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

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

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

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.

***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.*

[1] Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP), Campinas – SP – Brasil. Professor. Doutorando em Educação Escolar (UNESP). ORCID: https://orcid.org/0000-0003-4952-8618. E-mail: jackson@ifsp.edu.br
[2] Universidade Estadual Paulista (UNESP), Bauru – SP – Brasil. Professor do Departamento de Comunicação Social. Doutorado em Engenharia de Produção (EESC-USP). ORCID: https://orcid.org/0000-0001-6350-7026. E-mail: belda@faac.unesp.br
[3] Centro Estadual de Educação Tecnológica Paula Souza (CEETEPS), São Paulo – SP – Brasil. Professor do Programa de Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos e Pesquisador da Unidade de Pós-Graduação, Extensão e Pesquisa do Centro Paula Souza. Doutorado em Controladoria e Contabilidade (USP). ORCID: https://orcid.org/0000-0001-7922-0943. E-mail: charima@uol.com.br

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

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.*

Introdução

Segundo Davenport (1998, p. 18), "dados são simples observações sobre o estado do mundo" e tem como características ser: "facilmente estruturado, obtido por máquinas, frequentemente quantificado e facilmente transferível", enquanto informação seria um conjunto de "dados dotados de relevância e propósito", requerendo "unidade de análise, consenso em relação ao significado e, necessariamente, mediação humana". Tal mediação pode se apresentar pela "interação entre humanos e os sistemas, trazendo consigo conceitos como a segurança da informação e a privacidade envolvidos neste processo" (SOUZA; ARIMA; BELDA, 2020, p. 1310).

Estamos cercados por tecnologias diversas, de modo que a utilização de meios digitais para os processos de ensino e aprendizagem está diretamente relacionada ao tratamento de dados armazenados e utilizados pelas instituições, devendo estas adotar políticas de proteção de dados e informações pessoais com base em legislação específica.

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº. 13.709, de 14 de agosto de 2018 (BRASIL, 2018):

> Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Com a promulgação da Emenda Constitucional nº. 115 (EC115), publicada em 11 de fevereiro de 2022 na Seção 1, Edição 30, Página 2 do Diário Oficial da União, a Constituição Federal de 1988 brasileira passa a contemplar o rol de direitos e garantias fundamentais de

proteção de dados, fixando competência dos entes federativos em legislar sobre o tema (BRASIL, 2022).

A Lei nº. 11.892, de 29 de dezembro de 2008 (BRASIL, 2008), além de outras providências, institui que:

> Os Institutos Federais são instituições de educação superior, básica e profissional, pluricurriculares e *multicampi*, especializados na oferta de educação profissional e tecnológica nas diferentes modalidades de ensino, com base na conjugação de conhecimentos técnicos e tecnológicos com as suas práticas pedagógicas, nos termos desta Lei.

Neste sentido, esta pesquisa tem como objetivo estudar os instrumentos normativos de proteção de dados pessoais adotados numa instituição pública de ensino tecnológico e atuais desfechos para o desenvolvimento de políticas e procedimentos em um de seus *campi*.

Fundamentação teórica

Para Pierre Lévy (2014, p. 23), "nós não sabemos ainda como transformar sistematicamente dados em conhecimento", trazendo a reflexão quanto a uma "memória digital participativa, em vias de constituição, comum ao conjunto da humanidade em busca de solucionar este problema de interoperabilidade semântica".

Neste sentido, o autor estabelece uma unidade da natureza fundada na noção de informação, abordando uma imagem sintética da natureza informacional e seu conceito científico, concebendo a natureza da informação em camadas sucessivas: dos quarks aos átomos, das moléculas aos organismos, dos sistemas nervosos aos fenômenos e dos símbolos aos conceitos (LÉVY, 2014). Uma interpretação possível seria de que os dados equivaleriam a símbolos, ainda que não modalizados, porém não sem significado.

Em 24 de outubro de 1995, o Parlamento Europeu e o Conselho da União Europeia publicaram no Jornal Oficial nº. L 281 de 23/11/1995, páginas 31 a 50, a "Diretiva 95/46/CE relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados" (UNIÃO EUROPEIA, 1995).

O Artigo 29 da Diretiva 95/46/CE estabeleceu a criação do "grupo de proteção das pessoas no que diz respeito ao tratamento de dados pessoais", de caráter consultivo e independente, o "*Article 29 Working Party (WP29)"*, ou Grupo de Trabalho do Artigo 29 (GT29). Traz, ainda, a definição de dados pessoais fragmentando-a em 4 (quatro) pilares ou elementos principais:

> [...] ‘qualquer informação’, ‘relativa a’, ‘pessoa singular’, ‘identificada ou identificável’. Os quatro pilares estão intimamente relacionados e apoiam-se uns nos outros, determinando juntos se uma informação será ou não considerada dado pessoal [...] (UNIÃO EUROPEIA, 2007, p. 6, grifo do autor).

