

**FACULDADE PARA O DESENVOLVIMENTO SUSTENTÁVEL DA AMAZÔNIA  
COORDENAÇÃO DO CURSO BACHARELADO EM DIREITO**

**DOUGLAS GONÇALVES DA SILVA**

**AVANÇO LEGISLATIVO ACERCA DA PRIVACIDADE A LUZ DA LEI GERAL DE  
PROTEÇÃO DE DADOS (LGPD)**

**PARAUPEBAS**

**2023**

**DOUGLAS GONÇALVES DA SILVA**

**AVANÇO LEGISLATIVO ACERCA DA PRIVACIDADE A LUZ DA LEI GERAL DE  
PROTEÇÃO DE DADOS (LGPD)**

Trabalho de Conclusão de Curso (TCC) apresentado a Faculdade Para o Desenvolvimento Sustentável da Amazônia (FADESA), como parte das exigências do Programa do Curso de Direito para obtenção do título de Bacharel em Direito.

Orientadora: Me. Fernanda Lopes de Freitas Rodrigues.

**PARAUAPEBAS**

**2023**

**Da Silva, Douglas Gonçalves**

**Avanço legislativo acerca da privacidade a luz da lei geral de proteção de dados (LGPD);** Fernanda Lopes de Freitas Rodrigues 2023.

51 f.

Trabalho de Conclusão de Curso (Graduação) – Faculdade para o Desenvolvimento Sustentável da Amazônia - FADESA, Parauapebas – PA, 2023.

Palavras – Chave LGPD; RGPD; Privacidade; Dados pessoais; Direito fundamental

**Nota:** A versão original deste trabalho de conclusão de curso encontra-se disponível no Serviço de Biblioteca e Documentação da Faculdade para o Desenvolvimento Sustentável da Amazônia – FADESA em Parauapebas – PA.

Autorizo, exclusivamente para fins acadêmicos e científicos, a reprodução total ou parcial deste trabalho de conclusão, por processos fotocopiadores e outros meios eletrônicos.

Comitê de Ética

Protocolo nº:

Data:

**FACULDADE PARA O DESENVOLVIMENTO SUSTENTÁVEL DA AMAZÔNIA**

**AVANÇO LEGISLATIVO ACERCA DA PRIVACIDADE A LUZ DA LEI GERAL DE  
PROTEÇÃO DE DADOS (LGPD)**

**DOUGLAS GONÇALVES DA SILVA**

Trabalho de Conclusão de Curso apresentado a Faculdade Para o Desenvolvimento Sustentável da Amazônia (FADESA), como parte das exigências do Programa do Curso de Direito para obtenção do título de Bacharel em Direito.

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

**Banca Examinadora:**

CASSIA QUEREN  
CORREA  
FREITAS:02276374292

Assinado de forma  
digital por CASSIA  
QUEREN CORREA  
FREITAS:02276374292

---

Profª Esp. Cássia Queren Freitas - Membro

**MT**

---

Profº Me. Maicon Rodrigo Tauchert - Membro

Fernanda L. de F.  
Rodrigues

Assinado de forma digital por  
Fernanda L. de F. Rodrigues  
Dados: 2023.07.03 15:08:43 -03'00'

---

Profª Me. Fernanda Lopes de Freitas Rodrigues – Orientadora

Data de depósito do trabalho de conclusão \_\_\_\_/\_\_\_\_/\_\_\_\_

## DEDICATÓRIA

Dedico esta monografia à minha amada esposa, "**NENATA**", cujo amor, apoio e compreensão têm sido fundamentais em minha jornada acadêmica. Sua presença constante e incentivo incansável me motivaram a superar os desafios e a alcançar este importante marco em minha vida. Sua paciência, encorajamento e carinho incondicionais foram minha fonte de força nos momentos difíceis. Agradeço-lhe por compartilhar comigo alegrias, conquistas e também os obstáculos que encontramos no caminho. Seu amor e apoio são o alicerce do meu sucesso e gratidão. Esta monografia é dedicada a você, minha amada esposa, como uma expressão sincera de meu amor e apreço por tudo o que você representa em minha vida.

## **AGRADECIMENTOS**

Gostaria de expressar minha gratidão a Deus, que me sustentou durante todas as tribulações e me concedeu a força e o discernimento necessários para superar todos os desafios e concluir esta etapa. Agradeço, Senhor, por me guiar em todos os momentos, iluminando meu caminho e me protegendo de todos os perigos. Sua presença em minha vida tem sido a minha maior bênção e minha fonte de conforto e esperança. Mais uma vez, obrigado, meu Deus, por tudo o que tem feito por mim.

Gostaria de expressar todo o meu amor à minha amada mãe, que sempre se dedicou incansavelmente aos seus filhos, deixando suas próprias necessidades em segundo plano. Ela foi uma grande inspiração para mim e sempre esteve presente em todos os momentos importantes da minha vida. Sempre vibrou com todas as minhas vitórias e me apoiou em momentos difíceis. Sou eternamente grato por ser seu filho e por todo o amor incondicional que recebi dela. Te amo muito, mãe!

Agradeço à minha esposa Renata, que sempre me apoiou com amor incondicional e nunca mediu esforços em me proporcionar tudo o que eu precisava ao longo desta jornada. Agradeço por todo amor e companheirismo que compartilhamos. Obrigado, meu amor!

Gostaria de dedicar estas palavras aos meus filhos Guilherme e Gustavo, que todos os dias me desejaram boa sorte nas minhas aulas. O melhor presente que posso oferecer a vocês é o amor pela vida dos seres humanos, como Mahatma Gandhi disse: "Se eu pudesse deixar algum presente para você, deixaria o sentimento de amar a vida dos seres humanos." Agradeço por serem meus filhos e por me fazerem sentir tão amado. Vocês são a razão da minha vida e do meu amor pela humanidade.

Gostaria de expressar minha gratidão a Dona Ada e a todas as pessoas que, de alguma forma, me ajudaram a trilhar meu caminho e me tornar quem sou hoje. Agradeço por todo o suporte, ensinamentos e incentivos que recebi ao longo da minha jornada.

Agradeço à minha orientadora, Professora Fernanda Lopes de Freitas Rodrigues, por sua gentileza, tranquilidade e orientação durante a minha monografia. Sua experiência e conhecimentos foram inestimáveis.

Por fim, gostaria de expressar minha gratidão aos membros da banca por me proporcionarem a oportunidade de apresentar meu trabalho e por suas valiosas contribuições. Suas observações e sugestões foram fundamentais para o aprimoramento do meu estudo. Agradeço imensamente pela dedicação e pelo tempo investido na avaliação do meu trabalho. Obrigado a todos!

## RESUMO

O direito à privacidade é um princípio fundamental que protege a liberdade individual e a autonomia. Com a evolução tecnológica, a privacidade e a segurança dos dados tornaram-se um problema cada vez mais crítico. Para combater esses problemas, várias medidas estão sendo tomadas para proteger a privacidade e a segurança dos dados, como a implementação de leis de proteção de dados e privacidade, o uso de criptografia para proteger informações pessoais, o uso de firewalls e antivírus para proteger sistemas de computadores e o uso de medidas de segurança física para proteger dados armazenados em locais físicos. A LGPD é uma dessas leis e busca estabelecer uma proteção adequada para os dados pessoais, garantindo que as empresas e o governo colem, armazenem e usem esses dados de forma responsável e transparente. Além disso, é necessário que os cidadãos saibam como suas informações estão sendo usadas e que tenham a possibilidade de controlar e gerenciar seus próprios dados. O poder público é um dos principais coletores e tratadores de dados pessoais e, por isso, é de extrema importância que esteja sujeito às mesmas regras e obrigações estabelecidas pela LGPD.

**Palavras chaves:** direito a privacidade, privacidade, dados pessoais, lei geral de proteção de dados, LGPD, direito fundamental.



## **ABSTRACT**

The right to privacy is a fundamental principle that protects individual freedom and autonomy. With technological advancements, privacy and data security have become increasingly critical issues. To combat these problems, several measures are being taken to protect privacy and data security, such as the implementation of data protection and privacy laws, the use of encryption to protect personal information, the use of firewalls and antivirus software to protect computer systems, and the use of physical security measures to protect data stored in physical locations. The LGPD is one of these laws and aims to establish adequate protection for personal data, ensuring that companies and the government collect, store, and use this data responsibly and transparently. Additionally, it is necessary for citizens to know how their information is being used and to have the ability to control and manage their own data. The government is one of the main collectors and handlers of personal data, and therefore, it is extremely important that it is subject to the same rules and obligations established by the LGPD.

**Keywords:** right to privacy, privacy , personal data, general data protection law, LGPD, constitutional right

## LISTA DE ABREVIATURAS E SIGLAS

<b>ADI</b>	- Ação Direta de Inconstitucionalidade
<b>ANPD</b>	- Autoridade Nacional de Proteção de Dados
<b>CNIL</b>	- Comissão Nacional de Informática e Liberdades, na França
<b>CNPDPP</b>	- Comissão Nacional de Proteção de Dados Pessoais e da Privacidade
<b>COPPA</b>	- Lei de Proteção da Privacidade Online Infantil, nos Estados Unidos
<b>EUA</b>	- Estados Unidos da América
<b>LGPD</b>	- Lei Geral de Proteção de Dados
<b>PECR</b>	- Regulamentos de Privacidade e Comunicações Eletrônicas, no Reino Unido
<b>RG</b>	- Registro Geral
<b>RGPD</b>	- Regulamento Geral sobre a Proteção de Dados da União Europeia
<b>STF</b>	- Supremo Tribunal Federal
<b>STJ</b>	- Superior Tribunal de Justiça
<b>UE</b>	- União Europeia

## SUMARIO

1- Introdução .....	12
2.- Direito à privacidade.....	14
2.1- A Evolução histórica ao direito de privacidade.....	17
2.2- A evolução tecnológica e processamento de dados. ....	21
2.3- Proteção de dados pessoais como direito fundamental.....	24
2.4- A proteção de dados e os direitos da personalidade .....	26
3.- Historico das leis de proteção de dados e a privacidade na internet.....	29
3.1- A nova lei de proteção de dados pessoais no Brasil.....	31
3.2- Escopo de aplicação e princípios da LGPD. ....	34
3.3- O impacto econômico de uma lei geral de proteção de dados.....	36
4.- A lei 13.709/19 e o novo paradigma da privacidade .....	39
4.1-. Riscos de vazamento de dados para o indivíduo .....	40
4.2- Tratamento e responsabilidade do poder publico .....	41
5- Metodologia. ....	45
6- Conclusão .....	46
7- Referências Bibliográficas.....	47

## 1. INTRODUÇÃO

A proteção da privacidade é um direito fundamental reconhecido por muitos países ao redor do mundo, e com o crescente uso da tecnologia e a coleta de dados pessoais em larga escala, tornou-se essencial estabelecer leis que regulamentem o tratamento desses dados.

