

UNIVERSIDADE FEDERAL DO MARANHÃO  
CENTRO DE CIÊNCIAS SOCIAIS  
CURSO DE BIBLIOTECONOMIA

**JESSICA MELO SANTOS**

**A LEI GERAL DE PROTEÇÃO DE DADOS NA BIBLIOTECA ESCOLAR: um**  
estudo de caso em uma escola privada de São Luís

São Luís  
2023

**JESSICA MELO SANTOS**

**A LEI GERAL DE PROTEÇÃO DE DADOS NA BIBLIOTECA ESCOLAR: um  
estudo de caso em uma escola privada de São Luís**

Monografia apresentada ao curso de Biblioteconomia da Universidade Federal do Maranhão, como requisito para obtenção de grau de Bacharel em Biblioteconomia.

Orientadora: Profa. Dra. Dirlene Santos Barros.

São Luís  
2023

Ficha gerada por meio do SIGAA/Biblioteca com dados fornecidos pelo(a) autor(a).  
Diretoria Integrada de Bibliotecas/UFMA

Santos, Jessica Melo.

A Lei Geral de Proteção de dados na biblioteca escolar  
: um estudo de caso em uma escola privada de São Luís /  
Jessica Melo Santos. - 2023.

65 f.

Orientador(a): Dirlene Santos Barros.

Curso de Biblioteconomia, Universidade Federal do  
Maranhão, São Luís, 2023.

1. Biblioteca escolar. 2. Instituições de ensino. 3.  
Lei Geral de Proteção de dados. 4. LGPD. 5. Privacidade  
de dados. I. Barros, Dirlene Santos. II. Título.

**JESSICA MELO SANTOS**

**A LEI GERAL DE PROTEÇÃO DE DADOS NA BIBLIOTECA ESCOLAR:** um  
estudo de caso em uma escola privada de São Luís

Monografia apresentada ao curso de  
Biblioteconomia da Universidade Federal do  
Maranhão, como requisito para obtenção de  
grau de Bacharel em Biblioteconomia.

Orientadora: Profa. Dra. Dirlene Santos Barros

Aprovado em: \_\_\_\_/\_\_\_\_/\_\_\_\_.

**BANCA EXAMINADORA**

---

**Profa. Dra. Dirlene Santos Barros (Orientadora)**  
Doutora em Ciência da Informação  
Universidade Federal do Maranhão

---

**Profa. Dra. Maria Mary Ferreira**  
Doutora em Sociologia  
Universidade Federal do Maranhão

---

**Profa. Dra. Jaciara Januario da Silva**  
Doutora em Multimédias da Educação  
Universidade Federal do Maranhão

A Deus, à minha família e a todos que  
contribuíram de forma especial para a  
realização deste sonho.

## **AGRADECIMENTOS**

Em primeiro lugar agradeço a Deus, por cuidar e estar sempre ao meu lado, por todas as oportunidades que me foram dadas e por sempre renovar as minhas forças para enfrentar os desafios ao longo da vida. À Ele devo todas as minhas conquistas;

À minha família, por acreditar em mim e sempre me motivar a ir adiante, por me ensinarem que a educação é um instrumento transformador que abre portas para o futuro. Em especial, agradeço à minha mãe, Iracema Melo, ao meu pai, Marcos Santos, e à minha avó, Aracy Santos, por todo amor, cuidado, carinho, apoio, incentivo e compreensão, sem vocês eu não teria chegado tão longe;

À Universidade Federal do Maranhão, pela oportunidade de cursar Biblioteconomia;

À minha orientadora, Profa. Dra. Dirlene Santos Barros, que me deu a honra de ser sua orientanda, por seu precioso apoio e compreensão, por suas aulas e orientações, os quais foram essenciais para o desenvolvimento deste estudo;

Aos membros da banca examinadora, às professoras doutoras Maria Mary Ferreira e Jaciara Januário da Silva, por aceitarem participar desse momento importante na minha trajetória;

Aos professores do Departamento de Biblioteconomia, pelos ensinamentos que usaremos na vida e por exercerem a profissão de bibliotecário com maestria;

Aos amigos e colegas de universidade que o curso me deu de presente, e que estiveram comigo ao longo dessa jornada;

Aos meus estágios, os quais me proporcionaram muitos aprendizados no campo da Biblioteconomia e que contribuíram com a minha formação enquanto pessoa e profissional;

Aos meus queridos amigos, pelas mensagens de motivação e incentivo, por todo suporte e paciência;

A todos que de alguma forma, seja direta ou indiretamente, contribuíram para a concretização de um sonho em realidade.

## RESUMO

Estudo sobre a Lei Geral de Proteção de Dados e sua implementação em uma instituição de ensino privado de São Luís no contexto da biblioteca escolar. Apresenta o desenvolvimento histórico do direito à privacidade e a evolução da proteção de dados pessoais ao longo do tempo. Com os avanços sociais e tecnológicos, observou-se a necessidade de criar legislações que assegurassem os direitos fundamentais e o pleno desenvolvimento do indivíduo. No Brasil, surge a Lei nº 13.709 (Lei Geral de Proteção de Dados Pessoais), comumente conhecida como LGPD, sancionada em 14 de agosto de 2018 pelo ex-presidente da República Federativa do Brasil Michel Temer, a qual entrou em vigor em 18 de setembro de 2020, trazendo importantes desafios e impactos para as organizações, sejam elas de âmbito público ou privado. Verificou-se, neste ensejo, como a biblioteca da Escola A implementou esse novo marco regulatório nacional, uma vez que este espaço diariamente trabalha com os dados pessoais de seus usuários. Utilizou-se como metodologia a pesquisa bibliográfica para fundamentação teórica, a exemplo da contribuição dos autores Lugati e Almeida (2020), Assmann (2014), Guerra (2005) e Castells (2004). Na pesquisa de campo, aplicou-se como instrumento de coleta de dados duas entrevistas semiestruturadas, uma realizada com a responsável pela biblioteca e outra com o consultor em Sistema de Informação (SI) da instituição de ensino. Como resultado, foram apresentadas as medidas que a biblioteca tem implementado em suas rotinas administrativas, levando em consideração a LGPD e o meio pelo qual a Escola A buscou se adequar à Lei para garantir o correto tratamento de dados pessoais da comunidade escolar. Conclui-se que a biblioteca escolar, apesar de ainda não ter passado pelo processo de *Data Mapping*, busca atender às determinações da lei. E a Escola A, por sua vez, aplica às disposições da LGPD nas diversas áreas de atuação da instituição, e como reflexo tem-se a política de privacidade de dados que contém informações referentes às regras sobre o tratamento de dados e os direitos dos titulares.

Palavras-chave: Lei Geral de Proteção de Dados; LGPD; privacidade de dados; instituições de ensino; biblioteca escolar.

## ABSTRACT

Study on the General Data Protection Law and its implementation in a bilingual educational institution in São Luís in the context of the school library. It presents the historical development of the right to privacy and the evolution of personal data protection over time. With social and technological advances, there was a need to create legislation to ensure fundamental rights and the full development of the individual. In Brazil, Law n°. 13.709 (General Personal Data Protection Law), commonly known as the LGPD, was sanctioned on August 14, 2018 by the former president of the Federative Republic of Brazil Michel Temer, and came into force on September 18, 2020, bringing important challenges and impacts for organizations, whether public or private. In this context, we looked at how School A's library has implemented this new national regulatory framework, given that this space works with its users' personal data on a daily basis. The methodology used was bibliographical research for theoretical foundations, such as the contributions of the authors Lugati and Almeida (2020), Assmann (2014), Guerra (2005) and Castells (2004). In the field research, two semi-structured interviews were conducted, one with the person in charge of the library and the other with the Information System (IS) consultant at the educational institution. As a result, the measures that the library has implemented in its administrative routines were presented, taking into account the LGPD and the means by which School A has sought to adapt to the Law to ensure the correct processing of personal data of the school community. It can be concluded that the school library, although it has not yet gone through the Data Mapping process, is trying to comply with the law. And School A, in turn, applies the provisions of the LGPD in the various areas of activity of the institution, and as a result has a data privacy policy that contains information regarding the rules on data processing and the rights of data subjects.

Keywords: General Data Protection Law; LGPD; data privacy; educational institutions; school library.

## LISTA DE ABREVIATURAS E SIGLAS

ALA	American Library Association (Associação Americana de Bibliotecas)
ART.	Artikel (artigo, usado no texto constitucional)
ARTS.	Artikels (artigos, no plural, usado no texto constitucional)
ANPD	Autoridade Nacional de Proteção de Dados
BDSG	<i>Bundesdatenschutzgesetz</i> (Lei Federal de Proteção de Dados Pessoais alemã)
BDTD	Biblioteca Digital de Teses e Dissertações
BVerGE	<i>Bundesverfassungsgerichtsentscheidung</i> (Decisão do Tribunal Constitucional Federal alemão)
BVerGE	<i>Volkszählungsurteil</i> (Decisão sobre a Lei do Censo)
CC	Código Civil
CCB	Código Civil Brasileiro
CDC	Código de Defesa do Consumidor
CE	Conselho Europeu
CF	Constituição Federal
CIA	<i>Central Intelligence Agency</i> (Agência Central de Inteligência)
EU	União Europeia
EUA	Estados Unidos da América
GDPR	<i>General Data Protection Regulation</i>
IBICT	Instituto Brasileiro de Informação Científica e Tecnológica
IFLA	Federação Internacional de Associações e Instituições Bibliotecárias
LAI	Lei de Acesso à Informação
LDB	Lei de Diretrizes e Bases da Educação Nacional
LGPD	Lei Geral de Proteção de Dados
MDB/SP	Movimento Democrático Brasileiro/ São Paulo
MCI	Marco Civil da Internet
MEC	Ministério da Educação
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
ONU	Organização das Nações Unidas
NSA	<i>National Security Agency</i> (Agência de Segurança Nacional)
PT	Partido dos Trabalhadores
RGPD	Regulamento Geral sobre a Proteção de Dados

RS	Rio Grande do Sul
SI	Sistema de Informação
UE	União Europeia
UFMA	Universidade Federal do Maranhão
UFMG	Universidade Federal de Minas Gerais
UNESCO	Organização das Nações Unidas para a Educação, a Ciência e a Cultura

## SUMÁRIO

<b>1 INTRODUÇÃO.....</b>	<b>12</b>
<b>2 CONTEXTUALIZAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS: da criação à implementação no Brasil.....</b>	<b>15</b>
2.1 A construção histórica da LGPD no Brasil: ordenamento jurídico antecedente à LGPD no Brasil.....	25
2.2 A LGPD toma forma: sua constituição, estruturas e especificações.....	34
2.3 Privacidade e violação do uso dos dados pessoais.....	38
2.4 A biblioteca escolar no contexto da proteção dos dados pessoais dos seus usuários.....	43
<b>3 METODOLOGIA.....</b>	<b>47</b>
3.1 Lócus de pesquisa.....	49
3.1.1 A biblioteca da Escola A.....	50
<b>4 RESULTADOS E DISCUSSÃO.....</b>	<b>51</b>
4.1 Descrição e análise dos dados obtidos.....	51
<b>5 CONSIDERAÇÕES FINAIS.....</b>	<b>57</b>
<b>REFERÊNCIAS.....</b>	<b>59</b>
<b>APÊNDICE A- INSTRUMENTO DE COLETA DE DADOS.....</b>	<b>66</b>
<b>APÊNDICE B- INSTRUMENTO DE COLETA DE DADOS.....</b>	<b>67</b>

## 1 INTRODUÇÃO

A comunicação, inerente aos seres humanos, faz-se imprescindível nas relações sociais e por meio dela é possível acompanhar a evolução humana ao longo da história. Com a revolução tecnológica, tornou-se possível eliminar as barreiras geográficas e permitir a troca de informações entre pessoas de diversas partes do mundo.

Os meios tecnológicos transformaram-se em necessidade na sociedade contemporânea, possibilitando amplo acesso aos conteúdos veiculados na internet, constituindo-se como ferramentas diferenciais no mundo globalizado e em um mercado de trabalho cada vez mais competitivo, afirma Junkes (2014).

Se a tecnologia da informação é hoje o que a eletricidade foi na Era Industrial, em nossa época a Internet poderia ser equiparada tanto a uma rede elétrica quanto ao motor elétrico, em razão de sua capacidade de distribuir a força da informação por todo o domínio da atividade humana (Castells, 2004, p. 7).

Tomando a comunicação em sentido amplo, esta é concebida como um direito, garantida por legislações e declarações mundiais, a exemplo do direito à vida, à propriedade privada e à alimentação. Desse modo, a comunicação evidencia-se ao se falar em direito à liberdade de expressão e de opinião como garantia da dignidade humana (Simões, 2021).

Percebe-se então, que a comunicação, para além do processo de transmissão, constitui-se como um meio de interação entre emissor e receptor. E levando em consideração a rapidez com que os meios de comunicação evoluíram ao longo do tempo, observou-se a necessidade de implementação de leis que compreendessem o ato de comunicar-se. Isso porque, com a potencialização do fluxo informacional nas mídias digitais propiciada pelo *boom* da internet, os dados dos cidadãos foram produzidos, coletados, utilizados, reproduzidos, armazenados, avaliados e reutilizados, muitas vezes, sem o consentimento do titular (Simões, 2021).

No Brasil, a primeira legislação a tratar sobre a proteção de dados surgiu com a Lei nº 12.965 de 2014, mais conhecida como o Marco Civil da Internet (MCI), que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. (Brasil, 2014). Contudo, a lei deve acompanhar os avanços tecnológicos, culturais,

sociais, políticos e econômicos, bem como a conduta humana, no intuito de abranger e regular as novas demandas.

Posterior ao MCI, foi sancionada em 14 de agosto de 2018, pelo ex-presidente da República Federativa do Brasil, Michel Temer (MDB/SP), a Lei nº 13.709 ou Lei Geral de Proteção de Dados (LGPD), como medida para proteger os direitos fundamentais de liberdade e da privacidade individual. Esta lei disciplina sobre o tratamento de dados de pessoas físicas e/ou jurídicas, seja no âmbito público ou privado, e proporciona ao cidadão maior controle sobre seus dados, a exemplo do consentimento expresso do titular para a realização da coleta e do tratamento de dados pessoais para atender a uma finalidade específica.

Nesse sentido, a legislação supramencionada estabelecerá a aplicação de penalidades para criar um cenário de segurança jurídica, a fim de resguardar os dados pessoais dos cidadãos.

Não obstante, casos de roubo, vazamentos e/ou tratamento indevido de dados tornaram-se recorrentes, exigindo das empresas a implementação de medidas que objetivem a segurança das informações corporativas, impedindo que sejam acessadas por pessoas não autorizadas. Desse modo, considerando que as instituições armazenam uma quantidade significativa de dados pessoais e dados pessoais sensíveis, gerenciar documentos e informações tornou-se essencial.

De acordo com Schwaitzer, Nascimento e Costa (2021, p. 14):

[...] o tratamento limitado ao mínimo necessário e até o alcance das finalidades declaradas ao titular, conforme está previsto na LGPD, ocorre naturalmente quando: 1) evita-se a produção de documentos não essenciais; 2) controla-se o fluxo percorrido pelos documentos; 3) efetua-se a classificação; 4) fixa-se o prazo de guarda e 5) define-se a destinação final.

No caso das instituições de ensino, faz-se necessário a atuação do encarregado de dados- *Data Protection Officer* (DPO) como o responsável por manter a segurança da informação e assegurar que a instituição esteja em conformidade com a LGPD.

Ante a realidade exposta, o interesse pela temática surgiu ao cursar a disciplina Arquivística no 6º período do curso de Biblioteconomia, ministrada pela Prof.<sup>a</sup> Dr.<sup>a</sup> Dirlene Santos Barros, em que foram apresentados conceitos que convergem com o tema proposto, a exemplo de assuntos pertinentes à gestão de documentos e à Lei

de Acesso à Informação (LAI). Outro ponto considerado foi a vivência no campo de estágio não-obrigatório em biblioteca escolar.

Ao iniciar o processo de pesquisa bibliográfica, verificou-se que há poucos estudos e estudos de caso relacionados à LGPD e sua implementação na área educacional. Essa pesquisa foi desenvolvida em bibliotecas digitais, como a do Instituto Brasileiro de Ciência e Informação Tecnológica, Universidade Federal do Maranhão, Scielo dentre outras bibliotecas físicas. Portanto, foi desenvolvido um estudo investigativo em uma instituição de ensino particular da capital maranhense, a fim de analisar se e como a biblioteca escolar atende às disposições da lei.

Sendo a biblioteca um espaço que também realiza o tratamento de dados pessoais e dados pessoais sensíveis de seus usuários, surgiu a necessidade de verificar de que forma a biblioteca da Escola A implementou a LGPD em suas rotinas administrativas, com o propósito de garantir a privacidade e a segurança dos dados fornecidos pelos seus usuários.

Apresenta-se com objetivo geral deste estudo verificar como a biblioteca da Escola A está cumprindo a Lei Geral de Proteção de Dados desde sua implantação. Como objetivos específicos: a) descrever a história da proteção de dados e sua evolução; b) conceituar a LGPD e sua relação com a biblioteca escolar; c) caracterizar a implementação da LGPD pela biblioteca da Escola A.