No Brasil, a LGPD, além de trazer uma definição similar de dado pessoal, regulamenta em seus 10 (dez) capítulos:

> ‘Disposições gerais’; ‘tratamento de dados pessoais’; ‘direitos do titular’; ‘tratamento de dados pessoais pelo poder público’; ‘transferência internacional de dados’; ‘agentes de tratamento de dados pessoais’; ‘segurança e boas práticas’; ‘fiscalização’; ‘Autoridade Nacional de Proteção de Dados (ANPD) e Conselho Nacional de Proteção de Dados Pessoais e da Privacidade’ e ‘disposições finais e transitórias’ (BRASIL, 2018).

O artigo 6º da LGPD estabelece, entre outros, princípios a serem observados, de modo que as políticas de tratamento adotadas permitam aos usuários estarem cientes das formas pelas quais seus dados serão utilizados, possibilitando evitar ou reduzir a coleta e utilização de suas informações por terceiros. Visando aplicar os conceitos, sintetizou-se os principais elementos em dimensões, conforme a Tabela 1.

Tabela 1 – Dimensões de proteção de dados pessoais

1. **Fundamentos (FUN)**: Preocupação com a “proteção de dados pessoais quando do seu tratamento, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (BRASIL, 2018, s/p [web]).
2. **Princípios (PRI)**: Atendimento aos princípios da “finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas” (BRASIL, 2018, s/p [web]).
3. **Tratamento de dados pessoais (TRA)**: “Toda operação realizada com dados pessoais”, sendo indispensável o consentimento do titular “por escrito ou por outro meio que demonstre a manifestação de vontade” “livre e inequívoca” (BRASIL, 2018, s/p [web]).
4. **Direitos do titular (DIR)**: O direito de “revogação do consentimento”, “atualização”, “anonimização”, “bloqueio” ou “eliminação” dos dados pessoais ao titular dos dados (BRASIL, 2018, s/p [web]).

Fonte: Adaptado pelos autores com base na LGPD (BRASIL, 2018)

O capítulo 4º da LGPD regulamenta o tratamento pelo poder público, inclusive fazendo referência direta no caput do artigo 23 à Lei nº 12.527, de 18 de novembro de 2011, também conhecida como Lei de Acesso à Informação (LAI), devendo “[...] ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de

executar as competências legais ou cumprir as atribuições legais do serviço público" (BRASIL, 2018).

Adicionalmente, o artigo 50 faz, em seus três parágrafos, referências diretas a princípios elencados no artigo 6º, tais como da finalidade, qualidade, segurança, prevenção e prestação de contas.

Procedimentos metodológicos

Conforme classificação de pesquisa feita pelo cientista político Donald Stokes, esta é uma pesquisa básica-aplicada, impulsionada pela curiosidade investigativa sobre fenômenos particulares, não necessariamente visando "objetivos explanatórios gerais nem qualquer utilização prática à qual se destinem seus resultados" (STOKES, 2005, p. 119).

Segundo Yin (2001, p. 11 e 47), o estudo de caso é uma inquirição empírica com foco "em fenômenos contemporâneos inseridos em algum contexto da vida real", tendo como pré-requisito a sistematização de procedimentos por meio de protocolos.

Este estudo abrange o "*campus* Campinas vinculado ao Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – IFSP" e, por tratar-se de estudo de caso único, os dados coletados e sua consequente análise não permitirão a generalização dos resultados (BRASIL, 2018). Para a coleta de dados, adota-se como instrumento um questionário digital estruturado na plataforma *Google Forms*. Conta, ainda, com a participação voluntária de 80 docentes e gestores cadastrados no "Sistema Unificado de Administração Pública" (SUAP) do *campus*, tendo sido coletadas um total de 15 respostas.

Segundo Likert (1932), pesquisas que envolvam declarações de opinião e atitude são consideradas um método indireto de aferir disposições que são mais facilmente significadas e expressas na forma verbal, e podem, consequentemente, serem agrupadas em padrões. Utilizar-se-á, portanto, da escala Likert, na qual as respostas obtidas emitem o grau de concordância dos participantes com a frase, contemplando níveis de 1 a 5 da escala, classificados respectivamente como: "Discordo totalmente", "Discordo", "Neutro", "Concordo" e "Concordo totalmente".

No que diz respeito à investigação dos instrumentos normativos adotados pelo IFSP em atendimento aos requisitos abordados na LGPD, a pesquisa documental deste estudo contempla o Estatuto da instituição e as Portarias mais recentes, que aprovam o Regimento Interno do Comitê de Governança Digital e que atualizam a "Política de Segurança da Informação e Comunicação – PoSIC", assim como a "Política de Proteção de Dados Pessoais" (BRASIL, 2020).

Análise de dados

A interpretação dos resultados inicialmente será a partir da seguinte estrutura: PDP – Perfil dos Participantes e CDI – Contexto da instituição.