Nesse contexto, a Lei Geral de Proteção de Dados (LGPD) surge como um importante avanço legislativo no Brasil. A Lei 13.709/2018 - Lei Geral de Proteção de Dados tem por objetivo assegurar e proteger direitos fundamentais de liberdade e de privacidade e à proteção de dados pessoais da pessoa natural. A lei estabelece a definição de dado pessoal sensível em qualquer contexto relacionado ao tratamento de informações, incluindo dados obtidos através da internet, páginas da web e dispositivos conectados à rede, visando garantir a liberdade do desenvolvimento pessoal do indivíduo. Independentemente da localização da organização ou do centro de dados, bem como se é pública ou privada, a LGPD estabelece novas estruturas de governança, como a Autoridade Nacional de Proteção de Dados (ANPD) e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPDPP), dedicados exclusivamente à proteção de dados pessoais em qualquer operação de tratamento.

A LGPD também prevê exceções em que a lei não se aplica, como no tratamento de dados pessoais para fins exclusivamente particulares e não econômicos, além de situações específicas relacionadas à segurança pública, defesa nacional e investigação criminal.

O objetivo geral desta monografia é analisar o avanço legislativo da proteção da privacidade a luz da Lei Geral de Proteção de Dados (LGPD), identificando seus principais aspectos e contribuições para a proteção da privacidade no Brasil, bem como discutindo seus possíveis impactos nas empresas e na sociedade em geral. Como objetivos específicos iremos apresentar o contexto histórico e as principais leis de proteção de dados e privacidade em alguns países do mundo, definir os conceitos fundamentais da LGPD, como dados pessoais, dados pessoais sensíveis, tratamento de dados e consentimento; analisar a estrutura de governança estabelecida pela LGPD,

como a Autoridade Nacional de Proteção de Dados (ANPD) e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPDPP); discutir as exceções previstas na LGPD para o tratamento de dados pessoais; analisar os possíveis impactos da LGPD nas empresas e na sociedade em geral.

## 2- DIREITO À PRIVACIDADE

Uma das conquistas mais importantes da sociedade moderna é o reconhecimento do direito à privacidade como um direito fundamental. Esse direito é essencial para proteger a liberdade, a autonomia e a dignidade das pessoas, garantindo que elas possam manter uma esfera íntima e pessoal.

O direito à privacidade é um direito fundamental garantido pela maioria das constituições em todo o mundo. Esse direito envolve a proteção da vida privada das pessoas e de suas informações pessoais protege o indivíduo contra a divulgação ou exposição não autorizada de informações pessoais e a interferência na sua vida privada, familiar, lar e correspondência. Inclui o direito de controlar informações pessoais, de não ser vigiado ou monitorado sem justa causa, de não ser objeto de intromissões ilegítimas e de não ter informações pessoais utilizadas para fins discriminatórios.

O direito à privacidade é importante porque permite que as pessoas mantenham um espaço de liberdade e autonomia, longe do escrutínio público e governamental. Isso permite que os indivíduos sejam livres para desenvolver suas personalidades e expressar suas opiniões sem medo de perseguição ou retaliação.

Em um mundo cada vez mais digital, o direito à privacidade também se aplica à proteção dos dados pessoais. A coleta, o armazenamento e o uso de informações pessoais podem ser realizados por empresas, governos e outras organizações sem o conhecimento ou consentimento dos indivíduos afetados, o que pode violar o direito à privacidade. As leis de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (RGPD) na União Europeia, são projetadas para proteger o direito à privacidade, garantindo que os indivíduos tenham controle sobre seus dados pessoais e que as organizações processem esses dados de forma responsável e segura.

O direito à privacidade é um conceito fundamental dentro do direito, que diz respeito à proteção da intimidade e dos dados pessoais de um indivíduo. A seguir, apresento alguns conceitos da doutrina do direito à privacidade.

"The Right to Privacy", publicado em 1890 na Harvard Law Review, que é considerado um dos textos mais influentes na definição do direito à privacidade como um

direito fundamental, Warren e Brandeis desenvolveram a ideia de que a privacidade é um direito fundamental e que deve ser protegido pela lei, desenvolvendo os seguintes conceitos: Direito à solidão: o direito de estar sozinho e de ter momentos de privacidade, sem ser incomodado ou observado por terceiros. Direito à intimidade: o direito de controlar as informações pessoais que uma pessoa divulga sobre si mesma e que não deseja compartilhar com outras pessoas. Direito à reserva: o direito de se proteger contra a exposição pública não autorizada, incluindo a divulgação de fatos privados, como correspondência pessoal e fotografias. Direito a evitar a publicidade não solicitada: o direito de não ter o nome, a imagem ou a vida privada divulgados sem consentimento prévio e expresso.

Alan Westin, "Privacy and Freedom" (1967), defende que a privacidade é essencial para a dignidade humana, para a autonomia e para a liberdade individual. Ele argumenta que o direito à privacidade deve ser protegido por leis e instituições, e que a violação desse direito pode levar a uma diminuição da liberdade individual e da democracia. Portanto, assim como Warren e Brandeis, Westin também defende que a privacidade é um direito fundamental que deve ser protegido por lei e coleciona os seguintes conceitos relacionados ao direito à privacidade: Autonomia pessoal: o direito do indivíduo de controlar suas informações pessoais e decidir como e quando elas serão compartilhadas. Integridade pessoal: o direito do indivíduo de controlar seu próprio corpo e suas ações, e de não ser exposto a situações que possam afetar negativamente sua reputação. Limitação de acesso: o direito do indivíduo de controlar quem tem acesso às suas informações pessoais e em que circunstâncias essas informações podem ser divulgadas. Controle de informação: o direito do indivíduo de controlar as informações que são coletadas sobre ele e de ser informado sobre como essas informações serão utilizadas.

O livro "Direito e Internet: Liberdade de Expressão, Privacidade e Outros Temas", de Marcel Leonardi (2016) aborda diversos conceitos relacionados ao direito à privacidade na era digital. Segundo o autor, dados pessoais são informações que permitem a identificação de uma pessoa, como nome, endereço, telefone e CPF. Já a privacidade é o direito de cada indivíduo de manter suas informações pessoais e atividades fora do alcance de terceiros, protegendo sua intimidade e liberdade.

Para que uma empresa ou organização possa coletar, processar ou utilizar dados

personais, é necessário o consentimento prévio do titular dessas informações. Caso contrário, o processamento desses dados pode ser considerado ilegal.

Uma forma de garantir a privacidade dos dados pessoais é a anonimização, processo que transforma esses dados em dados não identificáveis. Além disso, é importante que as empresas e organizações adotem medidas de proteção de dados para garantir sua segurança.

O vazamento de dados é uma situação em que informações pessoais são divulgadas sem autorização, o que pode resultar em danos à privacidade, reputação e segurança dos indivíduos afetados. Já o direito ao esquecimento é o direito dos indivíduos de terem suas informações pessoais removidas da internet e de outros meios de comunicação digital, em determinadas circunstâncias.

As empresas e organizações que coletam, processam ou utilizam dados pessoais são responsáveis pela sua segurança e pela proteção da privacidade dos titulares dos dados, podendo responder civil e criminalmente em caso de violação.

A Constituição Federal de 1988 assegura a inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e telefônicas, ressalvadas as hipóteses previstas em lei para fins de investigação criminal ou instrução processual penal, mediante ordem judicial.

A Lei nº 12.965/2014 (Marco Civil da Internet) também estabelece a proteção do sigilo das comunicações realizadas pela internet, incluindo e-mails e mensagens eletrônicas, e prevê que o acesso aos registros de conexão e de acesso a aplicações de internet só pode ser realizado mediante ordem judicial, respeitando os requisitos legais.

As leis de proteção de dados, como a LGPD e o RGPD também desempenham um papel vital nessas proteções, estabelecendo regras e diretrizes para empresas, governos e outras organizações que lidam com dados pessoais, afim de preservar e evitar casos como os exemplos recentes de violações de privacidade, como por exemplo: o escândalo do Facebook e Cambridge Analytica (2018) um dos casos mais notáveis de violação de privacidade de dados na era da internet. A empresa de consultoria política Cambridge Analytica obteve acesso aos dados de cerca de 87 milhões de usuários do Facebook sem o consentimento explícito dessas pessoas, por meio de um aplicativo de teste de personalidade chamado "This Is Your Digital Life". Esses dados foram usados



para criar perfis psicológicos dos usuários e, em seguida, usados para direcionar anúncios políticos durante a campanha presidencial dos Estados Unidos em 2016. O Facebook foi multado por reguladores em vários países por não proteger adequadamente os dados dos usuários. O incidente também levou a mudanças significativas na política de privacidade do Facebook.

Uma das mais recentes polêmicas envolvendo o uso de tecnologia de reconhecimento facial foi da Clearview AI, uma empresa privada com sede nos EUA, em abril de 2021. Revelou-se que mais de 10 bilhões de imagens faciais foram coletadas pela empresa de reconhecimento facial sem o consentimento dos usuários. A empresa coletou as imagens a partir de redes sociais e outros sites na internet, e usou-as para criar um banco de dados de reconhecimento facial utilizado por agências de aplicação da lei em todo o mundo. Essa prática de coleta de imagens sem consentimento gerou preocupações sobre a privacidade e segurança dos dados biométricos dos indivíduos, especialmente considerando que as imagens foram coletadas sem o conhecimento ou autorização dos proprietários das imagens. A situação levantou questões sobre a necessidade de regulamentação mais rigorosa em torno da coleta e uso de dados biométricos, bem como a necessidade de proteger a privacidade dos usuários na era digital.

A agência francesa de vigilância da privacidade de dados, CNIL, ordenou que a Clearview AI pare de acumular e usar dados de pessoas residentes no país. O regulador disse que a empresa, usada como mecanismo de busca de rostos para ajudar agências de aplicação da lei e de inteligência em investigações, não pediu consentimento prévio daqueles cujas imagens foram coletadas online. "Esses dados biométricos são particularmente sensíveis, principalmente porque estão ligados à nossa identidade física (o que somos) e nos permitem ser identificados de uma maneira única", disse a autoridade (CNIL, 2021).

## **2.1 A EVOLUÇÃO HISTÓRICA AO DIREITO DE PRIVACIDADE**

Antes da criação das cidades-estado, "Polis", na Grécia Antiga e do desenvolvimento da economia monetária, a privacidade era uma questão menos

relevante na vida cotidiana. As pessoas geralmente viviam em comunidades rurais pequenas, onde as casas eram compartilhadas com a família e, às vezes, com outros parentes e amigos próximos. As atividades diárias eram realizadas em espaços públicos, como mercados ou templos, e a vida privada não era claramente definida.

A evolução da privacidade para o direito de privacidade pode ser observada desde a antiguidade, em diferentes culturas e sociedades. Na Grécia Antiga, a palavra “aikos” era usada para se referir ao espaço privado de uma pessoa, enquanto a polis era o espaço público. Essa distinção entre a esfera pública e privada influenciou a concepção de privacidade em sociedades posteriores.