A estrutura deste estudo está organizada em quatro seções, conforme segue: inicia-se pela introdução, com a contextualização do objeto de estudo, apresenta a problemática, os objetivos e a justificativa. Em seguida, a seção dois, aborda o referencial teórico, traça o conceito de privacidade e descreve o percurso da proteção de dados ao longo da história, destacando as principais legislações sobre o tema. Analisou-se também o desenvolvimento da proteção de dados brasileira e sua implementação em instituições de ensino e sua incidência em bibliotecas escolares. Na seção três, apresenta-se a metodologia utilizada para a pesquisa com a caracterização do *lócus* de estudo e caracterização da biblioteca analisada. Na quarta seção, são apresentados os resultados e discussões do assunto proposto. Na seção final, são realizadas as conclusões obtidas acerca do tema.

## 2 CONTEXTUALIZAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS: da criação à implementação no Brasil

A proteção de dados e da privacidade na internet são temas que vêm sendo amplamente discutidos ao longo do tempo nas mais diversas legislações espalhadas pelo mundo (Mendes, 2019; Menke, 2019; Doneda, 2020; Cravo; Cunda; Ramos, 2021; Crespo, 2021). Isto ocorre, em função do uso massivo de dados pessoais como recurso intangível pelas instituições, onde as legislações de proteção de dados exercem *status* ímpar no resguardo dos direitos individuais e na garantia do desenvolvimento social, econômico, político e cultural.

Importa ensejar que mediante a sociedade da informação<sup>1</sup>, fez-se necessário a criação de leis que disciplinassem a realização da coleta e do tratamento de dados, no intuito de impedir casos de roubos e vazamentos de informações pessoais, bem como, para preservar e assegurar a vida privada e o pleno desenvolvimento de cada indivíduo (Teixeira, 2020).

As primeiras legislações, também chamadas de “Leis de Primeira Geração”, tratam sobre a proteção de dados pessoais e o direito à privacidade e têm origem na União Europeia. Surgem como uma tentativa de normatizar o tratamento de informações pessoais dos cidadãos em um cenário marcado pelo final da Segunda Guerra Mundial e pelos crescentes avanços tecnológicos. São exemplos de Leis de Primeira Geração: a Lei do Land alemão de Hesse (1970), a Lei de Dados da Suécia (1973), o Estatuto de Proteção de Dados alemão de *Rheinland-Pfalz* (1974) e a Lei Federal de Proteção de Dados da Alemanha (1977) (Mendes, 2019).

De acordo com Lugati e Almeida (2020), a primeira geração de leis insere-se no contexto da primeira fase do Estado Moderno<sup>2</sup>, posto que essa forma de organização política era capaz de controlar a conduta de seus integrantes, por meio da centralização na monarquia, ou seja, no Estado. As leis de primeira geração propunham-se a regular um cenário marcado pelo armazenamento e centralização de dados em grandes computadores. Desse modo, não havia, portanto, a

---

<sup>1</sup> Nesta pesquisa adotaremos a concepção de Sociedade da Informação por concebê-la como “[...] uma nova era em que a informação flui a velocidades e em quantidades há apenas poucos anos inimagináveis, assumindo valores sociais e econômicos fundamentais [...]” (Takahashi, 2000, p.3). Essa sociedade está relacionada ao desenvolvimento das Tecnologias de Informação, enquanto que a Sociedade do Conhecimento, pressupõe o desenvolvimento social, político, institucional e cultural.

<sup>2</sup> Sobre o surgimento do Estado Moderno, a maioria dos historiadores considera o século XVI como o seu aparecimento, iniciado, primeiramente, na Itália (Florenzano, 2007).

descentralização de dados, tais como comumente acontecem atualmente, o que só foi possível através da popularização da internet na década de 90, também conhecida como o “boom da internet”.

Sob a perspectiva de Lugati e Almeida (2020), considerando o ordenamento jurídico, as legislações certificam que os dados pessoais dos indivíduos podem sim, ser objeto de tutela jurídica, por entender que o Estado irá garantir a preservação das informações coletadas.

E é na Alemanha que emerge a primeira lei formal de proteção de dados do mundo, a chamada Lei de Hesse (*Hessisches Datenschutzgesetz*), lei federal promulgada em 1970 no estado alemão de Hesse, cujo objetivo era:

[...] tratar com maior cuidado as informações pessoais de indivíduos armazenadas em meios eletrônicos. A lei, assim, foi pioneira ao tratar da coleta e tratamento de dados de indivíduos, ainda que não o fizesse de maneira objetiva e segmentada (Monteiro et al., [s.d.], p. 7).

Dessa forma, observa-se que a Lei de Hesse foi uma iniciativa de resguardar os dados pessoais no âmbito eletrônico, contudo, não garantiu aos cidadãos a segurança das informações armazenadas, mediante a ausência de diretrizes que dispusessem sobre o tratamento das informações coletadas, bem como a finalidade para a qual seriam utilizadas.

O Estado, por sua vez, tinha a pretensão de criar um censo que seria utilizado para coletar e controlar os dados pessoais dos cidadãos. O texto previa que em 1983 seria feito um censo demográfico por funcionários estatais para coletar dados relativos aos habitantes do país (Assmann, 2014).

De acordo com Florês e Silva (2020, p. 5), essa iniciativa tinha como objetivo:

[...] criar um censo que continha 160 (cento e sessenta) perguntas de cunho pessoal, voltadas à obtenção de dados referentes à vida profissional, ideologias políticas e crenças religiosas, informações que seriam confrontadas com dados contidos no registro civil. Quem não respondesse a esse censo estaria sujeito à multa, além de existir a possibilidade de os dados dessas pessoas serem encaminhados às autoridades federais.

Precederam-se assim, inúmeras discussões e reclamações dos cidadãos ante à lei de recenseamento alemã, visto à exposição dos indivíduos, o sentimento de insatisfação e a criação de um “Estado superinformado”, posto que os cidadãos não tinham instrumentos que defendessem seus interesses próprios face à coleta e à utilização de dados pessoais e dados pessoais sensíveis por terceiros sem prévio consentimento.

No entanto, a Corte alemã considerou inconstitucional o caso do censo demográfico, editado em 1982, também denominado como *Volkszählungsurteil*, por julgar procedentes as reclamações dos cidadãos, sob a justificativa de invasão à privacidade, incidindo em uma liberdade negativa, não possibilitando aos sujeitos autonomia para determinar como seria realizada a utilização de seus dados pessoais (Assmann, 2014).

Cabe ressaltar que essa decisão (BVerGE- *Bundesdatenschutzgesetz*) aprovada tanto pelo Parlamento, quanto pelo Conselho Federal foi um verdadeiro marco no que tange à proteção de dados. Ainda assim, levando em consideração os aspectos apontados, prosseguiu-se com a realização do censo demográfico com algumas alterações em seu texto, resguardando a proteção de dados dos cidadãos entrevistados, desautorizando a coleta de dados específicos, a exemplo de nome e endereço, bem como a transferência dessas informações a outros órgãos governamentais (Flôres; Silva, 2020).

Nesse contexto, surge, na Alemanha, o conceito da *autodeterminação informativa* (*informationelle Selbstbestimmung*) que garante aos indivíduos a decisão sobre a utilização de seus dados pessoais, com a capacidade de consentir quando e como seus dados deverão ser conhecidos. Interessante ressaltar que, esse termo se desenvolve tanto na doutrina, quanto na jurisprudência como um fundamento da proteção de dados pessoais, o qual permite ao indivíduo e às instituições públicas assegurar o exercício de boas práticas no tratamento de dados baseados nos valores da cidadania, democracia e liberdade (Hartmann et al., 2021).

Posterior à Lei de Hesse, foi aprovada em 1973, na Suécia, a primeira lei de proteção de dados em âmbito nacional, a *Sw. Datalagen* ou o Ato de Dados Sueco. Assim, como a Lei de Hesse, a lei sueca tratava a proteção de dados de forma mais abrangente, não considerando princípios para o tratamento de dados, dispondo somente que a coleta das informações deveria ser realizada com a anuência da agência governamental competente (Monteiro et al., 2020).

Seguindo a evolução histórica, no ano de 1974, surge o Estatuto de Proteção de Dados alemão do estado da Renânia- Palatinado, o qual foi idealizado como um recenseamento demográfico com o propósito de extrair e controlar as informações da população (Flôres; Silva, 2020). Nesse mesmo ano, nos Estados Unidos, adotada pela doutrina norte-americana, decretou-se a Lei de Privacidade (*Privacy Act*), que assim como as demais “[...] limitava o uso, tratamento e armazenamento dos dados e

informações pessoais dos indivíduos pelas agências do governo americano” (Burille, 2022, p. 8).

Em 1977, é implementado a *Bundesdatenschutzgesetz* (BDSG), Lei Federal da República Federativa da Alemanha sobre proteção de dados pessoais em âmbito nacional. Esta lei possui um texto analítico de 47 artigos, os quais são subdivididos em seis seções. A BDSG abrange de forma ampla a proteção de dados pessoais, buscando contemplar situações que porventura possam ocorrer, visto a dinamicidade da sociedade (Burille, 2022).

De acordo com o Art. 1º, inciso I, do conteúdo legal da BDSG, “A proteção dos dados tem por tarefa impedir danos a bens dignos de tutela pelo sujeito interessado, protegendo os dados relativos à sua pessoa de abusos na memorização, transmissão, modificação e cancelamento” (Losano, 1981, p.16).

Evidencia-se assim, o poder de tutela que a BDSG apresenta como forma de assegurar aos cidadãos a proteção de dados, o direito de correção e exclusão dos dados armazenados, de informação para qual a finalidade os dados foram coletados, e aplicação de sanções em caso de inobservância às disposições da lei (Assmann, 2014).

Essas legislações marcam a primeira geração da evolução das leis de proteção de dados, cujo objetivo era o consentimento prévio do titular para a criação de um banco de dados governamental, o qual seria regulamentado pelos órgãos públicos para controle de dados. No entanto, gerou-se uma preocupação com o tratamento das informações obtidas, visto que o foco não era prioritariamente resguardar a privacidade e os direitos fundamentais dos indivíduos. (Flôres; Silva, 2020).

Desse modo, observa-se que nessa época, várias leis acerca da proteção de dados foram implementadas na Alemanha, e conforme explica Gasiola (2019, p. 1):

[...] são reações a projetos estatais para implementar bancos de dados centralizados sobre a população, em meio à euforia tecnológica que marcou o pós-guerra. O choque entre a recente lembrança (ou presença) dos governos autoritários e a iminência de tais projetos levou ao reconhecimento expresso da proteção de dados perante as pretensões públicas de aumentar seu poder informacional. O objetivo dessas leis era, acima de tudo, estabelecer limites e garantir a transparência na criação de bancos de dados.

Portanto, essa conjuntura ensejou a segunda geração de leis de proteção de dados, atribuindo ao usuário a participação no processo de tratamento das informações, no que se refere ao consentimento de dados coletados para determinada

finalidade. Dentre estas fases, incluem-se a coleta, o uso e o compartilhamento de dados pessoais (Lugati; Almeida, 2020).

Esse segundo momento suscita uma mudança no âmbito jurídico, uma vez que descentraliza a figura do “*Big Brother*”<sup>3</sup>, ou seja, uma base de dados do Estado, para várias bases de dados tanto estatais como privadas, caracterizando o que se pode denominar de “Pequenos Irmãos”. Todavia, o compartilhamento de informações pessoais tornou-se necessário e indispensável para a vida em sociedade (Andrade et al, 2023).

Tal fato é corroborado por Mendes (2019) que aponta uma controvérsia entre a efetividade do consentimento que o cidadão possui e a liberdade de escolha de compartilhamento de dados, visto que por estar inserido na sociedade, muitas vezes a não disponibilização das informações ocasiona a sua exclusão social. Dessa forma, em certas ocasiões, o cidadão, a fim de usufruir de determinado serviço do mercado de consumo, sujeita-se a conceder as suas informações pessoais.

Nota-se desta forma, a inviabilidade do consentimento absoluto do titular em relação à utilização de seus dados, haja vista que há uma desconformidade entre as partes do fluxo de informação que impedem que o indivíduo tenha controle e conhecimento absolutos do tratamento de seus dados (Cravo; Cunda; Ramos, 2021).

Cabe ressaltar que, dentre as Leis de Segunda Geração, pode-se citar a Constituição Portuguesa e a Constituição Espanhola, cujo foco principal era identificar a utilização indevida dos dados pessoais dos cidadãos (Flôres; Silva, 2020). Nesse sentido, a Constituição Espanhola em seu Art. 18, inciso IV, dispõe sobre os limites de uso da informática, garantindo aos seus cidadãos a inviolabilidade da honra, intimidade pessoal e familiar, bem como o pleno exercício de seus direitos (Espanha, 1978).

A Constituição Portuguesa, por sua vez, no Art. 26, inciso I de seu ordenamento jurídico, assiste aos seus cidadãos os seguintes direitos pessoais:

1. A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à

---

<sup>3</sup> Traduzindo para o português, a figura do “Grande Irmão” surge na obra de George Orwell intitulada 1948, como um retrato de um estado totalitário, marcado pela tirania, invasão de privacidade e da liberdade humana, bem como do controle estatal. Traz também reflexões acerca da necessidade de proteção de dados pessoais numa sociedade marcada pela vigilância massiva e opressão do Estado. Esta expressão também pode ser remetida ao programa de entretenimento “Big Brother”, cujas características são marcadas pela ausência de privacidade, uma vez que os participantes estão sob exposição e vigilância de múltiplas câmeras 24 horas por dia, além do controle da produção televisiva (Andrade et al, 2023).

cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação (Portugal, 1976).

O Art.º 70 do Código Civil Português, em seus incisos I e II, que trata da Tutela Geral da Personalidade, conferem aos seus cidadãos maior grau de proteção do ordenamento jurídico, resguardando direitos fundamentais, possuindo como base a dignidade da pessoa humana.

1. A lei protege os indivíduos contra qualquer ofensa ilícita ou ameaça de ofensa à sua personalidade física ou moral.
2. Independentemente da responsabilidade civil a que haja lugar, a pessoa ameaçada ou ofendida pode requerer as providências adequadas às circunstâncias do caso, com o fim de evitar a consumação da ameaça ou atenuar os efeitos da ofensa já cometida (Portugal, 1966).

Paralelo à crescente evolução das tecnologias, ocorre o avanço das legislações para as Leis de Terceira Geração, cuja preocupação é a tutela do direito à privacidade, não somente do ponto de vista do consentimento, mas da garantia da efetividade deste direito. Nesta nova fase, a participação do indivíduo em todo o processo do tratamento de dados se amplia, configurando o conceito da “autodeterminação informativa”.

De acordo com Mendes (2019), esta geração é assinalada pela decisão do Tribunal Constitucional alemão de 1983, que tornou inconstitucional parte da Lei do Censo (lei de primeira geração). O veredito do tribunal partiu da reinterpretação da Lei Federal de Proteção de Dados Pessoais sob a égide da Lei Fundamental de Bonn. Esta lei possibilitou reflexões significativas, tomando por base os valores fundamentais da pessoa humana.

Na atual conjuntura tecnológica, a localização dos bancos de dados antes física, deu lugar ao armazenamento em redes, podendo agora, os dados serem processados e transferidos em curto período de tempo. São exemplos de Leis de Terceira Geração as leis dos Estados alemães, a Emenda à Lei Federal de Proteção de Dados Pessoais Alemã (1990), a Emenda da Lei da Áustria (1986), a alteração da Lei da Noruega e a previsão constitucional da proteção de dados pessoais da Holanda (Mendes, 2019).

Com o advento da quarta geração iniciada em 1990 com a reunificação da Alemanha<sup>4</sup>, buscou-se resolver as lacunas de proteção deixadas pelas legislações anteriores por meio de duas soluções: a primeira, fortalecer as normas jurídicas para permitir o autocontrole dos indivíduos sobre seus dados pessoais; e a segunda, retirar do controle do indivíduo determinadas questões, por entender que temas relativos aos dados pessoais sensíveis como etnia, orientação sexual, opinião política e religião deveriam ser altamente protegidos, haja vista a potencialidade que esses dados têm de suscitar a discriminação (Mendes, 2019).

Neste momento, o enfoque é equilibrar de um lado a posição do titular dos dados e do outro as entidades, organizações e quaisquer outras instituições que realizam o tratamento de dados pessoais, conferindo ao indivíduo o poder de consentimento ou não, bem como o compartilhamento de seus dados durante esse processo.

A Diretiva 95/46/CE do Parlamento Europeu e do Conselho Europeu (CE), de 24 de outubro de 1995 é um exemplo da quarta geração de leis de proteção de dados, que tinha como objetivo “[...] uniformizar a coleta, o tratamento e uso dos dados pessoais pelos estados-membros da União Europeia, servindo também como referência para países não membros” (Silva, 2019, p.16).

Essa diretiva, estruturada sob os moldes europeus, apresenta em seu escopo 72 considerações, com vistas a uniformizar a legislação, estabelecendo além da proteção, o livre fluxo da informação e diretrizes tanto para o tratamento de dados (*data controllers*<sup>5</sup>), quanto para o titular dos dados.

No que se refere às diretivas, estas devem ser também aplicadas à legislação interna dos estados-membros. Cada país possui um prazo para fazer a sua respectiva adaptação, também chamada de “transposição”. E em caso de morosidade de adequação, o país pode responder perante a Corte Europeia de Justiça.