Em seguida, serão investigadas dimensões de proteção de dados pessoais:

- FUN – Fundamentos da proteção de dados pessoais;
- PRI – Princípios da proteção de dados pessoais;
- TRA – Tratamento de dados pessoais;
- DIR – Direitos do titular de dados pessoais.

A amostra conta com 15 respostas coletadas. O perfil dos participantes caracteriza-se conforme faixa etária, escolaridade, tempo na instituição e se a pessoa participante ocupa cargo de gestão atualmente, conforme Tabela 2.

Tabela 2 – Perfil dos participantes

Docentes	Faixa etária	Escolaridade	Tempo instituição	Gestor
D1	30 a 39 anos	Mestrado	entre 4 e 10 anos	Não
D2	50 a 59 anos	Doutorado	entre 4 e 10 anos	Não
D3	30 a 39 anos	Mestrado	entre 4 e 10 anos	Não
D4	30 a 39 anos	Mestrado	entre 10 e 20 anos	Não
D5	50 a 59 anos	Doutorado	Mais de 20 anos	Sim
D6	40 a 49 anos	Doutorado	entre 4 e 10 anos	Sim
D7	60 a 69 anos	Doutorado	entre 4 e 10 anos	Não
D8	50 a 59 anos	Mestrado	entre 4 e 10 anos	Não
D9	30 a 39 anos	Doutorado	entre 4 e 10 anos	Sim
D10	40 a 49 anos	Doutorado	entre 4 e 10 anos	Sim
D11	50 a 59 anos	Doutorado	entre 4 e 10 anos	Não
D12	50 a 59 anos	Doutorado	entre 4 e 10 anos	Não
D13	40 a 49 anos	Mestrado	entre 4 e 10 anos	Não
D14	30 a 39 anos	Mestrado	entre 4 e 10 anos	Não
D15	18 a 29 anos	Mestrado	entre 4 e 10 anos	Não

Fonte: Resultados da pesquisa

O perfil do participante se altera conforme a escolaridade que possui, e observa-se que apenas duas faixas etárias englobam 64% dos docentes, sendo essas de 30 a 39 anos e de 50 a 59 anos; enquanto na primeira faixa a maior concentração é de mestrados, na segunda, a maioria possui doutorados.

A análise do contexto da instituição (CDI) abrange a investigação de:

- CDI1 – Adoção de uma Política de Segurança da Informação e Comunicações (PoSIC) suficientemente esclarecedora por parte da instituição;
- CDI2 – Controles técnicos de proteção para os dados pessoais armazenados;
- CDI3 – Transparência e livre acesso às informações e dados pessoais armazenados;

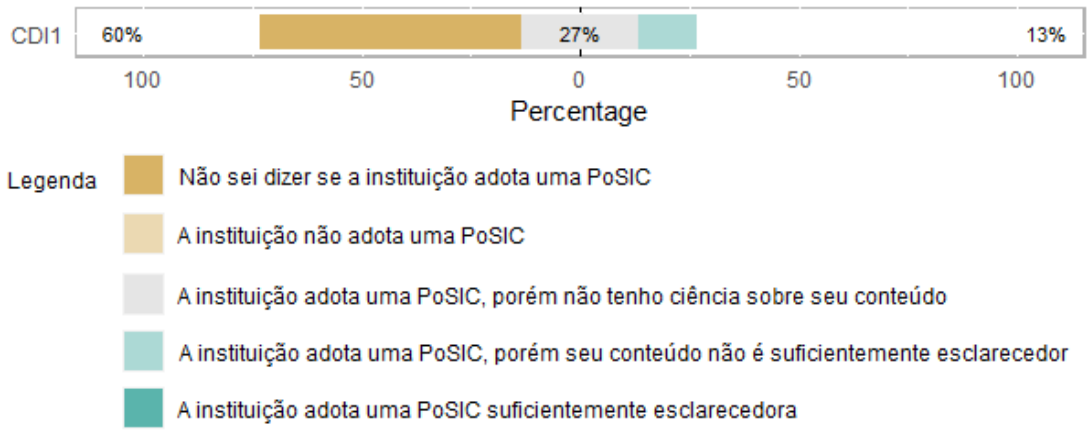
- CDI4 – Treinamentos ou eventos que tratem da privacidade e proteção de dados pessoais e operacionais;
- CDI5 – Adoção de diferentes métodos de autenticação;
- CDI6 – Comunicação, por meio de avisos, sobre privacidade e proteção de dados pessoais;
- CDI7 – Conscientização sobre segurança da informação;
- CDI8 – Conscientização sobre proteção de informações confidenciais em formato eletrônico.

Inicialmente, a ciência dos resultados quanto à adoção de uma Política de Segurança da Informação e Comunicações (PoSIC) suficientemente esclarecedora por parte da instituição, abordada pelo elemento CDI1, nos trará evidências de possíveis respostas neutras nas afirmações sobre o contexto da instituição.