Na Roma Antiga, a privacidade era valorizada principalmente pela classe aristocrática, eles consideravam suas atividades e discussões privadas como assuntos de importância estritamente pessoal e familiar, tinham o direito de se proteger de invasões e espionagem em suas residências. A partir do século III d.C., foram promulgadas leis que traziam certos direitos e proteções embora não fosse especificamente direcionado à proteção da privacidade dos cidadãos, pois enfatizava principalmente questões de propriedade.

Durante a Idade Média, a privacidade foi pouco valorizada, já que a vida em comunidade era predominante e a privacidade individual não era um conceito comum. Foi somente na Idade Moderna, com o surgimento da burguesia e a valorização da vida privada, que a privacidade voltou a ser um tema importante.

No entanto, algumas sociedades antigas tinham concepções de privacidade em alguns aspectos. Por exemplo, nas sociedades egípcias e mesopotâmicas, as mulheres tinham áreas privadas em casa para cuidar de si mesmas e de suas necessidades pessoais. Além disso, em algumas culturas pré-históricas, havia práticas de isolamento ou separação, como a reclusão das mulheres durante a menstruação.

Em geral, a ideia de privacidade como um direito individual e um valor social surgiu com a formação das sociedades urbanas e a crescente importância da propriedade privada. Com a construção de casas individuais e a delimitação de fronteiras territoriais, a privacidade começou a ser considerada um elemento essencial da vida privada e familiar.

A perspectiva histórica do direito à privacidade é importante para entender como

esse direito evoluiu ao longo do tempo e como as sociedades têm abordado a questão da proteção da privacidade.

A ideia de privacidade como um direito legal é relativamente recente na história. Na Grécia Antiga e em Roma, por exemplo, a privacidade era vista mais como uma questão moral do que legal. O direito à privacidade como um conceito legal começou a surgir no final do século XIX e início do século XX, com a crescente preocupação com a proteção dos indivíduos contra a invasão de sua privacidade.

Um marco importante na história do direito à privacidade foi o artigo de Samuel Warren e Louis Brandeis, "The Right to Privacy", publicado em 1890 na revista Harvard Law Review. Neste artigo, Warren e Brandeis argumentaram que a invasão da privacidade é uma violação dos direitos pessoais e que a lei deveria reconhecer e proteger esse direito.

O artigo de Warren e Brandeis foi inovador porque introduziu a ideia de que a privacidade não se limitava a um direito individual de manter informações em segredo, mas era um aspecto fundamental da liberdade e da autonomia pessoal. Eles argumentaram que a privacidade era necessária para garantir a livre expressão de ideias e pensamentos, bem como para evitar a interferência indevida do Estado e das instituições privadas na vida das pessoas. Essa nova visão da privacidade se tornou o ponto de partida para o conceito moderno de privacidade como um direito fundamental dos indivíduos, que deve ser protegido pela lei e respeitado por todas as instituições e indivíduos.

Nos Estados Unidos, o direito à privacidade foi reconhecido pela primeira vez em 1891, quando o estado de Massachusetts aprovou uma lei que proibia a publicação de fotografias de pessoas sem seu consentimento. A proteção da privacidade foi inicialmente abordada como um direito de propriedade, em que os indivíduos tinham o direito de controlar as informações sobre si mesmos. Posteriormente, foi reconhecido como um direito à privacidade, e a Suprema Corte dos EUA decidiu que a privacidade é um direito fundamental protegido pela Constituição. Embora o termo "privacidade" não seja mencionado explicitamente na Constituição.

Em outros países, a proteção legal da privacidade evoluiu de maneiras diferentes. Na Europa, a Convenção Europeia dos Direitos Humanos, de 1950, reconhece o direito

à privacidade como um direito fundamental, e muitos países europeus têm leis específicas que protegem a privacidade pessoal.

A Constituição de 1824 do Brasil, reconhecida também como Constituição do Império, outorgada pelo Imperador Dom Pedro I, não mencionava expressamente o direito à privacidade ou à intimidade. Isso não significa, porém, que esses direitos não fossem protegidos ou respeitados na época. Estabelecia a inviolabilidade do domicílio e a liberdade individual como direitos fundamentais dos cidadãos brasileiros. Segundo Fernandez (2020), há apenas referência ao sigilo da correspondência e à inviolabilidade do domicílio, não havendo uma proteção da privacidade por si só, pelo seu conteúdo ou por um aspecto mais subjetivo, mas sim uma proteção apenas contra a invasão, ou seja, o ato de romper uma barreira física.

O Código Criminal do Império, de 1830, previa penas para crimes como violação de correspondência e invasão de domicílio, o que indica uma preocupação com a proteção da privacidade individual.

Art. 129. Serão julgados prevaricadores os empregados publicos, que por affeição, odio, ou contemplação, ou para promover interesse pessoal seu:  
9º Subtrahirem, supprimirem, ou abrirem carta depois de lançada no correio; ou concorrerem para que outrem o faça.

Penas - de perda do emprego; de prisão por dous a seis mezes, e de multa correspondente á metade do tempo.

Se com abuso de poder commetterem os crimes referidos á respeito da carta dirigida por portador particular.

Penas - de prisão por vinte a sessenta dias, e multa correspondente á metade do tempo.

As penas em qualquer dos casos serão duplicadas ao que descobrir em todo, ou em parte o que na carta se contiver; e as cartas assim havidas não serão admittidas em Juizo. (Codigo Criminal do Imperio do Brazil, 1830)

Uma maior tutela dos direitos aos dados pessoais, frente ao princípio da privacidade foi consagrada diante da Declaração Universal dos Direitos Humanos, adotada pela Assembleia Geral das Nações Unidas em 10 de dezembro de 1948, reconhecendo o direito à privacidade como um direito fundamental do ser humano.

Art. 12º Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei. (Declaração Universal dos Direitos Humanos, 1948)

No entanto, é importante ressaltar que a concepção de privacidade e intimidade como direitos fundamentais, como é entendido hoje em dia, é resultado de um processo

histórico mais recente, influenciado por diversas correntes filosóficas e ideológicas. A Constituição de 1988, por exemplo, reconheceu expressamente o direito à privacidade e à intimidade como um direito fundamental dos cidadãos brasileiros.

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

[...]

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;

XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;

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)

A perspectiva histórica do direito à privacidade mostra que esse direito tem evoluído com o tempo, em resposta às mudanças na sociedade e às preocupações com a proteção dos direitos individuais. Hoje em dia, a proteção da privacidade é uma preocupação global, e muitos países têm leis e regulamentações para proteger a privacidade pessoal em vários aspectos da vida, incluindo a coleta e uso de informações pessoais por empresas, a vigilância governamental e a proteção da privacidade na Internet. Desde então, a noção de privacidade evoluiu e se expandiu para incluir outras dimensões além da privacidade física, como a privacidade das comunicações e a privacidade dos dados pessoais. A privacidade também foi reconhecida como um direito humano fundamental pela Organização das Nações Unidas e por muitos países em suas constituições e leis.

Nos últimos anos, com o rápido desenvolvimento da tecnologia e a crescente coleta e uso de dados pessoais, o direito à privacidade tornou-se ainda mais importante e complexo. Os governos e organizações enfrentam o desafio de encontrar um equilíbrio entre o acesso necessário aos dados para realizar atividades legítimas e a proteção da privacidade dos indivíduos.

## **2.2 A EVOLUÇÃO TECNOLÓGICA E PROCESSAMENTO DE DADOS**

Antes da era tecnológica, os meios de coleta de informações pessoais eram

principalmente manuais e físicos. As informações pessoais eram mantidas em arquivos e registros em papel, que eram armazenados em locais físicos, como gavetas, pastas e armários.

Os dados pessoais eram coletados por meio de formulários impressos, como formulários de registro de clientes, formulários de inscrição de emprego, fichas de pacientes em hospitais, formulários de inscrição de cartões de crédito, entre outros. Esses formulários geralmente eram preenchidos manualmente e coletados em mãos ou enviados pelo correio.

Também existiam outras formas de coleta de informações pessoais, como entrevistas, pesquisas, questionários e levantamentos realizados pessoalmente. Essas informações eram então digitadas ou registradas em arquivos físicos para armazenamento e referência futura.

Os meios de coleta de informações pessoais antes da era tecnológica eram menos invasivos e geralmente envolviam um processo mais demorado e manual. Houve uma ruptura da privacidade com a era tecnológica porque a tecnologia permitiu que as informações pessoais das pessoas fossem coletadas, armazenadas, compartilhadas e processadas de maneira mais fácil, rápida e em grande escala do que nunca. Antes da era da tecnologia, as informações pessoais eram principalmente mantidas em papel e armazenadas em locais físicos, o que dificultava o acesso e a manipulação dessas informações em grande escala.

As pessoas que utilizam smartphones, computadores pessoais e outros dispositivos eletrônicos estão de certa forma abrindo uma porta para sua intimidade e privacidade. Isso porque esses dispositivos muitas vezes coletam informações pessoais dos usuários, como localização, histórico de navegação na internet, contatos, entre outras.

A revolução da tecnologia da informação trouxe consigo diversos agentes que são responsáveis pela mudança do cenário tecnológico, e conseqüentemente pela transformação da sociedade. Alguns desses agentes são:

- Empresas de tecnologia: empresas como Google, Amazon, Facebook e Apple (conhecidas como GAFA) têm um papel central na revolução da tecnologia da informação, criando novas tecnologias e serviços que

transformam a forma como as pessoas se comunicam, trabalham e se relacionam.

- Desenvolvedores de software: os desenvolvedores de software são os responsáveis por criar as soluções tecnológicas que permitem que as empresas de tecnologia ofereçam serviços inovadores. Eles são responsáveis por programar, testar e implementar novas soluções.
- Usuários: os usuários da tecnologia da informação são outro agente importante na revolução da tecnologia da informação. Eles são os responsáveis por adotar as novas tecnologias e serviços oferecidos pelas empresas de tecnologia e utilizá-los em seu dia a dia.
- Governo: o governo também tem um papel importante na revolução da tecnologia da informação, sendo responsável por criar políticas e leis que regulamentam o uso da tecnologia e protegem os direitos dos cidadãos em relação à privacidade e segurança de dados.
- Hackers: hackers são indivíduos que possuem conhecimentos avançados em tecnologia da informação e podem utilizar esse conhecimento para fins legítimos ou maliciosos. Eles podem contribuir para a melhoria da segurança de sistemas e dados, mas também podem representar uma ameaça para a privacidade e segurança de informações.

A revolução da tecnologia da informação é impulsionada por uma série de agentes, incluindo empresas de tecnologia, desenvolvedores de software, usuários, governo e hackers. Cada um desses agentes desempenham um papel fundamental na transformação da sociedade e na construção de um futuro cada vez mais tecnológico.

Com a digitalização da informação, as informações pessoais das pessoas podem ser coletadas de várias maneiras, como através de dispositivos móveis, redes sociais, serviços online, entre outros. Essas informações podem ser usadas para fins de publicidade, marketing, análise de dados, pesquisas de mercado e outros fins comerciais.