Em 2013, passou-se a discutir a elaboração de uma nova lei de proteção de dados na união Europeia mediante o escândalo de vazamento de dados, desencadeados por Edward Snowden, ex-funcionário da Agência de Segurança Nacional Norte-Americana (*National Security Agency*- NSA, na sigla em inglês).

---

<sup>4</sup> Processo de unificação do território nacional alemão em outubro de 1990, o qual foi dividido em 1949, no contexto da Guerra Fria, em dois países: República Democrática Alemã (oriental e comunista) e República Federal da Alemanha (ocidental e capitalista). A reunificação ocorreu após tratados de cooperação e a queda do Muro de Berlim em 1989 (Badia, 1997).

<sup>5</sup> Termo utilizado para designar os controladores de dados.

Snowden trabalhou como assistente técnico da Central de Inteligência Americana (CIA), e nos anos posteriores exerceu atividades em empresas privadas de inteligência para a NSA e, no início de 2013, assumiu um posto na *Bozz Allen Hamilton*- instituição ligada à Agência Norte Americana no Havaí. Durante este período, ele realizou o *download* de documentos secretos da CIA e de parceiros internacionais, compilou e compartilhou as informações coletadas com o jornalista Greenwald e com a cineasta Laura Poitras, cuja finalidade era denunciar a NSA de espionagem e, conseqüentemente, a violação do direito à privacidade de milhões de usuários ao redor do mundo (Assmann, 2014).

Após a publicação das notícias, Snowden foi acusado de espionagem pelo governo norte-americano e teve seu passaporte revogado. Logo após, viajou para Moscou, na Rússia, onde aguardou o pedido de asilo político por mais de 20 países. Desde então, mora na Rússia depois de ter recebido o aceite temporário (Pilati; Olivo, 2014).

Este caso iniciou debates sobre a invasão do direito à privacidade e à violação de direitos humanos, trazendo à tona desdobramentos sobre a atual conjuntura da sociedade diante do desenvolvimento tecnológico de coleta de dados. Essa investigação revelou, a nível mundial, um esquema de vigilância promovido pelos EUA. Isso mostra que, ao mesmo tempo em que a coleta de dados se faz importante para garantir a segurança e organização social, evidencia o lado maléfico, à exemplo de comportamentos invasivos que violem a privacidade (Olmos; Favera, 2016).

Outro episódio semelhante diz respeito ao site *Wikileaks*<sup>6</sup> e ao seu fundador australiano Julian Assange, responsável pelo vazamento de documentos sigilosos do governo norte-americano divulgados na plataforma, comprovando a participação norte-americana na prática de crimes de guerra. Em novembro de 2010, Assange foi acusado de ter cometido abuso sexual contra duas mulheres na Suécia, recebendo da Procuradoria-Geral do país um mandado de detenção europeu, preso por policiais britânicos em dezembro de 2010. Em maio de 2012, a Suprema Corte entendeu que Assange deveria ser entregue à Suécia. Neste mesmo mês, é solto após pagamento de fiança. Antes de iniciar os trâmites para sua extradição, busca refúgio na Embaixada do Equador em Londres, onde ficou até sua prisão em 2019. Em abril deste mesmo ano, teve seu asilo político cancelado pelo presidente do Equador.

---

<sup>6</sup> Fundada em 2016, é uma organização sem fins lucrativos sediada na Suécia, especializada na publicação de documentos censurados ou restritos.

Desde então, Assange está detido na prisão de segurança máxima em Belmarsh. Ele é acusado por 18 crimes e pode ser condenado a 175 anos de prisão (Silva, 2016).

Para Melo (2011), a plataforma Wikileaks propunha-se a investigar e tornar público os acontecimentos em voga no mundo. Tais casos evidenciam ainda, a prática de espionagem norte-americana em outros países ao redor do mundo. De acordo com a autora:

[...] Assange tinha por hábito não dormir duas vezes no mesmo lugar para não dar entrevistas e não ser sequestrado. Ele foge, assim, do perfil tradicional de empresário de mídia, assumindo um papel de ativismo político, ou seja, retomando sentidos da prática do jornalismo clássico. Aliás, o site não é, por natureza, uma empresa com fins lucrativos: em quatro anos de existência, o WikiLeaks atraiu doadores privados anônimos como meio de garantir a sua sobrevivência e pôs no ar cerca de um milhão de documentos. Entre eles, as condições de presos em Guantánamo e a morte de jornalistas da Reuters por soldados norte-americanos em Bagdá. É, enfim, fruto do ideal de fazer fluir as informações (Melo, 2011, p. 263).

A privacidade, portanto, como um direito de personalidade do indivíduo, inerente à condição humana, ao longo do tempo, sofre modificações e adaptações em virtude do desenvolvimento social e político, ao passo em que as novas tecnologias da informação e comunicação evoluem, desencadeando mudanças no comportamento da sociedade vigente.

Acerca do conceito de *privacy* (privacidade), uma das possíveis doutrinas para sua origem surge nos Estados Unidos em 15 de dezembro de 1890, com a publicação do artigo de Samuel Warren e Louis Brandeis<sup>7</sup>, intitulado “*The right to privacy*”, que trata sobre o direito à privacidade. Este conceito surgiu depois que as informações pessoais de familiares de Samuel Warren foram expostas sem o consentimento do titular dos dados. A partir daí, Warren juntamente com Louis Brandeis deram início a essa doutrina, cujo principal aspecto era defender “o direito de estar só” (*right to be alone*), com o intuito de possibilitar ao indivíduo o controle sobre suas informações pessoais, sem a intromissão de terceiros. Desse modo, encontrou-se na doutrina um meio de conter a intrusão das tecnologias no direito de personalidade, a exemplo da câmera fotográfica e a exposição da imagem do indivíduo (Pilati; Olivo, 2014).

---

<sup>7</sup> Samuel Warren e Louis Brandeis escreveram o artigo “*The right to privacy*” quando eram sócios na advocacia, ambos cursaram Direito na *Harvard Law School*. Anos depois, Brandeis tornou-se ministro da Suprema Corte dos Estados Unidos.

Seguindo essa linha do tempo, em 27 de abril de 2016, surge o novo Regulamento (EU) 2016/679, denominado Regulamento Geral de Proteção de Dados (*General Data Protection Regulation*- GDPR), revogando a Diretiva Europeia 95/46/CE, contudo mantendo os princípios estabelecidos. Este regulamento abrange de forma mais completa a proteção de dados pessoais, influenciando inclusive, outras legislações internacionais, a exemplo do Brasil, que se inspirou na GDPR para a criação, em 2018, da Lei Geral de Proteção de Dados (LGPD) (Burille, 2022).

Este novo modelo europeu, que começou a ser idealizado no ano de 2012, ressalta a importância do consentimento, sendo este termo utilizado frequentemente ao longo do texto constitucional, e caracterizado diversas vezes como “de livre vontade”, “explícito”, “informado” e “inequívoco”. Destaca ainda, o princípio da autodeterminação informativa, conferindo ao indivíduo autonomia na participação no processo de tratamento de dados.

Segundo Pinheiro (2018), é importante lembrar que, a aplicabilidade deste regulamento contempla cidadãos e não cidadãos da União Europeia, bem como à prestadora de serviços, empresas, organizações e instituições, sejam elas de âmbito público ou privado. E tem como objetivo disciplinar a proteção de dados pessoais, no tocante à realização do tratamento dos dados e a sua livre circulação, também conhecida pela expressão “*free data flow*”<sup>8</sup>.

Embora tenha sido aprovada em 2016, o regulamento previu que dentro de dois anos, os países membros deveriam se adequar à GDPR, para assim, iniciar a aplicação de penalidades, o que só foi possível a partir de 2018. Para Pinheiro (2018, p. 8), o regulamento:

[...] ocasionou um ‘efeito dominó’, visto que passou a exigir que os demais países e as empresas que buscassem manter relações comerciais com a UE também deveriam ter uma legislação de mesmo nível que o GDPR. Isso porque o Estado que não possuísse lei de mesmo nível passaria a poder sofrer algum tipo de barreira econômica ou dificuldade de fazer negócios com os países da UE. Considerando o contexto econômico atual, esse é um luxo que a maioria das nações, especialmente as da América Latina, não poderia se dar.

Cabe observar que, no Art. 5º do GDPR da UE, consagra-se sete (7) princípios do tratamento de dados pessoais, a saber:

- a) **princípio da licitude, lealdade e transparência:** o tratamento de dados pessoais de pessoas físicas deve ser realizado com observância à legalidade

---

<sup>8</sup> Este termo refere-se à livre circulação de dados.

dos dados e a comunicação ao titular sobre a finalidade e utilização das informações coletadas;

- b) **princípio da limitação das finalidades**: os dados pessoais coletados devem atender às finalidades para as quais foram fornecidas, não devendo ser tratadas para outros fins;
- c) **princípio da minimização dos dados**: os dados devem ser tratados e limitados necessariamente para determinada finalidade específica;
- d) **princípio da exatidão**: deve-se zelar pela exatidão e atualidade dos dados recolhidos, cabendo ao titular dos dados a iniciativa de requerer a exclusão ou retificação das informações fornecidas;
- e) **princípio da limitação da conservação**: os dados pessoais devem ser conservados apenas pelo prazo necessário para a consecução das finalidades a que se destinam, e após cumprimento do período, deverão ser eliminados, exceto quando se destinarem para fins de investigação científica, história ou estatística;
- f) **princípio da integridade e confidencialidade**: aos dados pessoais deve-se garantir a proteção contra tratamentos indevidos, ilícitos ou não autorizados, assim como a adoção de medidas que assegurem a integridade e o direito à privacidade dos dados armazenados.
- g) **princípio da responsabilidade**: os responsáveis pelo tratamento de dados pessoais devem agir em conformidade com a lei.

Face a isso, o Regulamento Geral de Proteção de Dados europeu trouxe importantes contribuições que não foram contempladas nas legislações anteriores. Destaca-se aqui, a figura do indivíduo como elemento principal no processo de tratamento e fluxo de informação da sociedade. A seguir, investiga-se como essa evolução do direito à privacidade se deu no ordenamento jurídico brasileiro.

## **2.1 A construção histórica da LGPD no Brasil: ordenamento jurídico antecedente à LGPD no Brasil**

O tratamento de dados pessoais tem sido um tema amplamente discutido nas esferas públicas e privadas, tendo em vista o desenvolvimento tecnológico e o crescente fluxo de informação. Surge então, a necessidade de assegurar a proteção

de dados que são coletados e compartilhados no mercado de consumo. Ao realizar a aquisição de bens e serviços, evidencia-se muitas vezes, a hesitação do usuário em fornecer informações de cunho pessoal mediante a insegurança na manutenção da privacidade de seus dados.

A Lei nº 13.709/2018, de caráter geral e transversal, dispõe de objetivos, fundamentos e princípios que devem ser observados em toda e qualquer atividade que envolva o tratamento de dados. Ressalta que várias dessas disposições têm peso no que diz respeito às decisões automatizadas balizadas no tratamento de dados pessoais.

Em linha cronológica, o primeiro instrumento que trata a proteção de dados no Brasil é a Constituição Federal de 1988 (CF/88) que dispõe sobre direitos fundamentais humanos e sua inviolabilidade, liberdades básicas, inclusive o direito de personalidade do indivíduo (Silva, 2019). Em seu Art. 1º, reconhece a proteção como direito fundamental e que necessita ser garantido pelo Estado, visto que a dignidade da pessoa humana é soberana da República Federativa do Brasil, como se deixa entrever na transcrição abaixo:

CF/88, Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos:

I - a soberania;

II - a cidadania;

III - a dignidade da pessoa humana;

IV - os valores sociais do trabalho e da livre iniciativa;

V - o pluralismo político.

Parágrafo único. Todo o poder emana do povo, que o exerce por meio de representantes eleitos ou diretamente, nos termos desta Constituição (Brasil, 1988).

Observa-se que no Art. 5º, inciso X, a lei assegura a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas, bem como de penalidades cabíveis em caso de violação de direitos. O inciso IX, por sua vez, destaca a liberdade de expressão do cidadão, e o inciso XIV, garante o acesso à informação e o sigilo da fonte quando assim o julgar necessário (Brasil, 1988).

Importante ressaltar a relação dialógica com a Lei de Acesso à Informação, conhecida como LAI, nº 12.527/2011, na garantia da transparência que deve orientar toda relação entre o responsável pelo tratamento de dados pessoais e o titular dos dados, de forma a garantir o acesso aos seus dados pessoais.

Outra garantia constitucional presente no rol de direitos fundamentais diz respeito ao *habeas data* que determina no Art. 5º, inciso LXXII, *in verbis*<sup>9</sup>:

LXXII - conceder-se-á "*habeas-data*":

- a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
- b) para a retificação de dados, quando não se prefera fazê-lo por processo sigiloso, judicial ou administrativo (Brasil, 1988).

O *habeas data*, enquanto instrumento processual, assegura ao cidadão o direito de conhecer as informações relativas a sua pessoa, estejam elas armazenadas em registros, fichários, bancos de dados de entidades governamentais ou de caráter público, destacando-se como objeto de proteção constitucional (Mendes, 2019).

No plano infraconstitucional, o Código de Defesa do Consumidor (CDC), Lei nº 8.078/1990, surge como a primeira lei a tratar da privacidade e da proteção de dados pessoais, considerando as novas tecnologias de processamento de dados.

Esse conjunto de normas trouxe em seu bojo mudanças significativas na jurisdição brasileira, reconhecendo o consumidor como parte vulnerável das relações de consumo. Deste modo, buscou estabelecer alguns princípios, tais como: o princípio da devida informação, princípio da indisponibilidade de direitos, princípio da liberdade de escolha, princípio do equilíbrio, princípio da boa-fé objetiva e princípio da vulnerabilidade (Assmann, 2014).

Já no Art. 43º da referida lei, disciplina-se acerca dos bancos de dados e cadastros de consumidores, assegurando aos titulares dos dados o direito de ser informado sobre o acesso às informações fornecidas. Além disso, exige que os meios de coleta (cadastros e dados) sejam redigidos de forma clara, objetiva, verídica e de fácil compreensão. Nesse ponto, o consumidor tem o direito de impetrar o remédio constitucional "*habeas data*" para acessar seus registros pessoais (Silva, 2019).

No tocante às sanções, o CDC prevê nos Arts. 73º e 74º, a aplicação de sanções, respondendo pelas infrações penais aqueles que porventura tentarem impedir ou dificultar informações armazenadas nos instrumentos de coleta de dados ou mesmo deixar de retificar quaisquer dados. *In verbis*:

Art. 72. Impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros: Pena – Detenção de seis meses a um ano ou multa.

---

<sup>9</sup> Expressão latina usada para citar nos termos em que foi escrito.

Art. 73. Deixar de corrigir imediatamente informação sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata: Pena – Detenção de um a seis meses ou multa (Brasil, 1990).

Por fim, observa-se a preocupação do legislador em garantir a máxima proteção à privacidade do consumidor (autodeterminação informativa), abrangendo todos e quaisquer tipos de bancos de dados que realizem o tratamento de dados pessoais e, conseqüentemente, atinjam o livre desenvolvimento da personalidade humana. O *Habeas Data* também possui regulamentação própria na forma da Lei nº 9.507 de 12 de novembro de 1997.

Com a promulgação da Lei nº 10.406 de 10 de janeiro de 2002, estabeleceu-se o Código Civil Brasileiro (CCB) que assegura os direitos e deveres de personalidade, considerando todas as relações pertinentes à vida humana em todas as suas nuances, resguardando seus valores existenciais.

Sendo o CCB, considerado como uma das leis primordiais do ordenamento jurídico brasileiro, rege em sua amplitude assuntos relativos à esfera privada das pessoas. Conforme o Art. 21º da supracitada lei: “A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma [...]” (Brasil, 2002).

Tal preceito incide na proteção de dados pessoais, que de forma indireta, outorga ao juiz a adoção de medidas que impeçam a violação da privacidade do cidadão.

Em sentido amplo, observa-se no CCB, a valorização da condição humana e o indivíduo como foco central desta lei, trazendo em seu escopo direitos e deveres, regidos pela justiça, ética e preservação da igualdade entre os cidadãos.

Essa é a tendência também seguida pelo Código Civil de 2002 (CC/02), que se desprende da visão patrimonialista e coloca em foco a pessoa e suas relações, de modo que, numa perspectiva Kantiana, o indivíduo é um fim em si mesmo e deve respeitar à comunidade em que se insere. Dessa perspectiva, emergem princípios como o de solidariedade e função social (Lugati; Almeida, 2020, p.16).

Outra norma que passa a dispor sobre o tratamento da privacidade e da proteção de dados pessoais é a Lei do Cadastro Positivo, publicada em 09 de junho de 2011, alterada pela Lei Complementar nº 166/2019, que disciplina a formação e consulta a banco de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas para a formação de histórico de crédito.

Esta lei exige do titular dos dados consentimento expresso para que seja realizado o tratamento de dados, fato que não era contemplado no Código de Defesa do Consumidor, posto que havia apenas o ato de notificação aos cidadãos (Mendes, 2019).