Conforme também pode ser visualizado pela Figura 1, 40% dos participantes concordam que a instituição adota uma PoSIC; entretanto, 26,67% afirmam não terem ciência sobre seu conteúdo, e 13,33%, que seu conteúdo não é suficientemente esclarecedor.

A despeito de 60% dos participantes não saberem dizer se a instituição adota uma PoSIC, uma inferência prematura deste fenômeno poderia colocar em questão seu nível de familiaridade com o tema abordado. Entretanto, os participantes complementam em suas respostas que 'na instituição os servidores pouco conhecem sobre a LGPD, e não há medidas institucionais adotada para proteção de dados, ficando a cargo do bom senso do servidor a proteção dos dados', e ainda 'não ter conhecimento algum sobre proteção de dados em nossa instituição'.

Figura 1 – Representação gráfica das respostas de CDI1



Fonte: Resultados da pesquisa

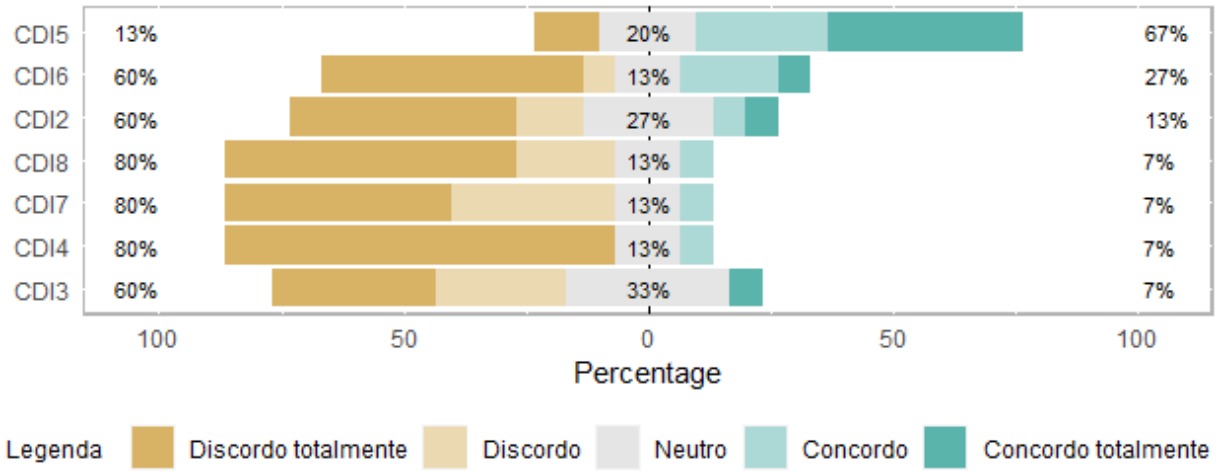
Para uma análise adequada, os fatores relacionados a este ponto são investigados com maior profundidade tanto nos próximos elementos de CDI quanto, em seguida, nas análises das dimensões de proteção de dados pessoais.

Em sequência, observa-se pela Figura 2 que o único aspecto que apresentou alto grau de concordância (67%) foi CDI5, que se refere ao fato de a instituição adotar, para o acesso dos usuários aos sistemas, diferentes métodos de autenticação, como por exemplo, usuário e senha, biometria, tokens por aplicativos.

As demais respostas apresentam alto grau de discordância, podendo ser divididas em dois grupos, um com 80% de discordância e outro com 60% de discordância. Com 80% estão CDI4, CDI7 e CDI8, ao abordarem aspectos referentes à condução de treinamentos ou eventos que tratem da privacidade e proteção de dados pessoais; à ciência do contexto da segurança da informação; e de como proteger informações confidenciais em formato eletrônico.

Em seguida, com 60% de discordância, tem-se CDI2, CDI3 e CDI6, ao tratarem de aspectos institucionais no tocante à implementação de controles técnicos para proteger dados pessoais armazenados em seus sistemas; se oferece aos titulares de dados transparência e livre acesso às informações e dados pessoais armazenados em seus sistemas; e a comunicação de questões que sejam relacionadas à privacidade e proteção de dados.

Figura 2 – Representação gráfica das respostas de CDI2 a CDI8



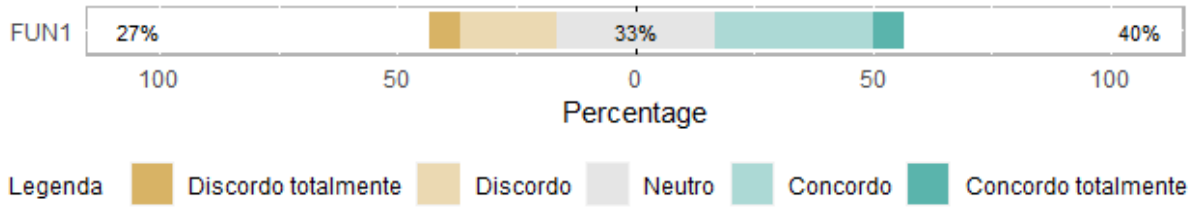
Fonte: Resultados da pesquisa

Destaca-se também o fato de CDI2, CDI3 e CDI5 apresentarem um certo grau de neutralidade em relação aos demais aspectos analisados, com destaque a 33% de CDI3, ao tratar da transparência e livre acesso às informações, o que indica uma possível relação dos índices aqui analisados com o fenômeno observado em CDI1.