No entanto, essa coleta e uso de informações pessoais também pode ser usada de maneira indevida ou prejudicial, como para roubo de identidade, fraude, assédio ou discriminação. Isso pode afetar a privacidade e a segurança das pessoas, especialmente quando os dados são compartilhados ou vendidos para terceiros sem o conhecimento ou

consentimento dos usuários.

O Fórum Econômico Mundial (2011), através de detido relatório sobre o assunto, classifica a obtenção massiva de dados de caráter pessoal em três vertentes, quais sejam, aqueles oferecidos voluntariamente através de redes sociais; aqueles observados, como nas hipóteses de geolocalização nos celulares; e aqueles inferidos, fornecidos para o estabelecimento de contratos. Por isso, é importante que as leis e regulamentações que visam proteger a privacidade dos usuários sejam atualizadas e aprimoradas para lidar com as novas tecnologias e práticas de coleta de dados.

A principal causa para a criação do Regulamento Geral de Proteção de Dados (RGPD) foi a necessidade de atualizar a legislação de proteção de dados pessoais na União Europeia (UE), que anteriormente era regulamentada pela Diretiva 95/46/CE, de 1995.

A Diretiva de 1995 já não era adequada para lidar com os desafios e as oportunidades que surgiram com o rápido desenvolvimento das tecnologias digitais e a crescente interconectividade global, que aumentou significativamente a quantidade de dados pessoais sendo processados e compartilhados em todo o mundo.

A RGPD (Regulamentação Geral de Proteção de Dados) foi um marco importante na regulamentação da proteção de dados pessoais na União Europeia, estabelecendo padrões rigorosos para o tratamento de dados pessoais e garantindo maior controle dos titulares sobre seus dados. A LGPD (Lei Geral de Proteção de Dados) brasileira, por sua vez, foi influenciada pela RGPD, uma vez que se inspirou nos princípios e diretrizes estabelecidos pela regulamentação europeia.

## **2.3 PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL**

A proteção de dados pessoais é reconhecida como um direito fundamental em muitos países, incluindo o Brasil, onde foi reconhecida expressamente pela Constituição Federal de 1988, em seu artigo 5º, inciso X.:

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. ( CF, BRASIL, 1988)

O reconhecimento da proteção de dados pessoais como direito fundamental



reflete a importância crescente dos dados pessoais na sociedade contemporânea e a necessidade de proteger esses dados contra o uso indevido ou abusivo. Dessa forma, a proteção de dados pessoais não é apenas uma questão de privacidade individual, mas também uma questão de direitos humanos e de garantia da liberdade e da dignidade da pessoa humana.

Isso significa que a proteção da privacidade e dos dados pessoais é um direito que deve ser garantido pelo Estado e respeitado por todas as organizações que coletam e processam esses dados. Também significa que as leis e políticas relacionadas à privacidade e proteção de dados devem ser elaboradas e aplicadas com base nesse princípio. Isso inclui a criação de regulamentações que garantam que as organizações que coletam e processam dados pessoais ajam de acordo com as leis de proteção de dados e protejam os direitos dos indivíduos.

Os direitos fundamentais têm um status especial e devem ser protegidos de maneira absoluta. Isso significa que, em situações em que há conflitos entre o direito a proteção de dados pessoais e outros interesses, o direito fundamental a proteção de dados deve ser priorizado.

No Brasil, em agosto de 2020, o STF julgou a ADI 6.387, uma Ação Direta de Inconstitucionalidade e decidiu pela constitucionalidade da LGPD. Os ministros entenderam que a proteção de dados pessoais é um direito fundamental e que a LGPD é necessária para garantir a proteção desse direito. A decisão afirmou que a privacidade e a proteção de dados são essenciais para a dignidade da pessoa humana, a liberdade e a autodeterminação, e que a LGPD é um importante instrumento para garantir esses valores.

Outro exemplo é a jurisprudência do STJ, que frequentemente analisa casos envolvendo a proteção da personalidade e da privacidade. Em um caso recente, o STJ decidiu que o Google não pode ser responsabilizado por imagens íntimas divulgadas na internet sem autorização, mas pode ser obrigado a remover os links que levam a essas imagens, protegendo assim a privacidade e a dignidade da pessoa afetada, conforme a jurisprudência recurso especial Nº 1912151 - SP (2020/0335308-9) data da publicação, 01/03/2023.

Decido.

1. A jurisprudência desta Corte firmou-se no sentido de que "o dano moral

decorrente de mensagens com conteúdo ofensivo inseridas no site pelo usuário não constitui risco inerente à atividade dos provedores de conteúdo, de modo que não se lhes aplica a responsabilidade objetiva prevista no art. 927, parágrafo único, do CC/02" (REsp 1308830/RS, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA, julgado em 08/05/2012, DJe 19/06/2012 - grifou-se).

Nos termos do art. 19 da lei 12.965/2014, o provedor somente será responsável civilmente, em razão de publicação gerada por terceiro, se descumprir ordem judicial determinando as providências necessárias para cessar a exibição do conteúdo ofensivo, com a finalidade de assegurar a liberdade de expressão e impedir a censura [grifou-se].

Com efeito, aplica-se a responsabilidade subjetiva do provedor de conteúdo nas hipóteses em que, depois de comunicado acerca de conteúdo ilícito, ou seja, que viola privacidade e configura ofensa à imagem e à honra do interessado, a empresa não reage de forma célere para retirar do ar a referida informação, tornando-se, assim, solidariamente responsável com o autor do dano pela reparação à vítima.

O Superior Tribunal de Justiça (STJ) através de sua jurisprudência, reflete a preocupação da corte em garantir a proteção da personalidade e da privacidade, o reconhecimento contínuo da importância da proteção de dados pessoais como direito fundamental e a necessidade de garantir sua efetiva aplicação e respeito pelos envolvidos.

## **2.4 A PROTEÇÃO DOS DADOS E OS DIREITOS DA PERSONALIDADE**

O direito da personalidade é um conjunto de direitos subjetivos da pessoa, que se vinculam à própria dignidade humana, e são tutelados juridicamente pela ordem jurídica. Em geral, compreende-se que os direitos da personalidade têm por finalidade assegurar a integridade moral, psicológica e física da pessoa, protegendo a sua honra, imagem, intimidade, privacidade, liberdade, entre outros.

Diniz (2005) nos ensina que a personalidade consiste no conjunto de caracteres próprios da pessoa. A personalidade não é um direito, de modo que seria errôneo afirmar que o ser humano tem direito à personalidade. A personalidade é que apoia os direitos e deveres que dela irradiam, é objeto de direito, é o primeiro bem da pessoa, que lhe pertence como primeira utilidade, para que ela possa ser o que é, para sobreviver e se adaptar às condições do ambiente em que se encontra, servindo-lhe de critério para aferir, adquirir e ordenar outros bens. Assevera que os direitos da personalidade são absolutos, intransmissíveis, indisponíveis, irrenunciáveis, ilimitados, imprescritíveis, impenhoráveis, inexpropriáveis e extrapatrimoniais.

Segundo o Código Civil brasileiro, os direitos da personalidade são considerados inalienáveis e irrenunciáveis, ou seja, não podem ser objeto de negociação ou renúncia pelo indivíduo, nem mesmo em benefício próprio. Além disso, a lei prevê que a violação dos direitos da personalidade acarreta o dever de indenizar o dano moral decorrente.

Dentre os principais dispositivos legais que protegem os direitos da personalidade no Brasil, destaca-se o artigo 5º, inciso X, da Constituição Federal, que dispõe sobre a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

O Código Civil, dos direitos da personalidade, por sua vez, prevê em seu artigo 11 que, com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.

A Lei Geral de Proteção de Dados (LGPD) brasileira, assim como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, reconhecem a importância dos direitos da personalidade e preveem medidas de proteção específicas para assegurar a privacidade e a segurança dos dados pessoais dos indivíduos. Isso porque a coleta, processamento e uso indevido de dados pessoais podem afetar negativamente a privacidade e a autonomia dos indivíduos, violando seus direitos da personalidade.

Segundo Diniz (2020), os direitos da personalidade são os direitos subjetivos de cada pessoa de terem respeitada a sua integridade física e psíquica, a sua identidade, a sua privacidade, a sua honra e reputação, o seu nome, o seu pseudônimo, o seu corpo, a sua imagem, a sua voz, a sua saúde, a sua segurança, o seu trabalho, a sua atividade intelectual, artística, científica e literária.

Os direitos da personalidade estão previstos em diversas legislações, incluindo a Constituição Federal (artigo 5º, incisos V, X, XIII, XIV e XXVIII) e o Código Civil (artigos 11 a 21). Além disso, o Brasil também é signatário da Convenção Americana de Direitos Humanos, que reconhece a proteção aos direitos da personalidade como um direito fundamental.

A proteção dos dados pessoais é um aspecto importante dos direitos da personalidade, pois o uso indevido ou a divulgação não autorizada desses dados pode prejudicar a privacidade, a imagem e a reputação de uma pessoa. É por isso que a proteção dos dados pessoais é considerada uma extensão dos direitos da personalidade.

No Brasil, a Lei Geral de Proteção de Dados (LGPD), em vigor desde setembro de

2020, estabelece regras para a coleta, o tratamento e o armazenamento de dados pessoais. A LGPD garante aos indivíduos o direito de acesso aos seus dados pessoais, o direito de corrigir informações imprecisas, o direito de solicitar a exclusão de dados desnecessários ou inadequados e o direito de revogar o consentimento para o uso de seus dados pessoais a qualquer momento.

### **3- HISTÓRICO DAS LEIS DE PROTEÇÃO DE DADOS E DA PRIVACIDADE NA INTERNET**

As leis de proteção de dados e da privacidade na internet têm uma história relativamente recente, começando a se desenvolver nos anos 1990, quando a Internet se tornou amplamente disponível para o público em geral. Abaixo, segue um breve histórico das principais leis de proteção de dados e da privacidade na internet em todo o mundo.

Desde 1995, com a Diretiva de Proteção de Dados da União Europeia, diversas leis e regulamentações foram criadas em todo o mundo para proteger a privacidade na internet. A Lei nº 9.296/1996 de Interceptação Telefônica brasileira estabeleceu regras para garantir a privacidade das comunicações dos cidadãos, enquanto a COPPA (Children's Online Privacy Protection Act ) dos Estados Unidos foi criada para proteger a privacidade de crianças menores de 13 anos na Internet. Já a PECR (Privacy and Electronic Communications Regulations ) do Reino Unido estabeleceu regras para o uso de cookies e envio de e-mails de marketing.

A Lei de Proteção de Dados Pessoais do Brasil, LGPD, de 2018, também estabeleceu regras para a coleta, armazenamento e uso de informações pessoais no país. A LGPD é abrangente e se aplica a todas as empresas e organizações que realizam o tratamento de dados pessoais, independentemente do meio ou forma em que sejam realizados.