Tal fato é corroborado no Art. 5º da Lei do Cadastro Positivo que dispõe sobre os direitos do cadastrado, requerendo do titular dos dados prévia autorização para abertura de cadastro mediante assinatura em dispositivo específico:

Art. 5º São direitos do cadastrado:

I - obter o cancelamento do cadastro quando solicitado;

II - acessar gratuitamente as informações sobre ele existentes no banco de dados, inclusive o seu histórico, cabendo ao gestor manter sistemas seguros, por telefone ou por meio eletrônico, de consulta para informar as informações de adimplemento;

III - solicitar impugnação de qualquer informação sobre ele erroneamente anotada em banco de dados e ter, em até 7 (sete) dias, sua correção ou cancelamento e comunicação aos bancos de dados com os quais ele compartilhou a informação;

IV - conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial;

V - ser informado previamente sobre o armazenamento, a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários dos dados em caso de compartilhamento;

VI - solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados; e

VII - ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados. (Brasil, 2011).

Sendo assim, configura-se o cadastro positivo como um banco de dados, cujas informações são relativas às operações de créditos de pessoas físicas e jurídicas, e que servem para a elaboração de um histórico de crédito. A partir dos dados coletados é possível analisar e traçar o perfil do consumidor e oferecer condições comerciais, créditos e taxas mais adequadas a cada um. Em suma, a Lei do Cadastro Positivo objetiva beneficiar os consumidores, garantindo que as informações fornecidas devem ser utilizadas para finalidades específicas, a exemplo de análise para concessão de crédito bancário (Lugati; Almeida, 2020).

Cabe ressaltar que a lei supracitada converge com o proposto pelo CDC ao prever que no momento de formação do banco de dados, as informações armazenadas devem ser claras, objetivas, verídicas e de fácil compreensão, a fim de possibilitar uma averiguação precisa e segura da situação econômica do indivíduo cadastrado.

Posterior a essa lei, em 30 de novembro de 2012 foi sancionada pela ex-presidente da República Federativa do Brasil, Dilma Rousseff, a Lei nº 12.737, também conhecida popularmente como “Lei Carolina Dieckmann”. Esta lei surgiu depois da repercussão envolvendo o nome da atriz brasileira Carolina Dieckmann, por esta ter sua intimidade violada em meios digitais.

Os sistemas informáticos não são mais sistemas restritos quanto a seu acesso e a troca de dados pode ocorrer entre diversos lugares por meio de diversos computadores. Diante dessa troca cada vez mais frequente, a intimidade do usuário está cada vez mais passível de sofrer algum tipo de violação. A maior causa de ameaça à intimidade é a própria ausência de conhecimento de quem a utiliza e pela falta de transparência por parte dos agentes que compõem o meio cibernético. (Bezerra, 2022, p. 55).

A vítima em questão sofreu ameaças para evitar a exposição, contudo teve 36 (trinta e seis) de suas fotos íntimas divulgadas nas redes sociais após seu computador passar por assistência técnica. Essa violação enquadra-se como crime cibernético e delitos informáticos, caracterizada pela invasão de privacidade, uma vez que os dados pessoais da vítima estavam armazenados em um dispositivo informático de caráter privado. Tal prática criminal transgride todos os princípios consagrados na CF/1988, a exemplo do direito à liberdade, à vida, à igualdade, à propriedade, à segurança e, sobretudo, à inviolabilidade humana (Bezerra, 2022).

Diante do fato, criou-se esta lei para amparar as pessoas vítimas de crimes virtuais, pois na época não havia uma legislação específica que dispusesse sobre a penalização para tais crimes. Com o advento da lei, aplica-se aos criminosos conforme o Artigo 154º, § 3º, acerca da invasão de dispositivos informáticos, a pena de reclusão de seis meses a dois anos, acrescido de multa, caso a conduta do crime não seja enquadrado na sua forma mais grave (Silva, 2019).

No contexto da evolução das normas brasileiras, na busca pela garantia do acesso à informação pública, surge a Lei nº 12.527 de 2011, LAI, cuja ementa regula o acesso a informações previsto no inciso XXXIII do Art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.

Esta lei determina os procedimentos de transparência pública a serem observados pelos entes federativos do Brasil, no intuito de garantir aos cidadãos o acesso à informação. Sabe-se que para cumprir as exigências da sociedade, faz-se

necessário que as informações dos atos e decisões públicas administrativas sejam de livre conhecimento para o exercício da cidadania.

Em uma sociedade democrática, a informação é um valioso bem que deve ser conduzido segundo os princípios constitucionais da publicidade e da moralidade. Desse modo, a LAI objetiva fazer com que o Poder Público atue com transparência na realização da coleta de dados que sejam de seu interesse.

Assim sendo, esta lei estabelece que toda e qualquer pessoa, seja ela física ou jurídica, obtenha informações de órgãos e entidades públicas, partindo do ponto de que o acesso à informação é um direito constitucional e humano. O Estado, por sua vez, tem a obrigação de dar transparência aos documentos e informações nos canais de comunicação dos entes públicos (Silva, 2019).

A LAI em consonância com o disposto no Art. 5º, inciso XIV, da CF/88, estabelece que “[...] é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional.” (Brasil, 1988). Nesse sentido, dados relativos à personalidade humana devem ser observados com a máxima cautela, pois, devem resguardar a intimidade, a privacidade e a confidencialidade das informações.

Será restringido o acesso às informações classificadas como sigilosas, ou seja, aquelas cuja divulgação possa colocar em risco a segurança da sociedade (vida, segurança, saúde da população) ou do Estado (soberania nacional, relações internacionais, atividades de inteligência). Por isso, apesar de serem públicas, o acesso a elas deve ser restringido por meio da classificação da autoridade competente (Silva, 2019, p.44).

Desta forma, faz-se necessário equilibrar a transparência das informações públicas e a proteção de dados pessoais. Portanto, tem-se a publicidade como regra, e o sigilo como exceção. Lugati e Almeida (2020) fazem importantes considerações sobre os limites entre o público e o privado, entre o que deve ser publicizado e o que deve ser resguardado.

Acerca da classificação da informação relacionada ao grau e prazos de sigilo, conforme o risco que possa oferecer à soberania da sociedade ou do Estado, aplica-se à informação os seguintes graus: ultrassecreta, secreta ou reservada. Às informações ultrassecretas é atribuído o prazo de 25 anos; às informações secretas 15 anos; e às reservadas, 5 anos, podendo todas essas classificações serem renovadas, por igual prazo, por mais uma vez. Após transcorridos os prazos mencionados, a informação torna-se de livre conhecimento.

Contudo, quando se trata de informações pessoais, relativas à intimidade, vida privada, honra e imagem, o Art. 31º, inciso I e II, estabelece, *in juris*:

- I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e
- II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem. (Brasil, 2011)

Para além destas, há ainda outras previsões constitucionais de hipóteses de sigilo, as quais são amparadas por outras legislações, a exemplo do sigilo bancário, fiscal e industrial. Demonstra-se então, a preocupação do legislador em contemplar circunstâncias específicas em que se faça necessário classificar a informação como sigilosa.

Mais adiante, surge a Lei nº 12.965, de 23 de abril de 2014, mais conhecida como o Marco Civil da Internet, sendo este o primeiro marco regulatório brasileiro, com vistas a estabelecer princípios, garantias, direitos e deveres para o uso da Internet no Brasil, aplicáveis à União, aos Estados, ao Distrito Federal e aos Municípios.

A lei está dividida em cinco capítulos assim distribuídos: Capítulo I- Disposições preliminares; Capítulo II- Dos direitos e garantias dos usuários; Capítulo III- Da provisão de conexão e de aplicações de internet; Capítulo IV- Da atuação do Poder Público; e Capítulo V- Disposições finais.

Este Marco buscou preencher uma lacuna existente nas legislações anteriores, no que se refere à proteção de dados pessoais e do uso da internet no país. A sua implementação trouxe “direitos e garantias dos usuários e deveres dos provedores” (Flôres; Silva, 2020, p. 9), bem como segurança jurídica para provedores e usuários de internet. Um dos fatores que também motivou a criação do Marco Civil foi a repercussão do caso de espionagem norte-americano revelado pelo ex-analista da NSA, Edward Snowden, conforme abordado anteriormente.

No Art. 4º, inciso I, da supracitada lei, figura como um dos direitos tutelados pelo Marco Civil, o direito de acesso à internet a todos. Tal disposição é corroborada na Declaração Conjunta sobre a Liberdade de Expressão e Internet, em que a Organização para as Nações Unidas (ONU) no dia 1º de junho de 2011, determinou

normas sobre a liberdade de expressão e medidas de promoção universal do acesso à internet.

Os Estados têm a obrigação de promover o acesso universal à internet para garantir o gozo efetivo do direito à liberdade de expressão. O acesso à internet também é necessário para assegurar o respeito a outros direitos, como o direito à educação, à saúde e ao trabalho, ao direito de reunião e associação, e ao direito a eleições livres. (ONU, 2011).

No tocante à privacidade, o Marco Civil da Internet garante aos seus usuários proteção no momento da coleta, armazenamento e tratamento das informações fornecidas. Analisando a lei, percebe-se a participação do titular dos dados e o direito ao consentimento, reforçando mais uma vez o princípio da “autodeterminação informativa” (Silva, 2019). Em seu artigo 3º, prevê-se os seguintes princípios:

Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:

I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;

II - proteção da privacidade;

III - proteção dos dados pessoais, na forma da lei;

IV - preservação e garantia da neutralidade de rede;

V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;

VII - preservação da natureza participativa da rede;

VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte (Brasil, 2014).

Como foi possível constatar, a regulamentação da Lei nº 12.965/2014 tornou o ambiente virtual mais democrático, dado que a liberdade de expressão foi concebida como direito fundamental para o uso da internet no Brasil. Contudo, se absteve de estabelecer previsões de forma mais específica à proteção de dados pessoais, principalmente, os dados pessoais sensíveis, tendo em vista os desafios marcados pelo avanço das tecnologias da informação e comunicação.

## **2.2 A LGPD toma forma: sua constituição, estruturas e especificações**

Diante de um cenário marcado pelo crescente desenvolvimento tecnológico, tornou-se necessário discutir acerca do tratamento de dados pessoais e, principalmente, de dados pessoais sensíveis, visto a sua relevância nas relações sociais e de consumo, o que trouxe novos desafios para o ordenamento jurídico brasileiro, incidindo ainda, nos âmbitos público e privado.

O surgimento do RGPD da União Europeia trouxe à tona a necessidade de disciplinar sobre princípios, definições e parâmetros relacionados aos dados pessoais. A partir daí, vários outros países buscaram adequar ou adaptar as suas legislações ao regulamento europeu, a exemplo do Brasil.

Inspirada pelo RGPD, surge a Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados (LGPD), que visa garantir a segurança jurídica e o desenvolvimento de boas práticas de governança corporativa através da aplicabilidade de programas e documentos normativos que assegurem o devido tratamento aos dados pessoais dos cidadãos.

Conforme o disposto no Art. 1º da LGPD, essa Lei se aplica à pessoa física e jurídica, seja ela de direito público ou privado, bem como os entes federativos da Administração Pública (União, Estados, Distrito Federal e Municípios), e tem como objetivo assegurar os direitos fundamentais de liberdade e de privacidade, bem como o devido tratamento de dados pessoais, independente do suporte onde a informação esteja armazenada. (Brasil, 2018).

Levando-se em consideração a abrangência dessa Lei, faz-se necessário discutir a sua aplicabilidade na Administração Pública e Privada, visto o grande fluxo de dados pessoais que são armazenados e tratados pelas instituições.

Diante do exposto, é inegável que com as mudanças sociais, decorrentes da chamada “era da informação”, tornou-se cada vez mais necessário o uso das tecnologias e da Internet para diversas finalidades. Essa nova conjuntura permite a coleta de dados para a efetivação de serviços, tornando as organizações detentoras de um dos principais aditivos: a informação (Flôres; Silva, 2020).

O escopo da Lei nº 13.709/2018 está dividido em 10 Capítulos, com 65 artigos, que em comparação ao Regulamento Europeu, apresenta uma estrutura mais enxuta. O Capítulo I trata das disposições preliminares e em seus artigos dispõe sobre a quem

se aplica a lei de proteção de dados, disciplina fundamentos e traz importantes definições e terminologias, *in verbis*:

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

IX - agentes de tratamento: o controlador e o operador;

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; (Brasil, 2018).

No Capítulo II é abordado o tratamento de dados pessoais, e apresentam-se os requisitos para o tratamento de dados pessoais e dados pessoais sensíveis, dados pessoais de crianças e adolescentes e o término do tratamento de dados. Os direitos do titular são normatizados no Capítulo III e descrevem as formas e os prazos pelos quais o cidadão pode exercer o seu direito à “autodeterminação informativa”.

Acerca do tratamento de dados pessoais pelo Poder Público, o Capítulo IV dedica-se a versar sobre as regras e as responsabilidades em caso de ocorrência de infração à LGPD. A transferência internacional de dados é descrita no Capítulo V e o Capítulo VI discorre sobre os agentes de tratamento de dados pessoais, bem como suas responsabilidades e sanções em caso de danos.

O Capítulo VII aborda a segurança e as boas práticas no tratamento de dados pessoais, enquanto o Capítulo VIII refere-se à fiscalização da proteção de dados e das sanções administrativas. No Capítulo IX aborda-se a Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade como órgãos fiscalizadores e reguladores da LGPD. O Capítulo X prevê as disposições finais e transitórias.

Acerca dos princípios que norteiam e que devem ser observados em todo o processo de tratamento de dados pessoais são:

- a) **princípio da finalidade:** o tratamento de dados deve ser realizado conforme propósito específico, sem posterior uso que transgrida a finalidade estabelecida;
- b) **princípio da adequação:** deve haver consonância entre os dados informados e a finalidade pela qual foi solicitada;
- c) **princípio da necessidade:** só serão fornecidos os dados necessários para a consecução de determinada finalidade;
- d) **princípio do livre acesso:** garante ao cidadão, titular dos dados, o requerimento à informações que lhe sejam pertinentes;
- e) **princípio da qualidade dos dados:** aos titulares é garantido o direito à obter dados exatos, claros, relevantes e atuais, proporcionais à necessidade e ao tratamento das informações;
- f) **princípio da transparência:** aos titulares, deve-se prestar informações claras, precisas e de fácil acesso sobre a atividade de tratamento dos dados, bem como sobre os agentes responsáveis pelo tratamento, resguardando os segredos comercial e industrial;
- g) **princípio da segurança:** resguarda por meio de medidas técnicas e administrativas os dados pessoais de violações do direito à privacidade.
- h) **princípio da prevenção:** adota medidas para coibir o risco de violação de dados pessoais, em virtude de seu tratamento;
- i) **princípio da não-discriminação:** impede a realização de tratamento de dados quando a finalidade for discriminatória, ilícita ou abusiva;
- j) **princípio da responsabilização e prestação de contas:** cabe ao agente de tratamento de dados, apresentar meios que comprovem o cumprimento do disposto na lei, salvaguardando os dados pessoais.

Importante observar que, a LGPD trouxe desafios e inovações ao ordenamento jurídico brasileiro, compreendendo que os dados, independente do suporte, devem ser levados em consideração, uma vez que são dotados de personalidade. Nesse sentido, os princípios mencionados configuram-se de suma importância para a efetivação e materialização dos titulares dos dados (Silva, 2019).

Cabe ressaltar que, até entrar em vigor, a LGPD passou por um longo processo no Congresso Nacional (CN). Publicada em 14 de agosto de 2018, o prazo para vigência se daria após meses a contar da publicação no Diário Oficial da União (DOU). Entretanto, como muitas empresas alegaram que este prazo era curto para adaptação à lei, esta prorrogou-se para agosto do ano de 2020 através da Lei nº 13.709.

Com a chegada da Covid-19 que afetou países do mundo inteiro, suscitaram-se novas discussões sobre a vigência da lei. Em vista da gravidade da pandemia, muitas organizações interromperam as suas atividades, e tiveram que lidar com crises econômicas e financeiras, estendendo ainda mais o prazo para adequação à LGPD.

Nesse percurso, foram impetradas duas ações em Brasília/DF para o adiamento da lei: a primeira delas em 3 de abril de 2020 com o Projeto de Lei nº 1.179/20, cujo intento era prorrogar o prazo de vigência para janeiro de 2021, assim como a aplicação de sanções administrativas; a segunda, deu-se em 29 de abril de 2020 através de uma Medida Provisória 959/2020 que dispunha sobre as regras para obtenção do auxílio emergencial aos trabalhadores, estabelecendo ainda, o adiamento da vigência da LGPD. De acordo com a medida supramencionada, a Lei Geral de Proteção de Dados entraria em vigor no dia 03 de maio de 2021, não se estendendo a essa data as sanções administrativas e resoluções da Autoridade Nacional de Proteção de Dados (ANPD).

Por fim, em 10 de junho de 2020 é publicada no DOU a Lei nº14.010/20 que manteve o disposto no Projeto de Lei nº 1179/2020, o qual prorrogou a vigência da LGPD para 03 de maio de 2021 com a aplicação de multas e sanções a viger no dia 01 de agosto de 2021.

O Senado Federal com a premissa de que a vigência da lei era necessária para a segurança da personalidade humana, principalmente, devido à expansão das tecnologias, decidiu pelo não adiamento da LGPD, a qual passou a vigorar 15 dias após conclusão.