A análise das dimensões de proteção de dados pessoais contemplará os Fundamentos (FUN), Princípios (PRI), Tratamento (TRA) e Direitos do Titular (DIR).

No que diz respeito aos fundamentos de proteção de dados pessoais (FUN), tem-se como pilar o disposto no caput do artigo 1º da LGPD, ao estabelecer que a instituição, em suas diversas atividades, deve preocupar-se com a "proteção dos dados pessoais quando do seu tratamento", "inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (BRASIL, 2018).

Figura 3 – Representação gráfica das respostas de FUN1



Fonte: Resultados da pesquisa

Conforme a Figura 3, observa-se que, apesar de 40% de concordância por parte dos respondentes, há um alto grau (33%) de neutralidade se comparado ao total e, além disto, aproximadamente 27% de discordância, trazendo assim resultados divergentes e inconclusivos.

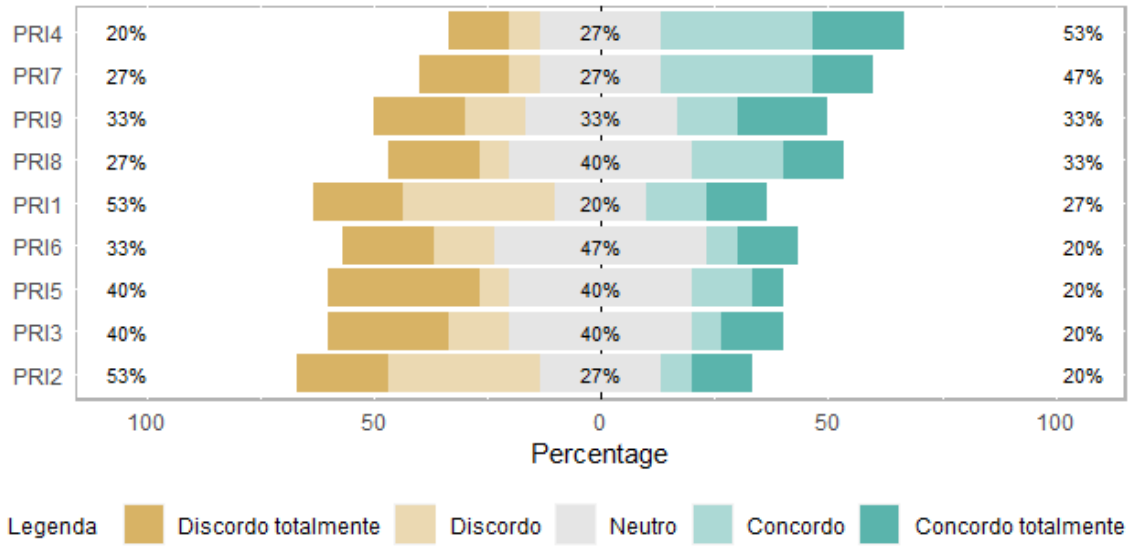
A análise dos princípios de proteção de dados pessoais (PRI) abrange a investigação de se, durante o processo de coleta e tratamento de dados pessoais, a instituição informa a seus titulares:

- PRI1 – "A(s) finalidade(s) específica(s) do uso desses dados" (BRASIL, 2018);
- PRI2 – "O nível de comprometimento em atender à(s) finalidade(s) informada(s)" (BRASIL, 2018);
- PRI3 – "Se permite consulta gratuita e facilitada sobre a forma e duração do tratamento, bem como a integralidade de seus dados pessoais" (BRASIL, 2018);
- PRI4 – "Se permite a atualização de seus dados" (BRASIL, 2018);
- PRI5 – "Se fornece acessibilidade e clareza de informações sobre a realização de tratamento" (BRASIL, 2018);
- PRI6 – "Se utiliza de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação" (BRASIL, 2018);

- PRI7 – "Se utilizam de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais", como por exemplo, restrições em acessos e autenticações, adoção de criptografias (BRASIL, 2018);
- PRI8 – "Se impossibilitará a realização de tratamento para fins discriminatórios, ilícitos ou abusivos", desde a coleta à sua utilização, modificação, difusão e eliminação dos dados (BRASIL, 2018);
- PRI9 – "Se adotará medidas de observância o cumprimento das normas de proteção de dados pessoais, se responsabilizando pela eficácia dessas medidas" (BRASIL, 2018).

