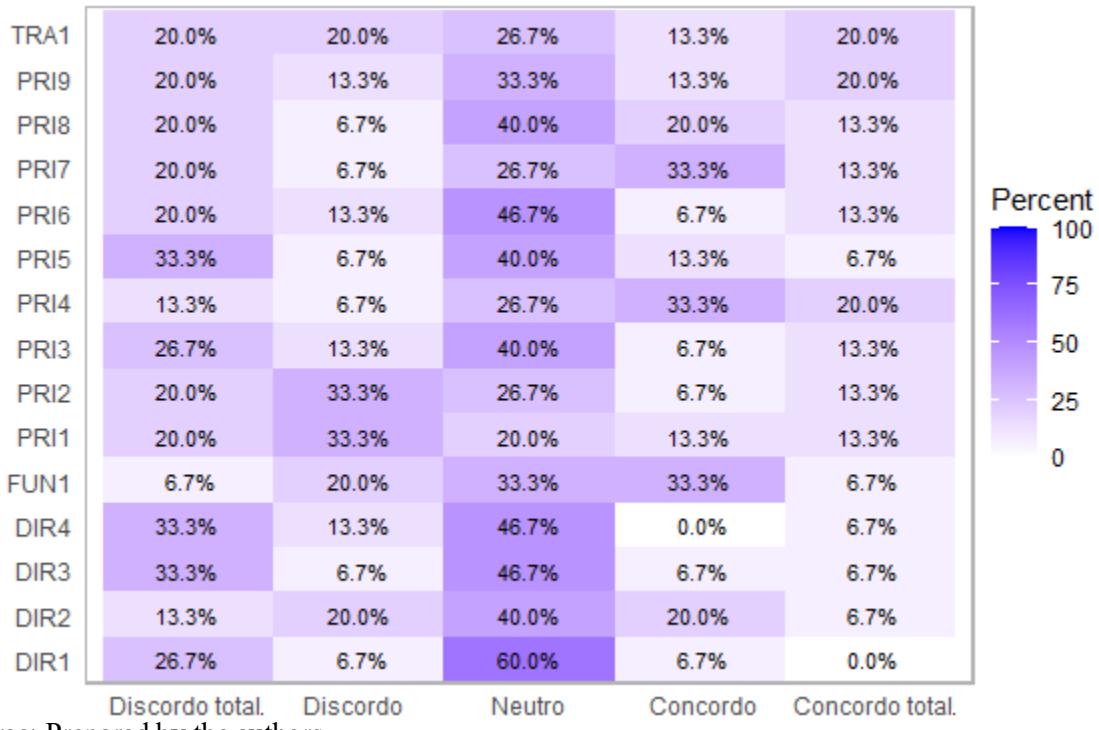
## Final remarks

The results and the data analysis demonstrate the relationship between the institutional context and the investigation of the dimensions that touch on fundamentals, principles, treatment of personal data and rights of the data subject, referring to the need for adjustments by the institution that, despite adopting a PoSIC, it is observed that a large part of the participants affirm not being able to say that this occurs.

Such statement corroborates the high degree of disagreement about the adoption of technical controls, transparency and free access, training or events that deal with privacy, communication and awareness about information security. The only exception is the adoption of different authentication methods by the institution, which significantly improves security as to access controls.

In turn, it can be seen from the heat map in Figure 7 that the analysis of the dimensions presents a certain degree of neutrality - central region of the map - when compared to those of disagreement and agreement.

**Figure 7** – Heat map of the answers of the personal data protection dimensions[6]




Source: Prepared by the authors

The dimensions analyzed address mandatory elements of the GDPR when dealing with fundamental rights constitutionally provided, such as freedom, privacy, free development of the personality of the natural person through the protection of personal data, as well as compliance with the principles listed by law: purpose, adequacy, necessity, free access, quality, transparency, security, prevention, non-discrimination, accountability.

Additionally, when processing their personal data, the consent of the holder must demonstrate their express and unequivocal manifestation of will, as well as the rights of revocation of consent, alteration, anonymization, blocking or elimination of the personal data. It must also ensure that each 'purpose' will be unique, legitimate, specified, explicit and in 'adequacy' to the context of each informed purpose, so that the operation is limited to the minimum 'necessity' and allows its full 'free access', free of charge and facilitated, guaranteeing the 'data quality' through its accuracy, relevance, updating and 'transparency', without renouncing to the adoption of measures capable of proving the 'security', 'prevention', 'non-discrimination', 'accountability and responsibility' of the processing agent.

Figure 8 represents the elements discussed and analyzed here, illustrating the flow of personal data protection within the institution.