Desse modo, tal como no molde europeu da RGPD, entrou em vigor em 18 de setembro de 2020, a LGPD brasileira com a permanência da aplicação de sanções administrativas para o dia 01 de agosto de 2021.

### 2.3 Privacidade e violação do uso dos dados pessoais

A privacidade enquanto direito fundamental dos seres humanos evoluiu ao longo da história, acompanhando o surgimento de legislações e implementações de normas ao redor do mundo. Ao contrário do que se pensa, o termo “privacidade” não é novo, pois desde a Idade Média, estudiosos discutiam acerca desse direito que se aplicava exclusivamente à classe dominante da sociedade feudal (Simões, 2017).

Ao tratar da privacidade, faz-se necessário estabelecer uma distinção clara entre os espaços público e privado, sendo o público caracterizado como tudo aquilo é genérico, comum e acessível, mas, não necessariamente, gratuito; enquanto o privado é marcado pela restrição, particularidade e personalidade dos cidadãos. Contudo, essas esferas se entrecruzam, numa relação de dependência.

Do mesmo modo, evidencia-se que a atuação pública da pessoa humana carece do reconhecimento de sua esfera privada, devidamente tutelada pelo Estado, como se vê: “A atuação pública dos cidadãos, isto é, o desenvolvimento da sua cidadania, não se exerce sem a preexistência de uma autonomia privada garantida por direitos fundamentais. Em outras palavras, sem os direitos que se desdobram dos princípios jurídicos da dignidade, igualdade e liberdade, e que permitem a construção do indivíduo consciente e autônomo, não se pode verificar o exercício consciente e autônomo dos direitos que asseguram sua autonomia pública (Guerra, 2015, p. 5).

Observa-se que as discussões acerca da privacidade se avolumam à medida em que as tecnologias da informação e comunicação se desenvolvem e as relações sociais se transformam ao longo do tempo. Com relação à internet, esta propicia novas formas de interação nos ambientes digitais. Algumas de suas características são a bidirecionalidade e liberdade de expressão que permite às pessoas exporem as suas ideias e opiniões sem restrição.<sup>10</sup>

Entretanto, não pode ser totalmente tratada como um espaço público, visto que para usufruir de determinados serviços e produtos exige-se que o acesso perpassse os limites da esfera pública e adentre a esfera íntima do indivíduo. Cabe assim, ao

---

<sup>10</sup> Contudo nos últimos quatro anos, durante a pandemia da Covid-19, o Brasil foi tomado por uma onda epidêmica de Fake News e desinformação, provocada pelo ambiente infodêmico, em que as notícias falsas prevaleciam sobre as notícias verdadeiras em um período histórico marcado pela incerteza, a exemplo dos movimentos antivacinas.

cidadão, avaliar e determinar quando, como e quem pode ter acesso às suas informações pessoais.

Enquanto o espaço público é o espaço das ações visíveis, onde qualquer fato pode ser conhecido por todos, o lugar aonde, a princípio, tudo é potencialmente visível; o espaço particular é o lugar das coisas e das práticas que não devem ser vistas. É o espaço da intimidade, dos interditos, protegido do olhar público por cortinas e portas, no qual só é admitido quem for convidado. Aliás, a proteção do espaço privado é uma das bases da democracia moderna; ninguém, exceto com ordem judicial, pode entrar na casa de outra pessoa sem autorização (Sá Martino, 2014, p. 94).

Acerca da origem etimológica da palavra, o termo privacidade deriva do latim *privare*, forma adjetiva *privatus*. Essa expressão de origem latina, tal como a utilizamos hoje, sofreu influências da língua inglesa (*privacy*), representando o anglicismo. Na doutrina brasileira, frequentemente aparece ao lado de termos como “vida privada, “intimidade”, “segredo”, “reserva” “intimidade”, dentre outros (Doneda, 2020).

Ao se traçar um percurso histórico, a origem da palavra privacidade teve suas primeiras discussões na Idade Média com “manifestação de necessidades de isolamento” (Simões, 2021, p. 51), visto a conjuntura social da época, este era um direito de poucos, a exemplo de senhores feudais e membros do clero.

No Reino Unido, o marco do início da proteção da *privacy* acontece com o *Justices of the Peace Act*<sup>11</sup> Lei do Parlamento Inglês sancionada em 1361, cujo objetivo era zelar e manter a paz na sociedade. Essa Lei, estabelecia os critérios de elegibilidade para se tornar um juiz de paz, bem como as suas atribuições e deveres. Assim, o papel desempenhado por um juiz de paz era combater infratores e violadores da privacidade alheia (Doneda, 2020).

As primeiras transformações começam a ocorrer na chegada do século XVI com o surgimento das cidades e uma nova organização social, a qual é marcada pela delimitação territorial, propiciando o isolamento. Ainda assim, a privacidade continuava sendo um direito da burguesia (Doneda, 2020).

Outro caso precedente aconteceu no Tribunal Civil de Sena, na França, em 1858, após a divulgação da imagem fotográfica de uma atriz francesa em seu leito de morte.

Ocorre que, de forma não autorizada, os fotógrafos disponibilizaram a sua imagem para elaboração de um desenho, que foi posteriormente publicado no seminário L'illustration. A família da atriz ajuizou ação em face do desenhista e o Tribunal Civil de Sena proferiu sentença no

---

<sup>11</sup> Lei dos Juizes de Paz, legislação vigente em 1361.

sentido de que não seria dado a ninguém reproduzir e dar publicidade a traços de uma pessoa em seu leito de morte, sem autorização formal da família (Machado, 2014, p.134).

Acerca do tema, considera-se a publicação de Samuel Warren e Louis Brandeis intitulada *The right to privacy* como a precursora nas discussões sobre o direito à intimidade e à vida privada, a qual posteriormente, evoluiu para o “*right to be alone*”, conceito que traduz o direito de ser deixado só, de proteger a privacidade individual, delimitando assim, as esferas pública e privada (Simões, 2021).

Todos os estudos e legislações citados anteriormente, foram essenciais para a reformulação do direito à privacidade, acompanhando as transformações sociais e as tecnologias da informação e comunicação. De acordo com Simões (2021), nessa linha histórica, em 1948, foi proclamada em Paris, a Declaração Universal dos Direitos Humanos, um documento histórico que disciplina acerca dos direitos fundamentais da pessoa humana.

Este importante marco, estabelece as garantias e as liberdades de todos os indivíduos sem distinção. Neste ponto, vale lembrar que o direito à privacidade, antes um privilégio da classe burguesa, passa a ser uma prerrogativa legal de todos os cidadãos, no intuito de estabelecer a equidade e justiça sociais.

Conforme o disposto no Art. 12 da Declaração Universal dos Direitos Humanos “Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques” (ONU, 1984, p. 9).

Na CF/1988, prevê-se de forma expressa o direito à privacidade e à inviolabilidade da personalidade humana no Art. 5º, incisos X e XX:

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;  
XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (Brasil, 1988).

Nesse sentido, com a vigência da LGPD objetivou-se tutelar a privacidade das pessoas físicas, pois as pessoas jurídicas não são dotadas de personalidade e, portanto, não gozam de igual proteção.

O que se percebe é que ao longo da evolução da regulamentação da proteção de dados no Brasil, a privacidade esteve amparada em diplomas legais, a exemplo da

Lei Magna, CCB, CDC, do Marco Civil da Internet e em tantos outros dispositivos (Silva, 2019).

[...] o direito à privacidade deixa de estar estruturado em torno do eixo 'pessoa-informação-segredo' e passa a se fundamentar no eixo 'pessoa-circulação-controle', ou seja, a proteção de dados se afasta do próprio discurso abstrato da privacidade. As técnicas de anonimização surgem, assim, como medidas técnicas de segurança, que legitimam a circulação e o tratamento de dados (Cravo, 2021, p. 46).

Para tanto, criou-se órgãos governamentais, comissões, organizações e autoridades que dispusessem sobre a necessidade de resguardar os dados pessoais dos cidadãos, além de buscar meios de combate à violação da privacidade. Como exemplo, tem-se o *Office Off the Australian Information Commissioner* (OAIC), uma agência reguladora fundada em 2010, cujo objetivo era garantir o direito de acesso às informações e aos dados pessoais dos cidadãos que estavam em poder do Estado, bem como assegurar a privacidade destas (Simões, 2021).

Na União Europeia, por sua vez, estabeleceu-se Autoridades de Controle em consonância ao disposto no RGPD, cujas atribuições são: receber e tratar as reclamações apresentadas pelos proprietários dos dados.

No Brasil, conseqüentemente, com a vigência da LGPD, criou-se a Autoridade Nacional de Proteção de Dados (ANPD), uma entidade responsável por fiscalizar o cumprimento da lei, aplicar sanções administrativas e receber denúncias de violações de dados.

A LGPD em seu Art. 55- C, define a composição da ANPD, formada por um Conselho Diretor, órgão máximo de direção; Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; Corregedoria; Ouvidoria, Procuradoria e Unidades Administrativas e Especializadas (Brasil, 2018).

Enquanto órgão fiscalizador, os agentes de tratamento de dados podem aplicar as seguintes sanções administrativas em caso de infração da lei:

- I - advertência, com indicação de prazo para adoção de medidas corretivas;
- II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- III - multa diária, observado o limite total a que se refere o inciso II;
- IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)

XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)

XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (Brasil, 2018).

Conforme o disposto neste mesmo artigo, leva-se consideração os seguintes critérios na aplicação das sanções (Brasil, 2018):

- a) **gravidade e natureza da violação da privacidade:** avalia-se a intensidade da violação do agente de tratamento em relação ao dispositivo legal, levando em consideração o impacto dos danos causados ao titular dos dados;
- b) **boa-fé do transgressor:** avalia-se a boa-fé do infrator para decréscimo de percentuais sob a penalidade aplicada;
- c) **vantagem auferida ou pretendida pelo infrator:** impede que a infração sirva de enriquecimento ilícito. Deve-se avaliar e prova a intenção do infrator de obter lucros;
- d) **condição econômica do infrator:** considera a situação econômica do infrator para aplicação de sanções, mais precisamente, de multas;
- e) **Reincidência:** repetição da prática criminosa dentro de um determinado período;
- f) **grau do dano e adoção de medidas corretivas:** avaliação do grau do dano em relação às pessoas afetadas pela infração. Para prevenir a reincidência danosa, aplica-se medidas corretivas de diferentes níveis de atenuantes;
- g) **cooperação do transgressor:** aplica-se decréscimo de percentuais sob o valor da penalidade do infrator e redução da pena em 5%, conforme também aplicado para a boa-fé;
- h) **adoção de medidas de proteção ao tratamento dos dados:** adoção de boas práticas de governança corporativa no tratamento de dados para minimizar os danos;
- i) **desenvolvimento de boas práticas e governança corporativas:** adoção de boas práticas no tratamento de dados pelas organizações para reduzir as possibilidades de sanções;

- j) **gravidade da falta e a intensidade da sanção:** deve-se avaliar a proporcionalidade entre a gravidade da infração e a intensidade da sanção, atenuando a penalidade quando constatado prejuízo a uma das partes.

#### **2.4 A biblioteca escolar no contexto da proteção dos dados pessoais dos seus usuários**

Para Pimentel (2007), etimologicamente, a palavra biblioteca origina-se dos termos gregos *biblíon* (livro) e *theka* (caixa), significando um espaço onde se guardam os livros. Mais precisamente, foi no Egito, a partir do século IV a.C., que surgiu uma das maiores e mais célebres instituições de produção do conhecimento do mundo da Antiguidade, a Biblioteca de Alexandria, cuja intenção era reunir em um só lugar toda a produção bibliográfica humana (Andrade, 2009).

No entanto, ao longo da história, as bibliotecas foram transformando-se e deixaram de ser apenas lugar de guarda de documentos, de “depósito de livros”, para voltar o foco aos usuários, propiciando a eles mecanismos de acesso à informação de forma mais dinâmica.

As bibliotecas representam um importante espaço de memória coletiva que guardam um vasto patrimônio intelectual construído ao longo da história da humanidade e que constituem-se como locais de diálogo, criação e inovação. São instituições dinâmicas que para além de colecionar saberes, são responsáveis por proporcionar acesso ao conhecimento humano, através de registros sejam eles nos mais diversos suportes informacionais, os quais são organizados de forma que sejam identificados, recuperados, disseminados e utilizados, compondo assim, o acervo de uma biblioteca (Lemos; Passos, 2020).

Conforme Nunes, Lira e Gehrke (2019), as bibliotecas surgem da necessidade de guardar, organizar e preservar os conhecimentos produzidos pelos seres humanos em diferentes épocas, lugares e contextos. Logo, sua origem remonta à própria história da humanidade. De acordo com Milanese (2002, p. 77):

Durante séculos a biblioteca definiu-se como acervo, coleção de impressos. Era a forma como os grupos humanos, os povos preservavam os seus conhecimentos acumulados, transferindo-os de geração para geração com os acréscimos feitos por novas produções. Com o tempo, os registros foram se diversificando, surgindo seções de jornais, revistas e, depois, o que se denominou “audiovisual”. Essas mudanças foram fortes no transcorrer do século XX, tornando-se evidentes em suas últimas décadas: a organização do acervo não é

mais a razão de ser da biblioteca, surgiram os serviços de informação moldados aos grupos específicos.

Dessa forma, percebe-se que a biblioteca torna-se um serviço atuante no que diz respeito à socialização da informação, em razão da segmentação do público que permite direcionar e adequar os serviços bibliotecários às necessidades de cada indivíduo. Importante ressaltar que, essas instituições podem ser classificadas em: nacionais, universitárias, escolares, públicas, especializadas. Portanto, cada uma delas evidencia uma função social específica, diferentes níveis de especialização do acervo, conhecimentos característicos e tipos de leitores particulares (Lemos; Passos, 2020).

De acordo com o Manifesto da Federação Internacional de Associações e Instituições Bibliotecárias (IFLA) e da Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO) em Defesa da Biblioteca Escolar (2002, p. 1), acerca da biblioteca escolar:

A biblioteca escolar (BE) propicia informação e idéias fundamentais para seu funcionamento bem sucedido na atual sociedade, baseada na informação e no conhecimento. A BE habilita os estudantes para a aprendizagem ao longo da vida e desenvolve a imaginação, preparando-os para viver como cidadãos responsáveis.

As bibliotecas escolares, foco deste estudo, são importantes recursos educativos que contribuem para o processo de ensino-aprendizagem, no processo de alfabetização e letramento e que através de seu acervo voltado para as atividades pedagógicas educacionais objetivam atender à comunidade escolar à qual está inserida.

E levando em consideração o contexto educacional à luz da LGPD, faz-se necessário que as instituições tanto públicas quanto privadas sigam as exigências dispostas na legislação, pois lidam diretamente com dados pessoais e dados pessoais sensíveis da comunidade escolar, a exemplo de informações pessoais de crianças e adolescentes.

No âmbito da biblioteca escolar não é diferente, para a utilização dos serviços bibliotecários há a necessidade de coleta e tratamento de dados pessoais de seus usuários, a exemplo do empréstimo domiciliar. Através deste serviço é possível traçar informações importantes sobre o perfil do usuário, já que a biblioteca possui em seu sistema, seja ele informatizado ou não, a custódia do histórico de seus utilizadores, o qual deve ser garantido a confidencialidade (Lemos; Passos, 2020).

Diante do exposto, a *American Library Association* (ALA) enfoca a relevância do direito à privacidade em bibliotecas:

As bibliotecas fornecem um local para o exercício da liberdade intelectual: uma troca livre e aberta de conhecimentos e informações, onde os indivíduos podem exercer a liberdade de pesquisa, bem como o direito à privacidade em relação às informações que procuram. A privacidade é essencial para o exercício da liberdade de expressão, do livre pensamento e da livre associação. Em uma biblioteca, o assunto dos interesses dos usuários não deve ser examinado ou examinado por outros. (USA PATRIOT ACT, [2005?] apud Lemos; Passos, 2020, p. 87).

Nesse sentido, evidencia-se a responsabilidade que as bibliotecas escolares carregam ao lidar com dados pessoais e dados pessoais sensíveis, a exemplo da coleta do nome completo do usuário, número da matrícula, número de registro no cadastro de pessoa física (CPF), endereço, lista de doadores de livros, dentre outras informações. Há que se falar ainda, do estudo de usuários, a partir do levantamento do perfil dos utilizadores, bem como de suas áreas de interesse, no intuito de oferecer um serviço personalizado, o que por outro lado, poderia incorrer na inobservância da LGPD (Lemos; Passos, 2020).

Entretanto, cabe destacar a importância do papel do bibliotecário e as atividades por ele desenvolvidas nesse contexto, uma vez que ele é o facilitador entre a informação e os seus usuários. Portanto, seu fazer profissional deve fundamentar-se em condutas éticas consoante à Resolução nº 2018, publicada pelo Conselho Federal de Biblioteconomia (CFB). Conforme o Art. 7, § 3º da LGPD, “O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização [...]” (Brasil, 2018).

Dessa forma, de acordo com Mendes e Bioni (2019), os princípios da LGPD objetivam conferir ao titular maior controle sobre o fluxo de seus dados, o direito de obter informações sobre o uso, a necessidade do consentimento expresso, de acessar os dados coletados, de corrigi-los ou mesmo apagá-los, no intuito de estabelecer limites ao tratamento de dados pessoais.