A Figura 4 demonstra que as respostas apresentaram uma faixa entre 20% e 46,67% de neutralidade, podendo indicar a necessidade de atenção aos princípios elencados pela LGPD, em especial ao PRI6 - princípio da segurança, previsto pelo artigo 6º, inciso VII, que trata da utilização, por parte da instituição, de "medidas técnicas e administrativas aptas a proteger dados pessoais" (BRASIL, 2018).

Figura 4 – Representação gráfica das respostas de PRI



Fonte: Resultados da pesquisa

Ainda analisando as respostas com alto índice de neutralidade quando comparadas aos índices de concordância e discordância, PRI8 - "princípio da não discriminação", previsto pelo artigo 6º, inciso IX, apesar dos 33,33% de concordância, apresenta um grau ainda maior (40%) de neutralidade, fato que se associa aos 26,67% de discordância ao tratar da adoção de medidas por parte da instituição que impossibilitem a "realização de tratamento para fins discriminatórios, ilícitos ou abusivos" desde a coleta à sua utilização, modificação, difusão e eliminação dos dados (BRASIL, 2018).

Neste mesmo intervalo de 40% de neutralidade, PRI5 - "princípio da transparência", previsto pelo artigo 6º, inciso VI, apresenta ainda 40% de discordância e atenta para possíveis adequações por parte da instituição quanto à garantia, aos titulares, de acessibilidade e clareza de informações sobre a "realização de tratamento e respectivos agentes responsáveis" pelo tratamento de dados (BRASIL, 2018).

Situação análoga ocorre com PRI3 - "princípio do livre acesso", previsto pelo artigo 6º, inciso IV, que prevê que a instituição garanta aos titulares consulta "facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais" (BRASIL, 2018).

O princípio PRI9 - "princípio da responsabilização e prestação de contas", elencado pelo artigo 6º, inciso X, apresenta índices iguais de 33,33% para discordância, neutralidade e concordância ao abordar a adoção de medidas de "observância e cumprimento das normas de proteção de dados pessoais, se responsabilizando pela eficácia dessas medidas" (BRASIL, 2018).

O maior grau de discordância encontra-se em PRI1 e PRI2, com o índice de 53,33%. PRI1 - "princípio da finalidade", previsto pelo artigo 6º, inciso I, prevê que a "realização do tratamento seja para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades" (BRASIL, 2018).

No mesmo contexto, PRI2 - "princípios da adequação e necessidade", previstos pelo artigo 6º, incisos II e III, tratam do "nível de comprometimento em atender às finalidades do tratamento de dados informadas ao titular, limitando o tratamento ao mínimo necessário" (BRASIL, 2018).

PRI4 e PRI7 foram os únicos elementos que apresentaram grau de concordância superior aos demais. Com 53,33% de concordância, PRI4 - "princípio da qualidade", previsto pelo artigo 6º, inciso V, prevê que "seja garantida ao titular a possibilidade de atualização, exatidão, clareza e relevância de seus dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento" (BRASIL, 2018).

Enquanto com 46,66% de concordância, PRI7 - "princípio da prevenção", previsto pelo artigo 6º, inciso VIII, trata da "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais", como por exemplo, restrições de acessos e autenticações e adoção de criptografias (BRASIL, 2018).

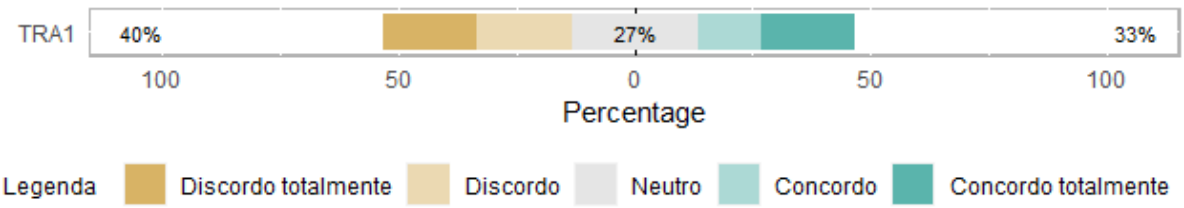
A análise do "tratamento de dados pessoais" (TRA) abrange a investigação de se a instituição:

- TRA 1 – solicita aos titulares ou responsáveis legais seu "consentimento por escrito ou por algum outro meio que demonstre manifestação de vontade", caso haja interesse no tratamento de dados (BRASIL, 2018).

Observa-se que as respostas apresentam certo grau de neutralidade (26,67%) quando comparado aos demais índices e, conforme também pode ser visualizado na Figura 5, o índice total de discordância é de 40%, enquanto o total de concordância é de 33,33%.

No que diz respeito aos 40% de discordância, observa-se a necessidade por parte da instituição em solicitar aos titulares ou responsáveis legais seu consentimento caso haja interesse no tratamento de dados, indo ao encontro do previsto no artigo 7º da LGPD, inciso I (BRASIL, 2018). Além deste, há outros nove incisos contendo as hipóteses que devem ser atendidas para que possa ser realizado o tratamento de dados pessoais (BRASIL, 2018).