Além disso, a General Data Protection Regulation (GDPR) da União Europeia, de 2010, é considerada a lei mais abrangente de proteção de dados da Europa e estabeleceu regras rigorosas para a coleta, armazenamento e uso de informações pessoais.

Também foram criadas leis para coibir os crimes cibernéticos, como a Lei Carolina Dieckmann (Lei nº 12.737/2012) brasileira, que estabelece a invasão de dispositivos informáticos sem autorização como uma violação à privacidade das pessoas. O Marco Civil da Internet (Lei nº 12.965/2014), estabeleceu princípios, garantias, direitos e deveres para o uso da internet no país, incluindo o direito à privacidade dos usuários. Todas essas leis tiveram um impacto significativo na proteção da privacidade na internet em todo o mundo.

Essas são apenas algumas das leis que reconhecem e protegem o direito à privacidade no Brasil e no mundo. Há ainda outras legislações que tratam do tema em contextos específicos, como a Lei de Acesso à Informação, a Lei Maria da Penha, entre outras.

A Lei de Acesso à Informação (Lei nº 12.527/2011) entrou em vigor em 2012 e regulamenta o direito de acesso às informações públicas. Ela estabelece que todas as informações produzidas ou custodiadas pelos órgãos públicos são públicas e devem estar disponíveis para consulta pela sociedade. A lei define os procedimentos para acesso às informações públicas e as exceções em que o acesso pode ser restrito. Observância da publicidade como preceito geral e do sigilo como exceção O objetivo é promover a transparência na gestão pública e permitir que a sociedade possa fiscalizar as ações dos órgãos públicos e participar mais ativamente na tomada de decisões.

Já Lei Maria da Penha (Lei nº 11.340/2006) visa combater a violência doméstica e familiar contra a mulher. Embora a lei não trate explicitamente do direito à privacidade, a proteção da intimidade e da vida privada é um direito fundamental previsto na Constituição Federal Brasileira e deve ser respeitado em todos os casos.

No âmbito da Lei Maria da Penha, o direito à privacidade pode ser protegido de diversas formas. Por exemplo, é comum que as vítimas de violência doméstica sejam orientadas a manter sigilo sobre o processo, a fim de evitar retaliações por parte do agressor.

No entanto, é importante ressaltar que a proteção da privacidade não deve ser usada como justificativa para ocultar casos de violência doméstica. Pelo contrário, a conscientização e o debate sobre a violência contra a mulher são fundamentais para promover mudanças na sociedade e prevenir novos casos. Nesse sentido, a privacidade deve ser protegida apenas quando necessária para garantir a segurança e o bem-estar da vítima. As leis de proteção de dados e da privacidade na internet continuam a evoluir e a se desenvolver em todo o mundo, à medida que as preocupações com a privacidade pessoal crescem e as tecnologias continuam a avançar como se estudará nos capítulos seguintes.

### 3.1 A NOVA LEI DE PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

A Lei Geral de Proteção de Dados Pessoais (LGPD) foi originalmente aprovada em agosto de 2018 com o número 13.709/2018, e sua entrada em vigor foi adiada diversas vezes, sendo a última data de adiamento para o início da vigência 3 de maio de 2021, por meio da Medida Provisória nº 959/2020.

A nova Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece as regras para o tratamento de dados pessoais, define dados pessoais como informações relacionadas a uma pessoa natural identificada ou identificável, tanto por empresas privadas quanto pelo governo e não se limita apenas ao tratamento de dados pessoais em formato digital. Ela se aplica a qualquer operação que envolva o tratamento de dados pessoais, independentemente do meio em que estejam armazenados ou do formato em que se apresentem. A LGPD tem como objetivo proteger a privacidade e a liberdade dos cidadãos, garantindo que seus dados pessoais sejam tratados de forma adequada e respeitando seus direitos.

A LGPD se aplica a todas as empresas que coletam, armazenam, processam ou compartilham dados pessoais no Brasil, incluindo empresas estrangeiras que atuam no país, isso inclui desde pequenas empresas até grandes corporações multinacionais. A lei estabelece que o tratamento de dados pessoais pelo governo também deve seguir as mesmas regras, prevê sanções administrativas para empresas que não cumprirem as suas disposições, incluindo multas que podem chegar a 2% do faturamento da empresa, limitadas a R\$ 50 milhões por infração e podem sofrer outras sanções administrativas, como a suspensão do tratamento de dados ou a proibição de exercer atividades relacionadas ao tratamento de dados pessoais, dependendo da gravidade da infração cometida.

O artigo 52, parágrafo 4º e 5º da LGPD, que estabelece as sanções administrativas que podem ser aplicadas em caso de infração à lei.

Art. 52. Sem prejuízo das sanções administrativas previstas nesta Lei, as infrações cometidas em razão dos dados pessoais serão apenadas segundo a legislação geral e setorial de defesa do consumidor.

(...)

§ 4º As sanções previstas neste artigo serão aplicadas aos agentes de tratamento que, em razão das infrações cometidas, tenham auferido vantagem econômica, e serão graduadas de acordo com a gravidade da infração, a vantagem auferida

e a condição econômica do infrator, sendo a sua aplicação precedida de procedimento administrativo que possibilite a oportunidade de defesa e recurso administrativo nos termos do art. 65.

§ 5º As sanções previstas neste artigo poderão ser aplicadas cumulativamente, inclusive com as previstas no art. 56, e serão devidamente motivadas."(LGPD, 2020).

Essa lei é crucial por estabelecer um marco regulatório moderno e eficaz para o tratamento de dados pessoais no Brasil, garantindo a proteção dos direitos fundamentais das pessoas e incentivando a economia digital e estabelece:

- **Proteção dos direitos fundamentais:** A LGPD garante a proteção dos direitos fundamentais das pessoas, como a privacidade, intimidade e proteção dos dados pessoais. Com isso, as pessoas têm mais controle sobre como seus dados pessoais são coletados, usados, compartilhados e armazenados.
- **Prevenção de abusos:** A LGPD estabelece regras claras e rigorosas para o tratamento de dados pessoais, evitando abusos por parte de empresas e organizações que coletam e processam esses dados.
- **Fomento à economia digital:** Com a LGPD, as empresas e organizações são incentivadas a adotar boas práticas de segurança da informação e a investir em tecnologias de proteção de dados, o que pode impulsionar a economia digital.
- **Conformidade com padrões internacionais:** A LGPD é inspirada em regulamentações internacionais, como o Regulamento Geral de Proteção de Dados (RGDP) da União Europeia, e contribui para que o Brasil esteja em conformidade com esses padrões globais de proteção de dados.

Os acordos comerciais entre Brasil e União Europeia poderiam ser impactados se o Brasil não tivesse criado a Lei Geral de Proteção de Dados Pessoais (LGPD) ou legislado sobre o tratamento de dados pessoais. Isso ocorre porque a União Europeia possui o Regulamento Geral de Proteção de Dados (RGDP), uma regulamentação bastante rigorosa para proteção de dados pessoais, e que exige que os países com os quais realiza acordos comerciais tenham normas equivalentes.

Sem a LGPD, o Brasil não estaria em conformidade com as normas europeias de proteção de dados pessoais, o que poderia dificultar ou até inviabilizar a realização de



acordos comerciais com a União Europeia. Isso ocorre porque a União Europeia pode impor restrições comerciais a países que não estejam em conformidade com suas normas de proteção de dados.

Além disso, empresas brasileiras que desejam fazer negócios com empresas europeias também poderiam enfrentar dificuldades se não estiverem em conformidade com as normas europeias de proteção de dados. Isso pode gerar um impacto negativo para a economia brasileira, uma vez que a União Europeia é um importante parceiro comercial do Brasil.

Por isso, a criação da LGPD é fundamental para garantir a conformidade do Brasil com as normas internacionais de proteção de dados pessoais, o que pode facilitar a realização de acordos comerciais e gerar oportunidades para a economia brasileira.

A Lei Geral de Proteção de Dados (LGPD) estabelece importantes disposições para proteger os dados pessoais dos cidadãos brasileiros. Uma das principais é a obrigatoriedade do consentimento expresso e informado do titular dos dados para a coleta, uso, processamento e compartilhamento de suas informações pessoais. Além disso, a LGPD garante que os titulares dos dados possam acessar, corrigir, eliminar ou transferir seus dados para outro fornecedor de serviços.

A manipulação de dados pessoais de crianças e adolescentes foi contemplada na LGPD, que trata do assunto no Artigo 14, lembrando que nessas hipóteses a lei deve ser aplicada e interpretada em consonância com o Estatuto da Criança e do Adolescente - ECA, e o Código Civil. Ao contrário do RGPD, a nossa lei não fixou a idade limite para que o titular dos dados promova o consentimento de forma autônoma, fixando apenas que o tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal (§ 1º do Artigo 14). Assim, entendemos que deve ser aplicado Art. 2º do ECA, que considera criança a pessoa até doze anos de idade incompletos.

As empresas também têm um papel importante na proteção dos dados pessoais, sendo responsáveis por adotar medidas de segurança adequadas para proteger essas informações contra acessos não autorizados e outros tipos de incidentes de segurança.

A LGPD também estabelece a criação da Autoridade Nacional de Proteção de Dados (ANPD), uma autarquia Federal vinculada à Presidência da República,

responsável por fiscalizar e aplicar sanções em caso de descumprimento da lei.

Embora a LGPD represente um importante avanço para a proteção de dados pessoais no Brasil, a implementação da lei ainda é um desafio para muitas empresas que precisam se adequar às novas regras e garantir a segurança dos dados que coletam e processam.

É importante destacar que o direito à privacidade deve ser entendido como o direito de cada pessoa de decidir quais informações pessoais quer compartilhar, com quem quer compartilhar e para que finalidade. O controle sobre as próprias informações é essencial para proteger a liberdade, a autonomia e a dignidade dos indivíduos na sociedade atual.

### **3.2 ESCOPO DE APLICAÇÃO E PRINCÍPIOS DA LGPD**

A Lei Geral de Proteção de Dados (LGPD) do Brasil tem como objetivo regular o tratamento de dados pessoais por empresas e pelo governo, garantindo a proteção da privacidade dos usuários e aumentando a transparência no uso dessas informações. A LGPD se aplica a qualquer operação que envolva o tratamento de dados pessoais, desde a sua coleta até o seu descarte.

Fernandez, na sua obra Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais, preleciona que a LGPD é uma Lei que:

dispõe sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade natural, INCLUSIVE POR MEIO DIGITAL (Art 1º). (FERNANDEZ, 2020, p. 17).

A Lei Geral de Proteção de Dados (LGPD) foi criada com o intuito de preservar os direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade, incluindo aspectos digitais. A LGPD é regida por nove princípios, sendo o primeiro deles a finalidade, que determina que os dados pessoais devem ser tratados para fins legítimos e explícitos. O princípio da adequação estabelece que o tratamento de dados pessoais deve ser limitado ao mínimo necessário, enquanto o princípio da necessidade determina que os dados pessoais devem ser coletados apenas na medida necessária para o tratamento.