Nesse sentido, as políticas de privacidade são de suma relevância, pois elas legalizam a coleta e o tratamento de dados por uma instituição. E em caso de danos causados a terceiros, a responsabilidade incide sobre a instituição que abriga a biblioteca, à própria biblioteca e ao bibliotecário, de forma subsidiária, se a sua conduta transgredir os princípios disciplinados na legislação, o qual será passível de

penalidades conforme os ditames do Art. 22 da Lei nº 4.084, de 30 de junho de 1962 que regula a profissão do bibliotecário (Lemos; Passos, 2020).

Nesse sentido, quando a inobservância violar algum dispositivo legal, a ANPD agirá junto com o Conselho Federal de Biblioteconomia para a aplicação de sanções. Desse ponto de vista, para Lemos e Passos (2020) as bibliotecas tornam-se aliadas da ANPD no tocante ao processo de adequação da lei a esses espaços de informação, bem como ao tratamento cabível aos dados coletados.

Em vista disso, para gerir a informação no contexto das instituições, faz-se necessário conhecer a sua estrutura, bem como a realização de diagnóstico para identificar os processos de produção, tramitação e arquivamento de dados para estabelecer as metodologias a serem aplicadas. Faz-se indispensável ainda, o estudo das normas e políticas que regem a unidade administrativa, o levantamento dos documentos produzidos pelos setores, bem como o mapeamento dos documentos que possuem dados pessoais e/ou dados pessoais sensíveis a fim de que sejam devidamente tratados (Schwaitzer; Nascimento; Costa, 2020).

Schwaitzer, Nascimento e Costa (2020) corroboram ao afirmar que a existência de um programa de gestão documental torna mais fácil o processo de adequação das diretrizes previstas na LGPD. No que diz respeito à biblioteca, o profissional bibliotecário desempenha importante papel, sendo aquele responsável pelas ações referentes ao tratamento de dados, no que lhe couber, preservando os interesses organizacionais e garantindo os direitos dos titulares dos dados.

Considerando a importância da aplicabilidade da LGPD tanto em instituições da esfera pública quanto privada, observa-se a necessidade da incrementação de políticas que visem garantir a proteção de dados pessoais dos consumidores. Segundo Crespo (2021, p. 16) as organizações têm buscado por “[...] consultorias ou, por si mesmas, feito ajustes com vistas a conquistarem um programa de *privacy compliance*” (Crespo, 2021, p. 16).

A partir desse contexto, tem-se como objetivo geral deste estudo verificar como a biblioteca da Escola A está cumprindo a Lei Geral de Proteção de Dados desde sua implantação. Na seção seguinte será apresentada a metodologia utilizada neste estudo, os métodos de pesquisa e os instrumentos utilizados para a obtenção dos dados.

### 3 METODOLOGIA

O método científico constitui-se como uma das etapas essenciais na produção do conhecimento científico que permite aos pesquisadores planejar o percurso metodológico da pesquisa, delimitando os procedimentos, abordagens e técnicas pelas quais serão desenvolvidas e realizadas as atividades propostas pelo objeto de estudo, mediante a natureza do problema a ser investigado (Fachin, 2005).

Para compreender a LGPD e sua aplicabilidade na gestão documental conduzir-se-á uma pesquisa de caráter exploratório e descritivo. Segundo Marconi e Lakatos (2003), a pesquisa exploratória objetiva a formulação de hipóteses e a aproximação do pesquisador do objeto investigado no intuito de explicar e esclarecer conceitos, contribuindo para a elaboração de pesquisas futuras mais claras.

Ressalta-se que essa pesquisa possibilitou estudar a privacidade, a LGPD em sua criação e constituição, aproximando-se do objeto e desvendando seu emprego, suas relações e sua transversalidade.

A pesquisa descritiva, por sua vez, conforme Gil (2002), é entendida como um instrumento que descreve as características dos fenômenos observados, determinando pontos em comum entre as variáveis. Esta pesquisa possibilitou caracterizar a LGPD e a Escola A no âmbito de suas atividades administrativas.

Para tanto utilizou-se a abordagem qualitativa, que segundo Fachin (2005, p. 81), caracteriza-se “[...] pelos seus atributos e relaciona aspectos não somente mensuráveis, mas também definidos descritivamente”.

Essa abordagem foi necessária para compreender os aspectos mais subjetivos como o processo da implementação da LGPD na Escola A relacionando-a com a literatura científica deste estudo.

Nesse contexto, o marco teórico é fundamentado pelas pesquisas bibliográfica e documental. A primeira foi desenvolvida em bibliotecas físicas, como a Biblioteca Central da Universidade Federal do Maranhão (UFMA) e fontes de informação digitais, a exemplo da Biblioteca Digital de Teses e Dissertações do Instituto Brasileiro de Informação Científica e Tecnológica (BDTD/IBICT), Scielo, Biblioteca Digital da UFMA, Universidade Federal de Minas Gerais (UFMG) dentre outras.

A pesquisa bibliográfica, na visão de Marconi e Lakatos (2003, p. 183), constitui-se também como fontes secundárias que:

[...] abrange toda bibliografia já tornada pública em relação ao tema de estudo, desde publicações avulsas, boletins, jornais, revistas, livros,

pesquisas, monografias, teses, material cartográfico etc., até meios de comunicação orais: rádio, gravações em fita magnética e audiovisuais: filmes e televisão. Sua finalidade é colocar o pesquisador em contato direto com tudo o que foi escrito, dito ou filmado sobre determinado assunto, inclusive conferências seguidas de debates que tenham sido transcritos por alguma forma, querem publicadas, quer gravadas.

A pesquisa documental realizou-se com base na leitura, análise de Leis, como a própria LGPD, CF/1988, LAI, dentre outros materiais primários necessários para subsidiar a construção teórica e fundamentar a análise dos dados coletados.

De acordo com Gil (2002), a pesquisa documental utiliza-se de materiais que ainda não foram objeto de estudo e/ ou passaram por tratamento analítico, constituindo-se de itens informacionais de valor primário. Nessa perspectiva, Gil (2002, p. 46) inclui nessa categoria “[...] os documentos conservados em arquivos de órgãos públicos e instituições privadas, tais como associações científicas, igrejas, sindicatos, partidos políticos etc”.

Soma-se a essas pesquisas, o Estudo de Caso, que embora tenha surgido no bojo das Ciências Médicas, foi amplamente utilizado pelas Ciências Sociais como uma modalidade de análise que permite aos pesquisadores diagnosticar, refletir e conhecer em profundidade o objeto investigado (Gil, 2002).

Nessa mesma linha, Yin (2005, p. 33) destaca a abrangência do estudo de caso na pesquisa científica como uma estratégia que “[...] compreende um método que abrange tudo - com a lógica de planejamento incorporando abordagens específicas à coleta de dados e à análise de dados”.

Para Fachin (2003, p. 45), o estudo de caso:

[...] é caracterizado por ser um estudo intensivo. No método estudo de caso, leva-se em consideração, principalmente, a compreensão, como um todo, do assunto investigado. Todos os aspectos do caso são investigados. Quando o estudo é intensivo, podem até aparecer relações que, de outra forma, não seriam descobertas.

Esta pesquisa foi realizada em uma Escola de ensino bilíngue, a qual se nomeia de Escola A, cuja pesquisa *in loco* foi permitida mediante o envio de um ofício à gestão da instituição (Apêndice A) que colaborou com o acesso aos documentos para a análise de dados.

Outro instrumento de coleta de dados utilizado foi a entrevista semiestruturada aplicada com os responsáveis pelo tratamento de dados pessoais de forma a obter informações sobre as diretrizes e os instrumentos pelos quais a biblioteca vem

adequando o tratamento de dados face às exigências da LGPD como garantia ao tratamento dos dados pessoais e ou dados pessoais sensíveis.

Segundo Marconi e Lakatos (2003, p. 195), a entrevista consiste no “[...] encontro entre duas pessoas, a fim de que uma delas obtenha informações a respeito de determinado assunto, mediante uma conversação de natureza profissional”.

Em relação a análise dos dados, ela ocorreu pelo estabelecimento de relações entre a teoria, a LGPD, aos dados coletados e a análise da pesquisadora que levou em consideração a sua vivência na biblioteca em estudo, o aprofundamento sobre a LGPD.

### **3.1 Lócus de pesquisa**

A Escola A está localizada em um bairro nobre da capital maranhense. Fundada em 2010, integra uma rede de franquias de educação bilíngue. Essa instituição de ensino está difundida em mais de 35 países com mais de 526 escolas presentes no mundo, e atualmente, no Brasil, existem mais de 171 unidades escolares.

A instituição trabalha com a educação infantil, ensino fundamental e ensino médio e tem como pilares a imersão na língua inglesa e as melhores práticas de educação. No Brasil, o programa acadêmico das escolas foi desenvolvido por educadores canadenses e brasileiros e está em consonância à Lei de Diretrizes e Bases da Educação Nacional (LDB) do Ministério da Educação (MEC).

Conforme informações do Guia da Família, documento enviado às famílias dos alunos, a missão da Escola A é formar cidadãos capazes de viver, transitar, influenciar e transformar qualquer lugar do mundo, empreendendo seus talentos de forma responsável, generosa, criativa e ética. Tem como visão manter-se como a melhor escola bilíngue do Maranhão e tornar-se referência nacional. E é pautada nos seguintes valores: inovação, responsabilidade, cooperação, gentileza, ética, pertencimento e respeito.

Acerca da estrutura física, a escola é composta por três andares, sendo o térreo direcionado às crianças com faixa etária entre 6 e 7 anos, enquanto que no primeiro e segundo andar são atendidos alunos até o ensino médio. Além disso, a escola possui salas de aulas, sala maker, auditório, laboratório, biblioteca, quadra de esportes, cantina, refeitório e parque recreativo, dentre outros espaços.

A escola possui ao todo 594 discentes matriculados. E acerca de seu quadro funcional: uma diretora geral, um diretor pedagógico, uma bibliotecária, nove coordenadores pedagógicos distribuídos nos segmentos; bem como professores regentes, professores assistentes, estagiários, assistentes administrativos entre outros colaboradores.

### 3.1.1 A biblioteca da Escola A

A biblioteca da Escola A foi inaugurada no ano de 2022, mediante a necessidade de um espaço para servir de apoio ao processo de ensino-aprendizagem, atuando junto à comunidade escolar, bem como para atender ao disposto na Lei nº 12.244, de 2010, que regula a universalização das bibliotecas nas instituições de ensino do País. O espaço foi organizado desde sua implantação por uma bibliotecária, com especialização em andamento em Gestão de Bibliotecas Escolares, juntamente com a colaboração de uma assistente administrativa e uma estagiária. Periodicamente, a escola oferece aos seus funcionários atividades formativas, visando a melhoria contínua no ambiente de trabalho de cada um.

O ambiente da biblioteca é subdividido em sala de estudo, salão de leitura com mesas e cadeiras e grande parte do acervo encontra-se nesse espaço que atende alunos do ensino fundamental ao ensino médio. Há também um espaço lúdico, com acervo voltado para o público infantil; setor de referência para atendimento aos usuários, além de um hall com quadros das turmas que se formaram no ensino médio.

O acervo é composto por materiais bibliográficos literários, técnicos, periódicos, obras de referência (dicionários e enciclopédias) e multimídias. Possui sistema informatizado que contabiliza mais de 10.000 títulos cadastrados, classificados de acordo com a Classificação Decimal Universal (CDU) e a Tabela de Cutter, além de serem sinalizados nas estantes por assunto.

A respeito dos serviços, a biblioteca escolar oferece aos seus usuários o empréstimo domiciliar, renovação, devolução, reserva, treinamento de usuários, sugestão de aquisição, atendimento aos usuários, empréstimo especial de materiais bibliográficos para uso em sala de aula, eventos literários, dentre outros. O período de maior fluxo no espaço dá-se durante o horário de intervalo de aulas e nos dias de atividades avaliativas nos turnos matutino e vespertino.

## 4 APRESENTAÇÃO DOS DADOS E SUA DISCUSSÃO

Nesta seção são apresentados os resultados deste estudo obtidos por meio dos dados coletados nos roteiros de entrevista realizados tanto com a profissional responsável pela biblioteca da Escola A quanto com o consultor em Sistema de Informação da instituição de ensino, que possui vasto conhecimento nos estudos da LGPD.

A seguir serão descritos os tipos de dados coletados pela biblioteca, a análise do cumprimento dos princípios da LGPD no âmbito da biblioteca e como é realizado o tratamento de dados pessoais e dados pessoais sensíveis.

### 4.1 Descrição e análise dos dados obtidos

De acordo com o roteiro de entrevista aplicado (APÊNDICE A), conforme a pergunta 1, os serviços bibliotecários são realizados de forma híbrida (manual e em sistema informatizado), já que o acervo está passando por processamento técnico e parte dos livros não estão cadastrados no banco de dados. Ainda assim, por possuir um sistema integrado, a biblioteca tem acesso aos dados pessoais e dados pessoais sensíveis dos usuários, os quais são acessados, somente para a finalidade de efetivação dos serviços.

Ressalta-se que os dados em posse da biblioteca escolar devem ser armazenados de forma a garantir a privacidade e a confidencialidade dos seus usuários. Esta prática é garantida pela LGPD brasileira e já era anunciada pelo primeiro Código de Ética da Biblioteconomia em 1939, cuja publicação foi pela *American Library Association* (ALA), onde dispunha em seu artigo 11 “[...] de tratar como confidencial y privada la información obtenida de los usuarios”. (Varela-Orol; Ameneiros Rodríguez, 2018, p.686).

Esse cenário intensificado pelo uso de tecnologias da informação pelos bibliotecários, cresce gradativamente as responsabilidades políticas, sociais e legais do bibliotecário, ele é o responsável pela mediação entre o usuário e a informação de forma a possibilitar o acesso a essa informação.

O Quadro 1 refere-se à questão 2 acerca do mapeamento dos tipos de dados pessoais coletados pela biblioteca para fins de utilização dos serviços e identificação de usuários.

Quadro 1- Mapeamento dos dados pessoais coletados pela biblioteca

<b>Dados para cadastro</b>	<b>Finalidade dos dados</b>	<b>Respaldo</b>
Nome completo e assinatura do usuário	Utilização dos serviços da biblioteca.	Base Legal
E-mail	Utilização dos serviços da biblioteca	Base Legal
Setor	Utilização dos serviços da biblioteca	Base Legal
Turma	Utilização dos serviços da biblioteca	Base Legal

Fonte: Elaboração da pesquisadora com base nos dados coletados (2023)

Em conformidade com o quadro apresentado, os dados coletados têm como base legal a LGPD em consonância ao disposto no Art. 7º da supracitada Lei, que dispõe sobre o tratamento de dados pessoais. Uma das hipóteses previstas é, segundo o inciso II, “[...] para o cumprimento de obrigação legal ou regulatória pelo controlador [...]” (Brasil, 2018).

No tocante à questão 3, sobre a efetivação dos serviços da Biblioteca, é necessário que os usuários consentam em disponibilizar seus dados pessoais, a exemplo do nome completo, assinatura, e-mail institucional para que se possa entrar em contato, notificando-o da necessidade de realizar a renovação e/ou mesmo devolução da obra emprestada.

Embora a biblioteca acesse os dados pessoais para efetivação dos seus serviços, a validação do consentimento, desses dados, devem ser observados em todas as fases do tratamento da informação (pré – art. 7º,I; durante - art. 7º, §5º e pós - art. 8º, § 5º e 6º; art. 9º).

Soma-se a isso, o requerimento de concessão seja específico ao se tratar dos dados sensíveis e, ao tratar dos alunos (crianças e adolescentes) - (art. 14, §1º), o consentimento deve ser dado por um dos pais.

Na questão 4, acerca do tratamento de dados pessoais que engloba desde a coleta até a eliminação, são realizados de duas formas: manual e via sistema de gerenciamento. Quando, por algum motivo, os dados pessoais não constam no banco de dados da biblioteca, faz-se necessário realizar a localização desse usuário no sistema integrado e verificar se há informações incompletas que impeçam as

atividades de circulação do acervo. Em caso de impedimento, o Núcleo de Informação e Tecnologia (NIT) ou a própria equipe da biblioteca podem realizar o cadastro e habilitação de usuário para utilização dos serviços de circulação (empréstimo, devolução e renovação).

Nesse caso, a Escola precisa informar aos responsáveis a checagem dos dados dos alunos no sistema integrado, considerando a transparência de suas ações. Essa checagem deve ser feita pelo funcionário da Escola que trabalha diretamente com a proteção de dados.

Para responder à última questão, foi apresentado à entrevistada os princípios dispostos na LGPD (finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, responsabilização e prestação de contas, e não discriminação), que devem ser observados na realização do tratamento de dados pessoais. Posteriormente, foi pedido à participante que fizesse breves comentários sobre como esses dispositivos poderiam ser cumpridos dentro da biblioteca escolar.