Figura 5 – Representação gráfica das respostas de TRA

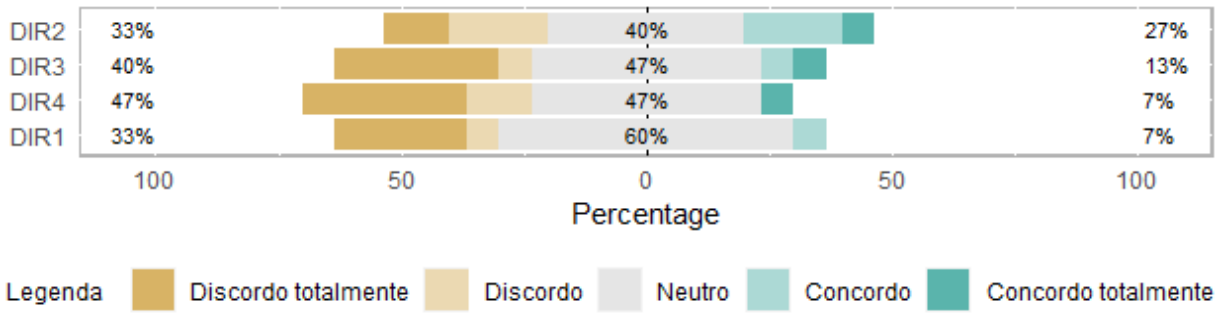


Fonte: Resultados da pesquisa

A análise dos "direitos do titular de dados" (DIR) abrange a investigação de se, quando do término da finalidade específica do tratamento, a instituição garante aos titulares dos dados o direito de: DIR1 – "Revogação do consentimento"; DIR2 – "Anonimização dos dados pessoais"; DIR3 – "Bloqueio dos dados pessoais"; DIR4 – "Eliminação dos dados pessoais" (BRASIL, 2018).

Observa-se pela Figura 6 que as respostas apresentaram uma faixa entre 40% e 60,00% de neutralidade, podendo indicar a necessidade de atenção aos "direitos do titular de dados" elencados pela LGPD, em especial ao DIR1 – "direito do titular de revogar seu consentimento" previsto pelo artigo 18, inciso IX (BRASIL, 2018).

Figura 6 – Representação gráfica das respostas de DIR



Fonte: Resultados da pesquisa

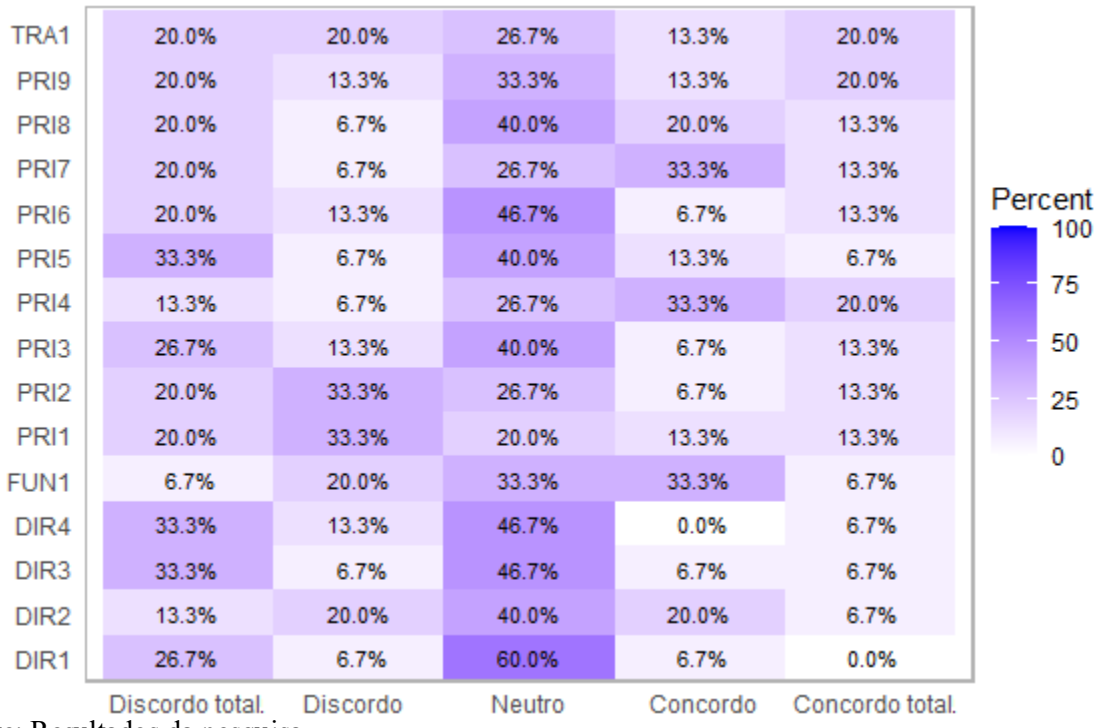
Considerações finais

Os resultados e as análises dos dados demonstram a relação entre o contexto institucional e a investigação das dimensões que tangem fundamentos, princípios, tratamento de dados pessoais e direitos do titular de dados, remetendo à necessidade de adequações por parte da instituição que, apesar de adotar uma PoSIC, observa-se que grande parte dos participantes afirmam não saber dizer que isto ocorre.