O princípio do livre acesso garante ao titular dos dados o acesso facilitado e

gratuito aos dados coletados, bem como à forma como estão sendo tratados. Já o princípio da qualidade determina que os dados pessoais devem ser precisos, claros, atualizados e pertinentes. A transparência é um princípio que garante que o titular dos dados pessoais seja informado de forma clara e completa sobre o tratamento desses dados.

A LGPD também estabelece o princípio da segurança, que determina que os dados pessoais devem ser protegidos por medidas técnicas e administrativas adequadas para evitar o acesso não autorizado ou ilegal, a destruição, perda, alteração, comunicação ou difusão. O princípio da prevenção exige que os responsáveis pelo tratamento de dados pessoais adotem medidas preventivas para evitar danos decorrentes do tratamento desses dados. Por fim, a LGPD também estabelece o princípio da não discriminação, que determina que o tratamento de dados pessoais não pode ser utilizado para discriminar o titular dos dados.

A LGPD busca estabelecer um conjunto de princípios que garantam o tratamento adequado e transparente dos dados pessoais, com o objetivo de proteger a privacidade dos usuários e aumentar a confiança na utilização dessas informações. Quanto à inaplicabilidade da LGPD, temos no artigo 4º a seguinte redação:

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II - realizado para fins exclusivamente:

a) jornalístico e artísticos; ou

b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

III - realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais; ou

IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

Dentro dessa limitação, Peck , Patricia (2018, p. 43-44) discursa que “o tratamento de dados pessoais deve seguir um propósito certo e funcional, mas que não supere a liberdade de informação e expressão, a soberania, segurança e a defesa do Estado.” Têm-se, nesse sentido, uma certa limitação buscando consigo uma maior segurança em temas relevantes da sociedade.

### **3.3 O IMPACTO ECONÔMICO DA LEI GERAL DE PROTEÇÃO DE DADOS**

Uma Lei Geral de Proteção de Dados (LGPD) pode ter um impacto econômico significativo, tanto positivo quanto negativo, dependendo da forma como é implementada e do setor econômico em questão.

Por um lado, a LGPD pode estimular a inovação e a criação de novos negócios baseados na privacidade e na proteção de dados pessoais, criando oportunidades para empresas especializadas em segurança cibernética e privacidade, bem como para empresas que desenvolvem tecnologias para ajudar as empresas a se conformarem com as regulamentações de proteção de dados. Além disso, a LGPD pode aumentar a confiança dos consumidores nas empresas que demonstram respeito e cuidado com seus dados pessoais, o que pode levar a um aumento na fidelidade do cliente e na receita.

Por outro lado, a LGPD também pode representar um desafio para empresas que não estão acostumadas a lidar com questões de privacidade e segurança cibernética, exigindo investimentos significativos em tecnologias e treinamento de pessoal para cumprir as novas regulamentações. Esses custos podem ser particularmente altos para empresas menores e com menos recursos.

A LGPD pode afetar negativamente setores que dependem fortemente da coleta e uso de dados pessoais, como o marketing digital, a publicidade online e a análise de dados. Isso pode levar a uma diminuição na eficácia dessas atividades e uma redução no valor das empresas que operam nesses setores.

No geral, a lei pode ter um impacto econômico significativo, tanto positivo quanto negativo, mas é importante lembrar que a proteção de dados pessoais é um direito fundamental e que as regulamentações de proteção de dados são importantes para

garantir a privacidade e segurança dos indivíduos.

Algumas possíveis implicações econômicas são:

- Custos de conformidade: as empresas precisam investir em recursos e tecnologias para se adequar às novas exigências de proteção de dados, o que pode gerar custos significativos. No entanto, esses custos podem ser amortizados ao longo do tempo, uma vez que as medidas de proteção de dados se tornem parte das práticas comerciais normais.
- Sanções e multas: em caso de violação da lei, as empresas podem ser sujeitas a sanções e multas, que podem ser significativas e afetar negativamente seus resultados financeiros.
- Melhoria da confiança do consumidor: a implementação da LGPD pode melhorar a confiança do consumidor nas empresas que tratam seus dados pessoais de forma responsável e transparente, o que pode levar a um aumento nas vendas e na lealdade do cliente.
- Inovação e competitividade: a lei pode estimular a inovação e a competitividade, uma vez que as empresas que desenvolvem tecnologias e práticas de proteção de dados mais eficazes podem ter vantagens competitivas.
- Proteção dos direitos dos cidadãos: a LGPD visa proteger os direitos dos cidadãos em relação à privacidade e à proteção de dados pessoais, o que pode ter um impacto positivo na sociedade como um todo.

A LGPD pode ter um impacto positivo na economia ao incentivar práticas de proteção de dados mais eficazes e aumentar a confiança do consumidor, mas pode gerar custos e sanções para as empresas que não cumprem as exigências da lei. No entanto, é possível que algumas empresas e organizações tenham argumentos contrários à LGPD. Alguns desses argumentos incluem:

- Custo elevado de implementação: Algumas empresas podem argumentar que a implementação das medidas de segurança e proteção exigidas pela

LGPD pode gerar custos elevados e dificuldades financeiras.

- Restrição à inovação: Algumas empresas podem argumentar que as normas da LGPD podem restringir a inovação e o desenvolvimento de novos serviços e produtos que envolvam o tratamento de dados pessoais.
- Interesse público: Algumas empresas e organizações podem argumentar que o interesse público pode justificar o tratamento de dados pessoais sem o consentimento do titular, como em casos de segurança nacional, investigações criminais ou saúde pública.

Apesar desses argumentos contrários, a implementação eficaz da LGPD mesmo que possa envolver desafios e custos, é importante reconhecer que ela também oferece uma série de benefícios tanto para as empresas quanto para os indivíduos, promovendo uma cultura de proteção de dados e impulsionando o desenvolvimento sustentável no contexto digital.

#### **4.0 A LEI 13.709/18 E O NOVO PARADIGMA DA PRIVACIDADE**

A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), representa um novo paradigma na privacidade e na proteção de dados pessoais no Brasil. A LGPD estabelece uma série de regras e princípios para o tratamento de dados pessoais por parte de empresas e do poder público, e tem como objetivo principal proteger a privacidade e os direitos dos titulares dos dados.

Antes da LGPD, não havia uma legislação específica sobre proteção de dados pessoais no Brasil. A LGPD veio para preencher essa lacuna, estabelecendo uma base legal para a coleta, uso e tratamento de dados pessoais, bem como definindo as obrigações das empresas e do poder público em relação a esses dados.

A LGPD segue o modelo de proteção de dados europeu, conhecido como Regulamento Geral de Proteção de Dados (RGPD). Ambas as leis têm como objetivo proteger os direitos dos titulares de dados, promovendo a transparência, a segurança e a privacidade na coleta e tratamento de informações pessoais.

Com a LGPD, as empresas precisam obter o consentimento dos titulares de dados para coletar e usar suas informações pessoais, e devem informar claramente sobre o propósito da coleta de dados e como eles serão usados. As empresas também precisam implementar medidas de segurança e privacidade para proteger esses dados.

Além disso, a LGPD garante aos titulares de dados o direito de acessar seus próprios dados pessoais, corrigi-los ou excluí-los, quando necessário. Os titulares também têm o direito de solicitar informações sobre como seus dados pessoais estão sendo usados e com quem estão sendo compartilhados.

A LGPD representa um novo paradigma na privacidade e na proteção de dados pessoais no Brasil, estabelecendo uma base legal para a coleta, uso e tratamento de dados pessoais. A LGPD promove a transparência, a segurança e a privacidade na coleta e tratamento de informações pessoais, garantindo os direitos dos titulares de dados. As empresas e o poder público precisam cumprir as obrigações estabelecidas pela LGPD, implementando medidas de segurança e privacidade e garantindo o respeito aos direitos dos titulares de dados.

## 4.1 RISCOS DO VAZAMENTO DE DADOS PARA O INDIVÍDUO

O vazamento de dados pessoais pode trazer uma série de riscos e prejuízos para o indivíduo afetado. Isso porque os dados pessoais podem incluir informações sensíveis, como nome completo, endereço, número de CPF, informações financeiras e de saúde, entre outros.

Entre os principais riscos do vazamento de dados pessoais, podemos destacar:

- Roubo de identidade: os dados pessoais podem ser usados por criminosos para roubar a identidade do indivíduo, abrindo contas bancárias, solicitando empréstimos e cartões de crédito, e realizando outras atividades fraudulentas.
- Fraudes financeiras: os dados financeiros do indivíduo podem ser usados para realizar fraudes, como compras fraudulentas ou transferências bancárias não autorizadas.
- Exposição de informações sensíveis: dados de saúde ou informações pessoais sensíveis podem ser expostos, causando danos à privacidade do indivíduo e potencialmente levando a consequências negativas em áreas como o emprego ou a saúde mental.
- Risco à segurança física: se os dados pessoais incluem informações de localização, por exemplo, podem ser usados para rastrear e perseguir o indivíduo.
- Danos à reputação: a divulgação de informações pessoais pode prejudicar a reputação do indivíduo, especialmente se as informações são comprometedoras ou embaraçosas.

Por esses motivos, é importante que empresas e o poder público tratem os dados pessoais com a devida importância e responsabilidade, implementando medidas de segurança e privacidade para proteger essas informações e prevenir o vazamento de dados. Os indivíduos também devem estar cientes dos riscos envolvidos e tomar medidas para proteger seus próprios dados, como utilizar senhas fortes, evitar compartilhar informações pessoais em sites suspeitos e monitorar regularmente suas contas financeiras e de crédito.



## 4.2 TRATAMENTO E RESPONSABILIDADE DO PODER PÚBLICO

O termo “Poder Público” é definido pela LGPD de forma ampla e inclui órgãos ou entidades dos entes federativos (União, Estados, Distrito Federal e Municípios) e dos três Poderes (Executivo, Legislativo e Judiciário), inclusive das Cortes de Contas e do Ministério Público. Assim, os tratamentos de dados pessoais realizados por essas entidades e órgãos públicos devem observar as disposições da LGPD, ressalvadas as exceções previstas no art. 4º da lei. A Lei Geral de Proteção de Dados estabelece que o poder público é responsável pelo tratamento adequado e transparente dos dados pessoais de cidadãos, sejam eles coletados de forma direta ou indireta. Essa responsabilidade é ainda mais relevante no caso do poder público, já que o tratamento de dados é uma das atividades centrais das instituições governamentais.

O poder público tem uma grande responsabilidade na proteção dos dados pessoais, são responsáveis pelos danos causados aos titulares de dados pessoais em virtude de tratamento desses dados de forma irregular ou ilegal. Isso significa que, caso um órgão público viole as disposições da LGPD no tratamento de dados pessoais, pode ser responsabilizado pelos danos causados aos titulares desses dados. O Estado é responsável por garantir que as informações pessoais coletadas sejam tratadas de forma adequada e protegidas de uso indevido ou abusivo.