Quadro 2- Comentários da questão 5

<b>Princípios da LGPD</b>	<b>Finalidade dos dados</b>
Finalidade	Nesse caso, a biblioteca sujeita-se a esse princípio quando realiza o cadastro do usuário, seja via sistema ou de forma manual, e também quando solicita somente os dados necessários para o acesso aos serviços de circulação.
Necessidade	Obedece ao princípio da necessidade quando o usuário, por exemplo, se desvincula da instituição e, por consequência, tem os seus dados excluídos da base de dados. Outra situação, é quanto à emissão do comprovante de empréstimo do usuário, o qual deve ser assinado para garantir a responsabilidade do usuário pela guarda do material.
Segurança	O comprovante de empréstimo domiciliar funciona como um documento legal que permite ao usuário o conhecimento da prestação do serviço, a exemplo do nome do usuário registrado, do título emprestado, bem como da data de empréstimo, devolução e instruções em caso de perda e/ou danos ao item. Com o propósito de preservar as informações dos usuários no sistema e no empréstimo manual, o acesso a esses dados é restrito apenas aos funcionários da biblioteca e às pessoas devidamente autorizadas.
Adequação	A biblioteca no processo de coleta de dados não solicita dados pessoais sensíveis, por não serem adequados à finalidade do cadastro do usuário para utilização dos serviços deste espaço.

Livre acesso	Os usuários têm acesso aos seus comprovantes de empréstimo e também podem solicitar consulta ao histórico de títulos emprestados. Ainda não há um sistema que disponibilize por meio digital o acesso a essas informações.
Qualidade dos dados	O acesso a esses dados são claros, com valor de prova e atualizados.
Transparência	A biblioteca deixa claro aos seus usuários que os dados coletados serão utilizados para realizar os serviços de empréstimos, de renovação e devolução. Isso é explicado nos treinamentos de usuários realizados com as turmas.
Responsabilização e prestação de contas	Quanto à responsabilidade, acredito que se aplique ao profissional bibliotecário, uma vez que lida com os dados pessoais e cabe a ele a prestação de contas, caso haja desconformidade com o tratamento das informações de seus usuários.
Não-discriminação	Como exemplo, procura-se evitar que outras pessoas tenham acesso ao histórico de empréstimo domiciliar de usuários para que não surjam situações constrangedoras em função do histórico de determinado aluno.

Fonte: Elaboração da pesquisadora (2023)

Destaca-se que o intuito da LGPD não é impedir as ações da biblioteca escolar estudada, pois o seu Art. 2º declara um dos seus fundamentos que é o desenvolvimento científico e tecnológico, onde a biblioteca contribui diretamente. Todavia, para que isso ocorra é preciso que haja o uso responsável das informações dos seus usuários.

Em seguida, aplicou-se entrevista com o consultor em SI da escola (Apêndice B) acerca da LGPD e seus impactos na instituição de ensino, obtendo-se os seguintes resultados, apresentados com seus respectivos comentários.

Quando questionado sobre a vigência da LGPD e sua aplicabilidade às instituições de ensino, o entrevistado respondeu que mediante a necessidade de adequação e para estar em conformidade com a lei, em fevereiro do ano de 2019, começou-se a implementar a legislação em suas atividades e rotinas administrativas.

A aplicação de medidas técnicas e organizacionais na Escola investigada sinaliza, em um primeiro momento, a busca da adequação na garantia da proteção de dados dos discentes.

Na questão 2, foi solicitado que o sujeito comentasse sobre as medidas de segurança utilizadas para o correto tratamento de dados pessoais (coleta, utilização, armazenamento e eliminação). Foi respondido que não há medidas definidas que se

apliquem a todas as situações, mas que são implementadas com base na realização de diagnóstico e *Data Mapping*.

De acordo com Lacerda (2022), o mapeamento de dados, mais conhecido como *Data Mapping*, consiste em um processo de mapeamento para identificação dos dados pessoais existentes dentro de uma organização para o correto tratamento das informações.

A unidade de análise, não só mapeia os processos, como também mapeia as ações de tratamento de dados de transferência de dados, ou seja, o compartilhamento dos dados pessoais (conhecido como *Data Flow Mapping*), seja ele para áreas dentro da organização ou para empresas parceiras ou terceiros. Por fim, na mesma planilha do *Data Flow Mapping* é realizado a análise de risco dos tais compartilhamentos (Lacerda, 2022, p. 25).

Como exemplo, o entrevistado respondeu que realiza atividades de conscientização, ajustes de *software*, *hardwares*, monitoramento, rastreabilidade e permissões, isso considerando o ponto de vista técnico, pois assuntos relacionados à área jurídica ficam a encargo de uma empresa terceirizada de advocacia.

Na questão 3, perguntou-se ao respondente se o encarregado de dados tinha conhecimento sobre o tratamento de dados pessoais realizados pela biblioteca, obteve-se uma resposta negativa, o mapeamento de dados foi iniciado neste ano e ainda não foi concluído. A previsão é de que até junho de 2024 todas as áreas mapeadas sejam concluídas. Com base nessa resposta, um dos fatores pelo qual a biblioteca, enquanto setor, não tenha passado por esse processo, deve-se à recente implantação desse espaço na Escola A.

Nesse contexto, é preciso ressaltar que a escola deve estar comprometida com o tratamento dos dados dos alunos e, que não coletam somente essas informações pessoais, mas também, da família, colaboradores e visitantes. Daí a necessidade em reverem os documentos que são coletados e arquivados e criar ou revisar sua política de privacidade.

Em relação à pergunta 4, constatou-se a existência de uma política de privacidade de dados, a qual é disponibilizada no site da instituição, de livre acesso e para conhecimento de todos.

Complementando a questão anterior, o controlador é caracterizado como pessoa natural ou jurídica de âmbito público ou privado, que realiza a tomada de decisões referente ao tratamento de dados pessoais. Nesse caso, de acordo com a resposta obtida, fica a encargo do Grupo institucional. Quanto ao operador, designa-

se como aquele que realiza o tratamento de dados pessoais em nome do controlador, assim como o controlador, pode ser pessoa jurídica ou física, de direito público ou privado. Na Escola A, considera-se como operador os usuários e parceiros com os quais os dados são compartilhados. O encarregado de dados ou o DPO, por sua vez, é a pessoa indicada pelo controlador e operador para mediar a comunicação entre o Grupo e a ANPD. Nesse quesito, o encarregado de dados fica sob a responsabilidade de uma empresa jurídica terceirizada.

Na questão 6, evidencia-se que foram realizados treinamentos com colaboradores de diversas áreas da Escola A para que tenham conhecimentos sobre a LGPD e aplicabilidade das disposições na prática. Outro ponto mencionado, foi que esses treinamentos acontecem anualmente e de forma constante, considerando a entrada de novos colaboradores.

Na questão 7, foi perguntado sobre a possibilidade de implementação de mudanças no que tange à LGPD e o tratamento de dados dos usuários. A resposta afirmativa parte do pressuposto de que as mudanças dependem da verificação no *Data Mapping*, dentre as medidas tomadas, implementou-se em áreas consideradas “críticas”, a exemplo da Secretária e Atendimento ao Cliente.

Diante das respostas coletadas pelos entrevistados, percebe-se que ambos compreendem satisfatoriamente a Lei de Geral de Proteção de Dados, e buscam implementar ações consoante à lei para o correto tratamento dos dados da comunidade escolar, resguardando o direito de proteção e privacidade dos dados.

## 5 CONSIDERAÇÕES FINAIS

A LGPD é um marco importante na legislação brasileira que impacta os diversos setores da sociedade e muitas áreas do conhecimento, inclusive o campo da Biblioteconomia. Mediante os avanços tecnológicos ao longo da história, buscou-se implementar legislações que regulassem acerca da proteção de dados, no intuito de criar um cenário de segurança jurídica às informações pessoais coletadas por instituições públicas e particulares.

Este estudo buscou verificar a aplicabilidade da LGPD em uma instituição de ensino particular, mais especificamente, no âmbito da biblioteca escolar, mediante um estudo de caso. E esta temática é de suma importância para a área da Biblioteconomia, dado que as bibliotecas, enquanto espaços de informação não são exceções e, portanto, devem implementar as exigências da lei em suas atividades administrativas, através da criação de medidas que resguardem a privacidade dos dados dos indivíduos.

No referencial teórico, objetivou-se contextualizar e discorrer sobre as gerações das legislações acerca da proteção de dados pessoais no contexto internacional. Logo em seguida, traçou-se um percurso histórico das legislações nacionais antecedentes à Lei Geral de Proteção de Dados, cujo surgimento foi influenciado pelo regulamento europeu- GDPR. Apresentou-se ainda, conceitos que serviram de base para o entendimento deste estudo, a exemplo do conceito de privacidade, reconhecido como direito fundamental e humano. Para tanto, utilizou-se como método o estudo de caso em uma biblioteca escolar sediada nas dependências de uma instituição de ensino.

Com base na revisão de literatura e nos dados coletados durante a aplicação da entrevista com a responsável pela biblioteca e pelo consultor em SI, os principais resultados foram: a biblioteca da Escola A busca implementar as disposições da LGPD em sua rotina diária, principalmente no que se refere ao tratamento de dados pessoais dos usuários desde a coleta até a eliminação, levando em consideração essa base legal.

Nesse sentido, no âmbito da biblioteca, a coleta, a utilização e o armazenamento das informações pessoais dos usuários são feitas através de um sistema de gerenciamento bibliotecário. Esse sistema de gestão integrado tem como principais características: facilitar a gestão e a tomada de decisão por ser composto de vários módulos que atendem às necessidades de cada setor.

Nesse contexto, quando se trata de desligamento funcional, por exemplo, o usuário depois da emissão do nada consta, deixa de ser vinculado à biblioteca e têm os seus dados pessoais excluídos do sistema. Todavia, os dados permanecem armazenados em base de dados de outros segmentos, visto que a não exclusão dessas informações são amparadas por outras legislações, que disciplinam sobre a permanência dos dados.

Os dados pessoais identificados no sistema de base de dados foram os relativos à (ao): cadastro de usuário para utilização dos serviços de empréstimo domiciliar, renovação, reserva, devolução, consulta de débitos e emissão de nada consta; e cadastro de autores e editoras. Por estar passando pelo processo de finalização do processamento técnico do acervo, alguns livros são emprestados mediante a coleta de dados pessoais como: nome completo, segmento, e-mail e turma. Quando os serviços são realizados via sistema, é solicitado apenas o nome do usuário e os demais dados são coletados no momento de ingresso do usuário na instituição de ensino.

Em vista dos aspectos mencionados, faz-se necessário deixar claro que, ao entrar na instituição, os dados pessoais dos sujeitos são coletados com a finalidade de formalizar relações contratuais entre as partes. A princípio, a finalidade não é a utilização dos serviços da biblioteca, mas uma vez que este indivíduo se dirija à biblioteca para ter acesso aos serviços de circulação, deverá fornecer mais uma vez os seus dados pessoais. Contudo, aqueles que não utilizarem os serviços da biblioteca, não terão seus dados registrados e habilitados.

Nesta pesquisa, um fator limitador para alcançar maiores resultados foram as poucas literaturas encontradas sobre essa temática. Ao passo em que a LGPD é amplamente discutida desde a sua entrada em vigor, há poucas publicações sobre este tema relacionadas à área da Biblioteconomia.

Com este estudo, pretende-se contribuir com discussões acerca da LGPD em instituições de ensino, e de como esta Lei é percebida no contexto das bibliotecas escolares. Como sugestão para o desenvolvimento de pesquisas futuras, recomenda-se o estudo da LGPD em outros ambientes informacionais, evidenciando o caráter interdisciplinar da Biblioteconomia em outras áreas do conhecimento.

## REFERÊNCIAS

- ANDRADE, M. L.; ANDADE, D. C. M.; REBOUÇAS, G. M. **A proteção de dados pessoais sob o olhar do “Grande Irmão”**: a ingerência política da ANPD em meio à era da infomação. *Revista Eletrônica Direito e Sociedade*, Canoas, v. 11, n. 1, p. 35-53, jun. 2023. Disponível em: <https://revistas.unilasalle.edu.br/index.php/redes/article/view/10266>. Acesso em: 11 out. 2023.
- ANDRADE, T. M. N. Bibliotecas: lugar de memória e de preservação- o caso da Biblioteca Nacional do Brasil. *Patrimônio e Memória*, São Paulo, v. 4, n. 2, p. 17-34, jun. 2009. disponível em: <https://pem.assis.unesp.br/index.php/pem/article/view/41/499>. Acesso em: 27 nov. 2023.
- ASSMANN, J. **O direito à autodeterminação informativa no direito germânico e brasileiro**. 2014. 65 p. Trabalho de Conclusão de Curso- Universidade Federal de Santa Catarina, Florianópolis, SC, 2014. Disponível em: <https://repositorio.ufsc.br/bitstream/handle/123456789/117169/Jhonata%20Assmann%20TCC%20pdfa.pdf?sequence=1&isAllowed=y>. Acesso em: 20 out. 2023.
- BADIA, Gilbert. Alemanha oriental: sete anos de unificação. **Crítica Marxista**, São Paulo, Xamã, v.1, n.5, 1997, p.27-39. Disponível em: [https://www.ifch.unicamp.br/criticamarxista/arquivos\\_biblioteca/artigo32Artigo1.2.pdf](https://www.ifch.unicamp.br/criticamarxista/arquivos_biblioteca/artigo32Artigo1.2.pdf). Acesso em: 19 dez. 2023.
- BELÉM, F. B. Gestão documental sistêmica e as adversidades na implantação de um sistema de arquivos na esfera governamental. **Revista do Arquivo**, São Paulo, n. 3, p. 2-16, 2016. Disponível em: [http://www.arquivoestado.sp.gov.br/revista\\_do\\_arquivo/03/pdf/BELEM\\_\\_Fabiane\\_Maques\\_-\\_Gestao\\_documental\\_sistematica\\_e\\_as\\_adversidades\\_na\\_implantacao\\_de\\_um\\_sistema\\_de\\_arquivos\\_na\\_esfera\\_governamental.pdf](http://www.arquivoestado.sp.gov.br/revista_do_arquivo/03/pdf/BELEM__Fabiane_Maques_-_Gestao_documental_sistematica_e_as_adversidades_na_implantacao_de_um_sistema_de_arquivos_na_esfera_governamental.pdf). Acesso em: 06 jan. 2022.
- BEZERRA, J. M. de V. Aplicabilidade da Lei nº12.737/12 sobre crimes cibernéticos. **Revista Interdisciplinar Encontro das Ciências – RIEC**, Icó, Ceará, v.5, n.2, p. 41-68, maio/ago. 2022. Disponível em: <https://riec.univs.edu.br/index.php/riec/article/view/246/195>. Acesso em: 21 out. 2023.
- BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Código de Defesa do Consumidor. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/l8078compilado.htm](https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm). Acesso em: 10 out. 2023.
- BRASIL. **Lei nº 12.414, de 09 de junho de 2011**. Lei do Cadastro Positivo. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2011/lei/l12414.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm). Acesso em: 15 out. 2023.

BRASIL. **Lei nº 12.737/2012. 2011.** Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_Ato2011-2014/2012/Lei/L12737.htm#art2](http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm#art2). Acesso em: 10 nov. 2023.

BRASIL. [**Constituição (1988)**]. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, [2019]. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 29 out. 2023.

BRASIL. **Lei nº 9.507, de 12 de novembro de 1997.** Regula o direito de acesso a informações e disciplina o rito processual do habeas data. Brasília, DF: Presidência da República, [1997]. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/LEIS/L9507.htm](http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm). Acesso em: 29 out. 2023

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF: Presidência da República, [2011]. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2011/lei/l12527.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm). Acesso em: 22 out. 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, [2018]. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm). Acesso em: 22 out. 2023.

BRASIL. **Lei nº 13.709/18, de 14 agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: [planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm). Acesso em: 10 out. 2023.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019.** Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidência da República, [2019]. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2019/lei/l13853.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm). Acesso em: 28 out. 2023.

BURILLE, J. R. P. **A proteção de dados pessoais amparada pela LGPD:** um estudo sobre os impactos causados no marketing digital. 2022. 34 p. Trabalho de Conclusão de Curso- Centro Universitário FADERGS, Porto Alegre, 2022. Disponível em: <https://repositorio.animaeducacao.com.br/bitstream/ANIMA/23041/1/TRABALHO%20DE%20CURSO%20JULIANA%20PACHECO.pdf>. Acesso em: 5 nov. 2023.

CASTELLS, Manuel. **A Galáxia Internet.** Lisboa. Fundação Calouste Gulbenkian, 2004.

CRAVO, D. C.; CUNDA, D. Z. G. da; RAMOS, R. (orgs.). **Lei Geral de Proteção de Dados e o poder público.** Porto Alegre: Centro de Estudos de Direito Municipal,

2021. 223 p. Disponível em:

[https://lproweb.procempa.com.br/pmpa/prefpoa/pgm/usu\\_doc/ebook\\_lgpd\\_e\\_poder\\_publico\\_23052021.pdf](https://lproweb.procempa.com.br/pmpa/prefpoa/pgm/usu_doc/ebook_lgpd_e_poder_publico_23052021.pdf). Acesso em: 25 out. 2023.

CRESPO, M. Proteção de Dados Pessoais e o Poder Público: noções essenciais. In: CRAVO, D. C.; CUNDA, D. Z. G. DA.; RAMOS, RAFAEL. **Lei Geral de Proteção de Dados e o poder público**. Porto Alegre: Centro de Estudos de Direito Municipal, 2021. 223 p. Disponível em:

[https://lproweb.procempa.com.br/pmpa/prefpoa/pgm/usu\\_doc/ebook\\_lgpd\\_e\\_poder\\_publico\\_23052021.pdf](https://lproweb.procempa.com.br/pmpa/prefpoa/pgm/usu_doc/ebook_lgpd_e_poder_publico_23052021.pdf). Acesso em: 05 jan. 2022.