[6] Discordo totalmente = Completely disagree; Discordo = Disagree; Neutro = Neutral; Concordo = Agree; Concordo totalmente = Completely agree

**Figure 8** – Flow of personal data protection[7]


Source: Prepared by the authors

The necessary adjustments to the campus are presented in the relationship of the institutional context with the dimensions of personal data protection provided by the GDPR, demonstrating the need to implement a privacy governance program that meets the institutional PoSIC, in a transparent way, with technical controls, training, communications and awareness.

Such measures consolidate a link of commitment and promote a relationship of trust between the data subject and the institution, as they are effectively integrated, applicable and adaptive.

[7] Contexto da instituição: Normas, políticas, procedimentos, controles e protocolos internos = Context of the institution: Norms, policies, procedures, internal controls and protocols; Fundamentos: Liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural = Foundations: Freedom, privacy and free development of the personality of the natural person; Princípios: Finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, não discriminação e responsabilização = Principles: Purpose, appropriateness, necessity, open access, quality, transparency, safety, prevention, non-discrimination, and accountability; Tratamento: Consentido, legal, finalístico, específico, formal, acessível e revigável = Treatment: Consent, legal, finalistic, specific, formal, accessible and revigable; Direitos do titular: Pivacidade, intimidade e liberdade de acesso, informação, correção, anonimização, portabilidade, eliminação e revogação = Rights of the holder: Pivacity, intimacy and freedom of access, information, correction, anonymity, portability, deletion and revocation

## REFERENCES

BRAZIL. **Lei n. 11.892, de 29 de dezembro 2008**. Institui a Rede Federal de Educação Profissional, Científica e Tecnológica, cria os Institutos Federais de Educação, Ciência e Tecnologia, e dá outras providências. Brasília, DF: Presidência da Repúlica, 2008. Available at: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11892.htm. Access on: 13 Dec. 2020.

BRAZIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Access on: 30 Aug. 2020.

BRAZIL. **Portaria IFSP n. 4296, de 14 de dezembro de 2020**. Aprova a atualização da Política de Segurança da Informação e Comunicação - PoSIC no âmbito do Instituto Federal de Educação, Ciência e Educação de São Pauto - IFSP. São Paulo: IFSP, 2020. Available at: https://www.ifsp.edu.br/component/content/article?layout=edit&id=2679. Access on: 11 Feb. 2022.

BRAZIL. **Emenda Constitucional n. 115**. 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. Brasília, DF: Atos do Congresso Nacional, 2022. Available at: https://in.gov.br/en/web/dou/-/emenda-constitucional-n-115-379516387. Access on: 11 Feb. 2022.

DAVENPORT, T. H. **Ecologia da informação:** Por que só a tecnologia não basta para o sucesso na era da informação. São Paulo: Futura, 1998.

LÉVY, P. **A esfera semântica**. São Paulo: Annablume, 2014.

LIKERT, R. A techniqueforthemeasurementofattitudes. **Archives ofPsychology**, v. 22, n. 140, p. 55, 1932. Available at: https://psycnet.apa.org/record/1933-01885-001. Access on: 06 Nov. 2021.

SOUZA, J. G. S.; ARIMA, C. H.; BELDA, F. R. Análise de tratamento da segurança da informação na gestão de riscos da governança de tecnologia da informação de uma instituição de ensino público federal. **Revista Ibero-Americana de Estudos em Educação**, Araraquara, v. 15, n. 3, p. 1309-1321, jul./set. 2020. Available at: https://periodicos.fclar.unesp.br/iberoamericana/article/view/13584. Access on: 18 Oct. 2021.

STOKES, D. E. **O quadrante de Pasteur**: A ciência básica e a inovação tecnológica. Campinas: Editora da Unicamp, 2005.

UNIÃO EUROPEIA (EU). **Diretiva n. 95/46/CE, de 24 de outubro de 1995**. Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Estrasburgo: Parlamento Europeu, 1995. Available at em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=EL. Access on: 03 Mar. 2021.

UNIÃO EUROPEIA (EU). Opinion 4/2007 ontheconceptofpersonal data. **European Commission**, 2007. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf. Access on: 03 Mar. 2021.

YIN, R. K. **Estudo de caso**: Planejamento e métodos. 2. ed. Porto Alegre: Bookman, 2001.

**How to reference this article**

SOUZA, J. G. S; BELDA, F. R.; ARIMA, C. H. GDPR application analysis in a public educational institution: a case study. **Revista Ibero-Americana de Estudos em Educação**, Araraquara, v. 17, n. 3, p. 1855-1871, July./Sept. 2022. e-ISSN: 1982-5587. DOI: https://doi.org/10.21723/riaee.v17i3.16789

**Submitted**: 18/02/2022
**Revisions required**: 27/03/2022
**Approved**: 10/05/2022
**Published**: 01/07/2022

**Processing and publishing by the Editora Ibero-Americana de Educação.**
Correction, formatting, standardization and translation.