Tal afirmação corrobora com o alto grau de discordância quanto à adoção de controles técnicos, transparência e livre acesso, treinamentos ou eventos que tratem da privacidade, comunicação e conscientização sobre segurança da informação. A única exceção encontra-se na adoção de diferentes métodos de autenticação por parte da instituição, o que aprimora significativamente a segurança quanto aos controles de acesso.

Por sua vez, observa-se pelo mapa de calor da Figura 7 que a análise das dimensões apresenta certo grau de neutralidade – região central do mapa –, quando comparado aos de discordância e concordância.

Figura 7 – Mapa de calor das respostas das dimensões de proteção de dados pessoais



Fonte: Resultados da pesquisa

As dimensões analisadas abordam elementos obrigatórios da LGPD ao tratar direitos fundamentais previstos constitucionalmente, como de liberdade, de privacidade, livre desenvolvimento da personalidade da pessoa natural pela proteção de dados pessoais, assim como atendimento aos princípios elencados pela lei: finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, não discriminação, responsabilização.

Adicionalmente, quando do tratamento de seus dados pessoais, o consentimento do titular deve demonstrar sua manifestação de vontade expressa e inequívoca, assim como os direitos de revogação do consentimento, alteração, anonimização, bloqueio ou eliminação dos dados pessoais. Deve-se, ainda, assegurar que cada 'finalidade' será única, legítima, especificada, explicita e em 'adequação' ao contexto de cada finalidade informada, de modo que a operação se limite à mínima 'necessidade' e permita seu 'livre acesso' integral, gratuito e facilitado, garantindo a 'qualidade dos dados' pela sua exatidão, relevância, atualização e 'transparência', sem renunciar à adoção de medidas capazes de comprovar a 'segurança', 'prevenção', 'não discriminação', 'responsabilização e prestação de contas' por parte do agente de tratamento.

A Figura 8 representa os elementos aqui discutidos e analisados, ilustrando o fluxo de proteção de dados pessoais dentro da instituição.

Figura 8 – Fluxo de proteção de dados pessoais

Fonte: Elaborado pelo autor

As adequações necessárias ao *campus* apresentam-se no relacionamento do contexto institucional com as dimensões de proteção de dados pessoais previstos pela LGPD, demonstrando a necessidade de implementação de um programa de governança em privacidade que vá ao encontro da PoSIC institucional, de forma transparente, com controles técnicos, treinamentos, comunicações e conscientizações.

Tais medidas consolidam um elo de comprometimento e promovem uma relação de confiança entre o titular de dados e a instituição, por serem efetivamente integradas, aplicáveis e adaptativas.

REFERÊNCIAS

BRASIL. **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. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11892.htm. Acesso em: 13 dez. 2020.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 30 ago. 2020.

BRASIL. **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. Disponível em: https://www.ifsp.edu.br/component/content/article?layout=edit&id=2679. Acesso em: 11 fev. 2022.

BRASIL. **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. Disponível em: https://in.gov.br/en/web/dou/-/emenda-constitucional-n-115-379516387. Acesso em: 11 fev. 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 technique for the measurement of attitudes. **Archives of Psychology**, v. 22, n. 140, p. 55, 1932. Disponível em: https://psycnet.apa.org/record/1933-01885-001. Acesso em: 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. Disponível em: https://periodicos.fclar.unesp.br/iberoamericana/article/view/13584. Acesso em: 18 out. 2021.

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

UNIÃO EUROPEIA. **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. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=EL. Acesso em: 03 mar. 2021.

UNIÃO EUROPEIA. Opinion 4/2007 on the concept of personal data. **European Commission**, 2007. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf. Acesso em: 03 mar. 2021.

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

Como referenciar este artigo

SOUZA, J. G. S; BELDA, F. R.; ARIMA, C. H. Análise de aplicação da LGPD numa instituição pública de ensino: Um estudo de caso. **Revista Ibero-Americana de Estudos em Educação**, Araraquara, v. 17, n. 3, p. 1856-1872, jul./set. 2022. e-ISSN: 1982-5587. DOI: https://doi.org/10.21723/riaee.v17i3.16789

Submetido em: 18/02/2022
Revisões requeridas em: 27/03/2022
Aprovado em: 10/05/2022
Publicado em: 01/07/2022

Processamento e editoração: Editora Ibero-Americana de Educação.
Revisão, formatação, normalização e tradução.