DONEDA, D. Da privacidade à proteção de dados pessoais. Rio de Janeiro. Renovar, 2020. 364 p.

ESPANHA. [Constituição (1978)]. **Constituição Espanhola**. Madri: Agencia Estatal Boletín Oficial del Estado, 2020. Disponível em:

[https://www.boe.es/biblioteca\\_juridica/codigos/abrir\\_pdf.php?fich=387\\_Constitucion\\_Espanola\\_Constituicao\\_Espanhola.pdf](https://www.boe.es/biblioteca_juridica/codigos/abrir_pdf.php?fich=387_Constitucion_Espanola_Constituicao_Espanhola.pdf). Acesso em: 20 dez. 2023.

FLÔRES, M. R. de; SILVA, R. L. da . Desafios e perspectivas da proteção de dados pessoais sensíveis em poder da administração pública: entre o dever público de informar e o direito do cidadão de ser tutelado. **Revista de Direito**, [S. l.], v. 12, n. 02, p. 01–34, 2020. DOI: 10.32361/2020120210327. Disponível em:

<https://periodicos.ufv.br/revistadir/article/view/10327>. Acesso em: 10 set. 2023.

FACHIN, O. **Fundamentos de metodologia**. 5. ed. São Paulo: Saraiva, 2005. Disponível em:

<http://maratavarespsictics.pbworks.com/w/file/fetch/74302802/FACHIN-Odilia-fundamentos-de-Metodologia.pdf>. Acesso em: 03 jan. 2022.

GASIOLA, G. G. **Criação e desenvolvimento da proteção de dados na Alemanha**. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-daprotecao-de-dados-na-alemanha-29052019>. Acesso em: 13 set. 2023.

GIL, A. C. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008. 220 p. Disponível em: <https://ayanrafael.files.wordpress.com/2011/08/gil-a-c-mc3a9todos-e-tc3a9nicas-de-pesquisa-social.pdf>. Acesso em: 03 jan. 2022.

GUERRA, S. Globalização, informação e o direito fundamental à privacidade. **Revista do Programa Avançado de Cultura Contemporânea**, 2015, ano 3, v. 1. Disponível em: <http://revistazcultural.pacc.ufrj.br/globalizacao-informacao-e-o-direito-fndamental-a-privacidade-de-sidney-guerra/> Acesso em: 22 out. 2023.

HARTMANN, G. H.; PATZ, S. R.; PIAIA, T. C. O impacto da autodeterminação informativa na proteção de dados pessoais e no direito ao esquecimento. **Revista DIREITO UFMS**, Campo Grande, MS, v.7, n. 1, p. 154-167, jan./jun. 2021. Disponível em: <https://periodicos.ufms.br/index.php/revdir/article/view/14482>. Acesso em: 10 set. 2023.

JUNKES, G. da S. **Evolução da tecnologia da informação e comunicação (TIC) e seus benefícios para as empresas**. 2014. 47 f. Trabalho de Conclusão de Curso (Bacharelado em Administração) - Universidade do Extremo Sul Catarinense, Criciúma, SC, 2014. Disponível em: <http://repositorio.unesc.net/bitstream/1/2879/1/GUILHERME%20DA%20SILVA%20JUNKES.pdf>. Acesso em: 25 nov. 2023.

LACERDA, L. C. de. **O uso da inteligência artificial na gestão da inovação tecnológica**: automatização do processo de mapeamento de dados. 2022. 69 f. Trabalho de Conclusão de Curso (Graduação em Engenharia de Produção) - Escola de Engenharia de Petrópolis, Universidade Federal Fluminense, Petrópolis, 2022. Disponível em: <https://app.uff.br/riuff/bitstream/handle/1/25224/LIDIA%20CORREA%20DE%20LACERDA.pdf?sequence=1&isAllowed=y>. Acesso em: 18 nov. 2023.

LAKATOS, E. M.; MARCONI, M. de A. **Fundamentos de metodologia científica**. 4. ed. São Paulo: Atlas, 1992. Disponível em: [https://forumturbo.org/wp-content/uploads/wpforo/default\\_attachments/1553321464-Metodologia-do-trabalho-cientifico-Eva-M-Lakatos-e-Marina-de-A-Marconi.pdf](https://forumturbo.org/wp-content/uploads/wpforo/default_attachments/1553321464-Metodologia-do-trabalho-cientifico-Eva-M-Lakatos-e-Marina-de-A-Marconi.pdf). Acesso em: 03 jan. 2022.

LE MOS, A. N. L. E.; PASSOS, E. A adequação das bibliotecas à Lei Geral de Proteção de Dados. **Cadernos de Informação Jurídica**, Brasília, v. 7, n. 1, p. 85-103, jan./jun. 2020. Disponível em: <http://www.cajur.com.br/>. Acesso em: 20 nov. 2023.

LOSANO, M. G. A lei alemã sobre a proteção dos dados. *Revista da Procuradoria-Geral do Estado*, Porto Alegre, v. 11, n. 29, p. 11- 22, 1981. Disponível em: <https://www.pge.rs.gov.br/upload/arquivos/201703/23121859-rpge29.pdf>. Acesso em: 10 out. 2023.

LUGATI, L. N.; ALMEIDA, J. E. de. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. **Revista de Direito**, [S. l.], v. 12, n. 02, p. 01–33, 2020. DOI: 10.32361/2020120210597. Disponível em: <https://periodicos.ufv.br/revistadir/article/view/10597>. Acesso em: 12 set. 2023.

MACHADO, Joana de Moraes Souza. A expansão do conceito de privacidade e a evolução na tecnologia de informação com o surgimento dos bancos de dados. **Revista da AJURIS**, v. 41, n. 134, jun. 2014. Disponível em: <https://revistadaajuris.ajuris.org.br/index.php/REVAJURIS/article/view/206/142>. Acesso em: 23 out. 2023.

MELO, P. B. de. Polêmicas no jornalismo do século XXI: discussões a partir da Revista Carta Capital. Dossiê temático: Wikileaks – cibercultura e política, **Revista Contemporânea Comunicação e Cultura**, Salvador- BA, v. 9, n. 9, p. 260-280, ago. 2011. Disponível em: <https://periodicos.ufba.br/index.php/contemporaneaposcom/article/view/5043/3889>. Acesso em: 07 de jan. 2024.

MENDES, L. S. **A Lei Geral de Proteção de Dados Pessoais**: um modelo de aplicação em três níveis. São Paulo: Ed. RT, 2019. p. 35-56. Caderno Especial LGPD. Disponível em:

[https://edisciplinas.usp.br/pluginfile.php/7695210/mod\\_resource/content/1/2%20-%20Revista%20de%20Direito%20ao%20consumidor%2C%20V.%20130%2C%20p.%20471%2C%202020.pdf](https://edisciplinas.usp.br/pluginfile.php/7695210/mod_resource/content/1/2%20-%20Revista%20de%20Direito%20ao%20consumidor%2C%20V.%20130%2C%20p.%20471%2C%202020.pdf). Acesso em: 20 set. 2023.

MENKE, F. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. **Revista Jurídica Luso-Brasileira - RJLB**, Ano 5, nº 1, p. 781-809, 2019. Disponível em: [https://www.cidp.pt/revistas/rjlb/2019/1/2019\\_01\\_0781\\_0809.pdf](https://www.cidp.pt/revistas/rjlb/2019/1/2019_01_0781_0809.pdf). Acesso em: 23 set. 2023.

MILANESI, L. **Biblioteca**. São Paulo, SP: Ateliê Editorial, 2002. 107p.

MONTEIRO, R. L.; GOMES, M. C. O.; NOVAES, A. L.; MORIBE, G.; CAMARA, D. E. G.; GHERINI, P. M. de M. **Lei Geral de Proteção de Dados e GDPR**: histórico, análise e impactos. São Paulo; Baptista Luz Advogados, [s.d.]. 37 p. Disponível em: <https://baptistaluz.com.br/wp-content/uploads/2019/01/RD-DataProtection-ProvF.pdf>. Acesso em: 23 set. 2023.

NUNES, M. A.; LIRA, A. C. M.; GEHRKE, M. A biblioteca escolar e as crianças: novos conceitos, velhos desafios. **Acta Scientiarum. Education**, Maringá, v. 43, n. 1, p. 1-10. Disponível em: <https://periodicos.uem.br/ojs/index.php/ActaSciEduc/article/view/47845>. Acesso em: 23 nov. 2023.

OCDE. Organização para Cooperação e Desenvolvimento Econômico. **Diretrizes da OCDE sobre a proteção da privacidade e do fluxo transfronteiriço de dados pessoais**. 2013. Disponível em: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm#recommendation>. Acesso em 20 set. 2023.

OLMOS, M. de Q.; O.; BOLSON; FAVERA, R. B. D. A Ciberespionagem e a Privacidade sob o Crivo dos Direitos Humanos. **Revista Eletrônica Direito & TI, [S. l.]**, v. 1, n. 5, p. 5, 2016. Disponível em: <https://direitoeti.emnuvens.com.br/direitoeti/article/view/57>. Acesso em: 20 dez. 2023.

SÁ MARTINO, L. M. **Teoria das mídias digitais**: linguagens, ambientes e redes. 2. ed. Petrópolis, RJ: Vozes, 2014. 273 p.

SCHWAITZER, L.; NASCIMENTO, N.; COSTA, A. de S. Reflexões sobre a contribuição da gestão de documentos para programas de adequação à Lei Geral de Proteção de Dados Pessoais (LGPD). **Acervo**, v. 34, n. 3, p. 1-17, 31 ago. 2021. Disponível em: <https://revista.an.gov.br/index.php/revistaacervo/article/view/1732/1667>. Acesso em: 06 jan. 2022.

SILVA, A. P. da S. O caso do asilo diplomático de Julian Assange: três anos depois. **Revista da Faculdade de Direito da UERJ - RFD**, [S. l.], n. 30, p. 34–54, 2016. Disponível em: <https://www.e-publicacoes.uerj.br/rfduerj/article/view/18388>. Acesso em: 19 dez. 2023.

SILVA, V. J. da. **Proteção Geral de Dados**: comunidade Europeia x Brasil. 2019. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Universidade Federal de Santa Catarina, Florianópolis, SC, 2019. Disponível em: <https://www.univates.br/bduserver/api/core/bitstreams/cb6348ff-35c6-4e20-aa9a-5fcfbb029b4d/content>. Acesso em: 3 nov. 2023.

SIMÕES, A. L. **Comunicação na internet e a violação do direito à privacidade**: uma análise avaliativa das políticas e termos de uso na internet. 2017. 213 f. Dissertação (Mestrado em Comunicação Social) - Universidade Metodista de São Paulo, São Bernardo Campo. Disponível em: <http://tede.metodista.br/jspui/bitstream/tede/1715/2/Alessandra.pdf>. Acesso em: 15 out. 2023.

SIMÕES, A. L. **Comunicação e privacidade de dados na internet**: estudo sobre as percepções do usuário à luz da LGPD. 2021. 203 f. Tese (Doutorado em Comunicação Social) - Universidade Metodista de São Paulo, São Bernardo Campo. Disponível em: <file:///C:/Users/USER/Downloads/Tese%20Alessandra%20L%20Simoes2%20v8.pdf>. Acesso em: 20 nov. 2023.

PILATI, J. I.; OLIVO, M. V. C. de. Um novo olhar sobre o direito à privacidade: caso Snowden e pós-modernidade jurídica. **Sequência**, Florianópolis, n. 69, p. 281–300, jul. 2014. Disponível em: <https://www.scielo.br/j/seq/a/BKdjxJFTbXNPwJnnP4hk8kF/?format=pdf&lang=pt>. Acesso em: 28 out. 2023.

PINHEIRO, P. P. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018. Disponível em: <https://bibliotecadigital.tse.jus.br/xmlui/handle/bdtse/5974>. Acesso em: 20 out. 2023.

PORTUGAL. Decreto-Lei n.º 47344, de 25 de novembro de 1966. Aprova o Código Civil e regula a sua aplicação - Revoga, a partir da data da entrada em vigor do novo Código Civil, toda a legislação civil relativa às matérias que o mesmo abrange. **Diário do Governo**: série I, Lisboa, Portugal, n. 274, p. 1-464, 25 nov. 1966. Disponível em: <https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1966-34509075>. Acesso em: 20 dez. 2023.

PORTUGAL. [Constituição (1976)]. **Constituição da República Portuguesa**. 7. ed. Lisboa: Assembleia da República, 2022. 155 p. Disponível em: <https://www.parlamento.pt/ArquivoDocumentacao/Documents/CRPVIIrevisao.pdf>. Acesso em: 19 dez. 2023.

PT. **DIRECTIVA 95/46/CE**. Disponível em: <https://www.anacom.pt/render.jsp?contentId=965550>. Acesso em: 20 out. 2023

TAKAHASHI, T. (Org.). **Sociedade da Informação no Brasil**: livro verde. Brasília, Ministério da Ciência e Tecnologia, 2000. Disponível em: <https://www.ufmg.br/proex/cpinfo/cidadania/wp-content/uploads/2014/04/Livro-verde.pdf>. Acesso em: 26 dez. 2023.

TEIXEIRA, G. C. **O papel social da Lei Geral de Proteção de Dados no Brasil**. 2020. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Universidade do Sul de Santa Catarina, Araranguá, 2020. Disponível em: <https://repositorio.animaeducacao.com.br/bitstream/ANIMA/7514/1/Monografia%20Guilherme%20Cardoso%20Teixeira.pdf>. Acesso em: 18 dez. 2023

UNESCO. **Manifesto IFLA/UNESCO para biblioteca escolar**. 2002. Disponível em: <https://archive.ifla.org/VII/s11/pubs/portuguese-brazil.pdf>. Acesso em: 26 nov. 2023.

YIN, R. K. **Estudo de caso**: planejamento e métodos. 2.ed. Porto Alegre: Bookman, 2001. 200 p. Disponível em: [https://saudeglobaldotorg1.files.wordpress.com/2014/02/yin-metodologia\\_da\\_pesquisa\\_estudo\\_de\\_caso\\_yin.pdf](https://saudeglobaldotorg1.files.wordpress.com/2014/02/yin-metodologia_da_pesquisa_estudo_de_caso_yin.pdf). Acesso em: 04 jan. 2022.

## APÊNDICE A- INSTRUMENTO DE COLETA DE DADOS

O roteiro da entrevista abaixo foi elaborado pela discente de graduação Jessica Melo Santos sob a orientação da Prof.<sup>a</sup> Dr.<sup>a</sup> Dirlene Santos Barros com o intuito de descrever e analisar como a Lei Geral de Proteção de Dados tem papel no âmbito educacional e se insere no contexto da biblioteca escolar. Em face do exposto, solicito a sua colaboração para responder às seguintes questões desta entrevista. Importante ressaltar que todas as informações coletadas serão apresentadas e discutidas neste estudo, preservando sobretudo, a imagem da instituição.

1. A biblioteca tem acesso a dados pessoais da comunidade escolar? Que tipo de dados são esses?
2. Quais são os tipos de dados pessoais coletados na biblioteca para fins de utilização dos serviços?
3. De que forma ocorre o consentimento dos usuários no fornecimento de dados para utilização dos serviços biblioteconômicos?
4. Como é realizado o tratamento de dados pessoais (coleta, utilização, acesso, armazenamento, eliminação etc.) dos usuários da biblioteca?
5. A Lei Geral de Proteção de Dados prevê princípios que devem ser observados na realização do tratamento de dados pessoais. De que forma a biblioteca obedece a cada um desses princípios (finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, responsabilização e prestação de contas, e não discriminação)?

## APÊNDICE B- INSTRUMENTO DE COLETA DE DADOS

O roteiro da entrevista abaixo foi elaborado pela discente de graduação Jessica Melo Santos sob a orientação da Prof.<sup>a</sup> Dr.<sup>a</sup> Dirlene Santos Barros com o intuito de descrever e analisar como a Lei Geral de Proteção de Dados tem papel no âmbito educacional e se insere no contexto da biblioteca escolar. Em face do exposto, solicito a sua colaboração para responder às seguintes questões desta entrevista. Importante ressaltar que todas as informações coletadas serão apresentadas e discutidas neste estudo, preservando sobretudo, a imagem da instituição.

1. A LGPD entrou em vigor em setembro de 2020, exceto os dispositivos que disciplinam sobre a aplicação de sanções administrativas. Nesse sentido, em que momento a Escola A buscou se adequar à lei?
2. Quais medidas de segurança são necessárias no momento da coleta, utilização, armazenamento e eliminação de dados pessoais?
3. O setor responsável pela proteção de dados da Escola A tem conhecimento de como os dados pessoais são tratados na biblioteca?
4. Existe um regulamento ou política específica para o tratamento de dados pessoais na escola?
5. No escopo da lei, prevê-se as funções de controlador, operador e encarregado de dados que participam do processo de tratamento de dados. Quem ocupa esses papéis e quais as funções desempenhadas por cada um dentro da Escola A?
6. Na escola A, os colaboradores que lidam diariamente com dados passaram por algum treinamento e ou formação para conhecerem sobre a LGPD, no intuito de aplicarem às disposições da lei em suas atividades diárias?
7. Será implementada alguma mudança no que tange à LGPD no tratamento de dados dos usuários?