Em muitos países, existem leis específicas que regem a coleta e o tratamento de dados pessoais pelo poder público, tais como a LGPD no Brasil e a RGPD na União Europeia. Essas leis estabelecem diretrizes e princípios para o uso de dados pessoais, incluindo a transparência, a finalidade específica, a minimização dos dados coletados, a segurança e a proteção contra acesso não autorizado.

O poder público deve ser responsável por proteger os dados pessoais coletados e usados em seus sistemas e serviços, bem como garantir que esses dados sejam processados de acordo com a legislação aplicável. Isso inclui implementar medidas técnicas e organizacionais adequadas para proteger os dados pessoais, monitorar o uso de dados e realizar auditorias regulares para garantir a conformidade com as leis de proteção de dados.

Além disso, o artigo 42 da LGPD prevê que os titulares de dados pessoais têm

direito a serem indenizados pelos danos patrimoniais, morais, individuais ou coletivos que venham a sofrer em decorrência do tratamento de seus dados pessoais. O artigo 43 estabelece que os órgãos públicos são solidariamente responsáveis pelos danos causados pelo tratamento de dados pessoais, ou seja, todos os órgãos envolvidos no tratamento de dados pessoais podem ser responsabilizados pelos danos causados, independentemente de culpa ou dolo. Cabe ressaltar que, para que a responsabilidade do poder público seja efetivada, é necessário que haja comprovação do dano causado e da relação de causalidade entre o tratamento de dados pessoais e o dano sofrido pelo titular dos dados.

As instituições governamentais devem ser transparentes sobre como os dados pessoais são coletados e usados, bem como garantir que as pessoas afetadas tenham acesso a seus próprios dados pessoais e possam solicitar sua correção ou exclusão, quando necessário.

O setor público tem uma grande responsabilidade na proteção dos dados pessoais. É fundamental garantir que as informações pessoais coletadas sejam tratadas de forma adequada e protegidas de uso indevido ou abusivo. As leis de proteção de dados estabelecem diretrizes e princípios para o uso de dados pessoais pelas instituições governamentais, e é importante que essas leis sejam implementadas e seguidas corretamente. A transparência, a segurança e a proteção dos dados pessoais são fundamentais para garantir a privacidade e os direitos dos cidadãos.

Um aspecto importante a ser considerado nesse contexto é a previsão legal contida no artigo 7º, inciso II, da LGPD, que estabelece que o tratamento de dados pessoais pelo Poder Público pode ser realizado para o cumprimento de obrigação legal ou regulatória pelo controlador.

Essa disposição da lei reconhece a necessidade de os órgãos governamentais coletarem e utilizarem dados pessoais como parte de seu dever legal ou regulatório. O tratamento de dados pelo Poder Público é frequentemente necessário para o cumprimento de diversas obrigações legais, tais como a administração de programas sociais, a execução de políticas públicas, a manutenção da ordem pública e a promoção da segurança nacional.

Essas obrigações legais ou regulatórias podem exigir o tratamento de dados

sensíveis, que são informações pessoais especialmente protegidas pela LGPD, como dados relacionados à saúde, origem racial ou étnica, convicções religiosas, entre outros. O artigo 11, inciso II, alínea a, da LGPD também prevê essa hipótese, permitindo o tratamento de dados sensíveis pelo Poder Público quando necessário para o cumprimento de obrigação legal ou regulatória.

O poder público deve garantir a proteção adequada dos dados pessoais que coleta, tratando-os de forma transparente, segura e respeitando os direitos dos titulares desses dados. Além disso, é importante que o poder público limite a coleta de dados pessoais, permitindo apenas o que for estritamente necessário para o exercício de suas funções e atividades.

Transparência é essencial nesse processo, e o poder público deve informar aos titulares dos dados sobre o tratamento de seus dados pessoais, incluindo as finalidades para as quais são coletados, as bases legais para o tratamento e os direitos dos titulares. Os titulares devem ter o direito de acessar, corrigir, excluir e controlar seus dados pessoais.

Outra obrigação do poder público é garantir a segurança dos dados pessoais. Para isso, devem ser adotadas medidas de segurança apropriadas, a fim de evitar perda, acesso não autorizado, destruição ou divulgação indevida desses dados.

No caso de violação de dados pessoais por parte do poder público, a LGPD prevê a aplicação de sanções administrativas, como advertência, multa, publicização da infração e suspensão parcial ou total do tratamento de dados. Além disso, os titulares dos dados pessoais têm o direito de buscar a reparação de danos morais e materiais decorrentes da violação.

A Autoridade Nacional de Proteção de Dados desempenha um papel central na interpretação da Lei Geral de Proteção de Dados e no estabelecimento de normas e diretrizes para sua implementação. Ela possui competência para deliberar administrativamente sobre a interpretação da lei, suas próprias atribuições e casos omissos, em caráter terminativo conforme o art. 55-K, parágrafo único; art. 55-J, XX.

Além disso, a ANPD é responsável exclusiva pela aplicação das sanções administrativas previstas na LGPD, prevalecendo suas competências sobre outras entidades e órgãos da administração pública em relação à proteção de dados pessoais

conforme o art. 55-K.

Portanto, a ANPD possui competência original, específica e uniformizadora no que diz respeito à proteção de dados pessoais e à aplicação da LGPD. No entanto, essa previsão legal deve ser interpretada de forma a compatibilizar-se com a atuação de outros entes públicos que também possam tratar do assunto. A LGPD estabelece a necessidade de coordenação e articulação da ANPD com outros órgãos e entidades públicas, buscando assegurar o cumprimento eficiente de suas atribuições e promover o adequado funcionamento dos setores regulados conforme o art. 55-J, § 3º.

Os servidores públicos que violarem a LGPD também podem ser responsabilizados administrativamente de forma pessoal e autônoma, de acordo com o art. 28 do Decreto-Lei nº 4.657, de 4 de setembro de 1942 Lei de Introdução às Normas do Direito Brasileiro. Portanto, o tratamento indevido de dados pessoais, como a venda de bancos de dados, a alteração ou supressão inadequada de cadastros ou o uso de dados pessoais para fins ilegítimos, pode resultar na responsabilização do servidor público que cometeu tais atos ilegais.

Vale ressaltar que a Lei de Acesso à Informação (Lei 12.527/11) também estabelece que o poder público é responsável por garantir o acesso à informação pública de forma transparente e segura, ampliando ainda mais o compromisso do poder público com a proteção e tratamento adequado dos dados pessoais.

## **5- METODOLOGIA**

A realização desta monografia baseou-se em pesquisa bibliográfica, envolvendo artigos científicos, leis, livros e outros documentos relevantes sobre a privacidade, direito a privacidade, LGPD e proteção de dados no Brasil. A revisão da literatura permitiu a coleta de informações atualizadas e abrangentes, abarcando diferentes perspectivas e abordagens relacionadas ao tema em estudo.

## 6- CONCLUSÃO

O direito à privacidade é um direito fundamental reconhecido mundialmente sendo crucial para proteger a liberdade, a autonomia e a dignidade dos indivíduos, permitindo-lhes manter uma esfera pessoal e íntima longe do escrutínio público e governamental. Com o uso crescente da tecnologia e a coleta massiva de dados, tornou-se necessário o estabelecimento de leis que regulamentem o tratamento desses dados. A LGPD no Brasil é um avanço legislativo essencial que visa garantir e proteger os direitos fundamentais de liberdade, privacidade e proteção de dados pessoais dos usuários.

A proteção de dados pessoais está intrinsecamente ligada aos direitos da personalidade é um assunto que diz respeito a todos, pois a coleta, o processamento e o uso indevido de dados pessoais podem afetar a privacidade e a autonomia dos indivíduos. As leis de proteção de dados, como a LGPD no Brasil e o Regulamento Geral de Proteção de Dados (RGPD) na União Europeia, foram elaboradas para garantir a proteção de dados. Esta é uma questão global, e muitos países adotaram leis semelhantes à LGPD e RGPD, indicando a crescente importância da proteção de dados pessoais em todo o mundo. No entanto, ainda há muito a ser feito para garantir que os indivíduos tenham controle sobre seus dados pessoais e que as organizações processem esses dados com responsabilidade e segurança.

Para que este direito fundamental seja respeitado e protegido é fundamental trabalharmos em conjunto. Isso inclui o governo, empresas, organizações da sociedade civil e indivíduos. Ao proteger a privacidade e os dados pessoais, estamos protegendo a dignidade humana, a liberdade e a autonomia, valores fundamentais para uma sociedade justa e democrática.

## 7- REFERÊNCIAS

BAIÃO, R. B. S. M. **Lei Geral de Proteção de Dados, Direito ao Apagamento, Correção dos Dados e Blockchain: Análise da Pertinência Tecnológica.** Cadernos Jurídicos, São Paulo, v. 21, n. 53, p. 151-162, jan./mar. 2020. Disponível em: [https://bdjur.stj.jus.br/jspui/bitstream/2011/142292/lei\\_geral\\_protecao\\_baiao.pdf](https://bdjur.stj.jus.br/jspui/bitstream/2011/142292/lei_geral_protecao_baiao.pdf) Acesso em: 11 mar. 2023.

BASAN, A. P. **Publicidade Digital e Proteção de Dados Pessoais: O Direito ao Sossego.** São Paulo: Editora Foco, 2021.

BENTHAM J. **An Introduction to the Principles of Morals and Legislation.** New York: Hafner Press, 1948. Disponível em: <https://www.earlymoderntexts.com/assets/pdfs/bentham1780.pdf>. Acesso em: 20 mar. 2023.

BENTIVEGNA, C. F. B. **Liberdade de Expressão, Honra, Imagem e Privacidade: Os Limites Entre o Lícito e o Ilícito.** Barueri: Manole, 2019.

BIONI, B. R. **Proteção de Dados Pessoais: a Função e os Limites do Consentimento.** 2. ed. rev. atual. e reform. Rio de Janeiro: Forense, 2020.

BIONI, B. R. **Proteção de Dados Pessoais: a Função e os Limites do Consentimento.** 3ed. Rio de Janeiro: Forense, 2021.

BRASIL. **Código Criminal do Império do Brasil, LEI DE 16 DE DEZEMBRO DE 1830.** Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/lim/lim-16-12-1830.htm](https://www.planalto.gov.br/ccivil_03/leis/lim/lim-16-12-1830.htm). Acesso em: 09 abr. 2023.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília: Presidência da República, 2020. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 20 abr. 2023.

BRASIL. **Código Civil, LEI Nº 10.406, DE 10 DE JANEIRO DE 2002.** Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/2002/l10406compilada.htm](https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm) Acesso em: 23 mar. 2023.

BRASIL.STJ- **Decisões Monográficas.** Ministro MARCO BUZZI. 01.MAR 2023. Disponível em: <https://scon.stj.jus.br/SCON/pesquisar.jsp?livre=GOOGLE+NAO+PODE+SER+RESPOSTA+ABILIZADO&b=DTXT&p=true&tp=T>. Acesso em 15 mar 2023.

BRASIL. **Marco Civil da Internet.** LEI Nº 12.965, DE 23 DE ABRIL DE 2014 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: 27 mar. 2023.

BRASIL. **Lei Carolina Dieckmann**. Brasília, DF: Congresso Nacional, 2012. LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/l12737.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm) . Acesso em: 23 mar. 2023.

BRASIL. Agencia Nacional de Proteção de Dados. **Guia Orientativo: Tratamento de Dados Pessoais Pelo Poder Público**. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 15 mar. 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. **Lei Geral de Proteção de Dados Pessoais**. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/lgpd>. Acesso em: 10 mar. 2023.

BRASIL. Lei Nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_Ato2015-018/2018/Lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_Ato2015-018/2018/Lei/L13709.htm). Acesso em: 26 fev. 2023.

BRASIL. Lei nº. 8078, de 11 de setembro de 1990. **Dispõe Sobre a Proteção do Consumidor e das Outras Providências**. Brasília: Presidência da República, 2017. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/l8078compilado.htm](http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm). Acesso em: 20 abr. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República, 2020. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato20192022/2020/lei/l14020.htm](https://www.planalto.gov.br/ccivil_03/_ato20192022/2020/lei/l14020.htm). Acesso em: 11 mar. 2023.

BRASIL. Supremo Tribunal Federal. **Medida Cautelar Na Ação Direta De Inconstitucionalidade 6.387**. DISTRITO FEDERAL, 2020. Disponível em: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629>

BRASIL. Conselho Nacional de Justiça. **Lei Geral de Proteção de Dados Pessoais**. Disponível em: <https://www.cnj.jus.br/poder-judiciario/relacoes-institucionais/lei-geral-de-protecao-de-dados-pessoais-lgpd/>. Acesso em: 12 mar. 2023.

BRASIL. LEI Nº 9.296, DE 24 DE JULHO DE 1996. **Interceptação De Comunicações Telefônicas E Telemáticas No Âmbito Penal**. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/L9296.htm](http://www.planalto.gov.br/ccivil_03/leis/L9296.htm) Acesso em: 12 mar. 2023.

CADWALLADR C., GRAHAM H. E. (2018). **Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach**. The Guardian, March 17. Disponível em: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> Acesso em: 21 mar. 2023



CARROLL R., SHOTTON D. (2018). **The Cambridge Analytica Scandal: what you need to know.** The Guardian, March 23. Disponível em: <https://www.theguardian.com/technology/2018/mar/23/facebook-cambridge-analytica-data-scandal-explained> 21mar. 2023.

COUNCIL OF EUROPE. **European Convention on Human Rights.** Strasbourg cedex, 1950. Disponível em: [https://www.echr.coe.int/Documents/Convention\\_ENG.pdf](https://www.echr.coe.int/Documents/Convention_ENG.pdf). Acesso em: 09 mar. 2023

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro.** 22. ed, rev. e atual. São Paulo: Saraiva, 2005. v. 1, p. 121

DINIZ, M. H. et al. **Direito em Debate:** volume 1. São Paulo: Almedina, 2020

DONDA, D. **Guia Prático de Implementação da LGPD.** São Paulo: Labrador, 2020.

EHRHARDT J, M; CATALAN, M.; MALHEIROS, P. **Direito Civil e Tecnologia.** Belo Horizonte: Fórum, 2020.

FEDERAL TRADE COMMISSION. **Children's Online Privacy Protection Rule ("COPPA").** Washington, 1995. Disponível em: <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>. Acesso em 10 mar. 2023.

FRANÇA. CNIL. **Reconhecimento facial: CNIL ordena que CLEARVIEW AI deixe de reutilizar fotografias disponíveis na Internet.** Dez 2021. Disponível em: <https://www.cnil.fr/en/facial-recognition-cnil-orders-clearview-ai-stop-reusing-photographs-available-internet>. Acesso em: 16 mar 2023.

GARCIA, L.R. et al. **Lei Geral de Proteção de Dados Pessoais (LGPD): Guia de Implantação.** São Paulo: Blucher, 2020.

GONÇALVES, M. A. **Interceptação Telefônica:** teoria e prática. 2. ed. São Paulo: Saraiva, 2014.

MENDES, L.S; FONSECA, G.C. **Proteção De Dados Para Além Do Consentimento.** Disponível em: <file:///D:/521-Texto%20do%20Artigo-2105-2050-10-20200907.pdf> Acesso em: 15 mar. 2023.

Instituto Brasileiro de Defesa do Consumidor. **Guia LGPD: Lei Geral de Proteção de Dados Pessoais.** Disponível em: <https://guiadlgpd.idec.org.br/>. Acesso em: 15 mar. 2023.

JORNAL OFICIAL DA UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho** de 27 de abril de 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN> Acesso em: 10 mar. 2023.

Leonardi, M. **Direito e Internet: Liberdade de Expressão, Privacidade e Outros Temas**. São Paulo: Atlas. 2016.

MACIEL, R. F. **Manual Prático Sobre a Lei Geral de Proteção de Dados Pessoais (lei nº 13.70918)**. Disponível em: <https://pt.slideshare.net/MattosMattos6/manual-prtico-sobre-a-lei-geral-de-proteo-de-dados-pessoais-lei-n-1370918pdf>. Acesso em: 16 mar. 2023

MALDONADO, V. N. et al. **LGPD - Lei Geral de Proteção de Dados Pessoais: Manual de implementação**. 3ed. Belo Horizonte: Forum, 2022.

MARTINS, G.M.; LONGHI, J.V.R.; FALEIROS JUNIOR, J.L.de M. **A Consolidação Legislativa da Proteção de Dados no Brasil: Comentários às Alterações da Lei nº 13.853/2019**. Rio de Janeiro, 2020. Disponível em: [https://www.mprj.mp.br/documents/20184/1904621/Guilherme\\_Magalh%C3%A3es\\_Martins\\_&\\_Jo%C3%A3o\\_Victor\\_Rozatti\\_Longhi\\_&\\_Jos%C3%A9\\_Luiz\\_de\\_Moura\\_Faleiros\\_J%C3%BAnior.pdf](https://www.mprj.mp.br/documents/20184/1904621/Guilherme_Magalh%C3%A3es_Martins_&_Jo%C3%A3o_Victor_Rozatti_Longhi_&_Jos%C3%A9_Luiz_de_Moura_Faleiros_J%C3%BAnior.pdf). Acesso em: 11 mar. 2023.

MARTINS, P.L. et al. **Proteção de Dados**. Rio de Janeiro: INSTITUTO DE DIREITO PÚBLICO E PRIVADO – IDP, 2021. Disponível em: <Phttp://ppgdin.uff.br/wp-content/uploads/sites/5/2021/03/Livro-Estudos-do-Grupo-de-Prote%C3%A7%C3%A3o-de-Dados-Pessoais-%E2%80%93-CNPQ.pdf> Acesso em: 16 mar. 2023.

MAYER S., V., & CUKIER, K. (2013). **Big Data: A Revolution That Will Transform How We Live, Work, and Think**. Boston, MA: Houghton Mifflin Harcourt. Disponível em: [https://www.researchgate.net/publication/282515732\\_Book\\_Review\\_Big\\_Data\\_A\\_R\\_evolution\\_That\\_Will\\_Transform\\_How\\_We\\_Live\\_Work\\_and\\_Think](https://www.researchgate.net/publication/282515732_Book_Review_Big_Data_A_R_evolution_That_Will_Transform_How_We_Live_Work_and_Think) Acesso em: 11 mar.

MENDES, L. S. **O Direito Fundamental à Proteção de Dados Pessoais**. Revista de Direito do Consumidor. Disponível em: <https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1228/1155>. Acesso em: 19 mar. 2023.

MENDES, L.S; FONSECA, G.C.S. **Proteção de Dados para Além do Consentimento: Tendências Contemporâneas de Materialização**. Revista Estudos Institucionais, v. 6, n. 2, p. 507-533, maio/ago. 2020.

Ministério da Economia. **Lei Geral de Proteção de Dados**. Disponível em: <https://www.gov.br/economia/pt-br/assuntos/legislacao/protecao-de-dados-pessoais>. Acesso em: 16 mar. 2023.

MORAES, M.F. **Direito ao Esquecimento na Internet**. Ed. Lumen Juris, 2014 Disponível em: [http://www.mpsp.mp.br/portal/page/portal/documentacao\\_e\\_divulgacao/doc\\_biblioteca/ibli\\_servicos\\_produtos/BibliotecaDigital/BibDigitalLivros/TodosOsLivros/Melina-Ferracini-de-Moraes.pdf](http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/ibli_servicos_produtos/BibliotecaDigital/BibDigitalLivros/TodosOsLivros/Melina-Ferracini-de-Moraes.pdf) Acesso em: 15 mar. 2023.

NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. Disponível em: <https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf>. Acesso em: 09 mar.2023

NAÇÕES UNIDAS BRASIL. **Artigo 12: Direito à privacidade**. Disponível em: <https://nacoesunidas.org/artigo-12-direito-a-privacidade/>. Acesso em: 12 mar. 2023.

OCTACIANO N. **Constituição, história, Brasil. I. Brasil. [Constituição (1824)]**. 3.ed. Brasília : Senado Federal,Subsecretaria de Edições Técnicas, 2012. Disponível em: [https://www2.senado.leg.br/bdsf/bitstream/handle/id/137569/Constituicoes\\_Brasileiras\\_v1\\_1824.pdf](https://www2.senado.leg.br/bdsf/bitstream/handle/id/137569/Constituicoes_Brasileiras_v1_1824.pdf)

PARLAMENTO EUROPEU E CONSELHO DA UNIÃO EUROPEIA. **Directiva 95/46/ce do Parlamento Europeu e do Conselho**. Jornal Oficial das Comunidades Europeias n.1, l. 281/31, 1995.

RANGEL, P. A. **Interceptação telefônica**: aspectos controvertidos e jurisprudência. 4. ed. rev., atual. e ampl. São Paulo: Atlas, 2018.

SOLOVE, D. J. (2008). **Understanding Privacy**. Cambridge, MA: Harvard University Press. Disponível em: [https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2075&context=faculty\\_publications](https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2075&context=faculty_publications). Acesso em: 13 mar. 2023.

TARTUCE, F. **Manual de Direito Civil: volume único**.5. ed.Rio de Janeiro: Forense, 2015.

WARREN S. D.,BRANDEIS, L.D. **The Right to Privacy**. Harvard Law Review, Vol. 4, No. 5 (Dec. 15, 1890), Disponível em: <https://www.jstor.org/stable/1321160>, <https://doi.org/10.2307/1321160>

WESTIN, A. F. (1968). **Privacy and Freedom**. New York: Atheneum. Disponível em: <https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20/> Acesso em: 11 mar.2023.




WORLD ECONOMIC FORUM - WEF. **Personal Data: The Emergence of a New Asset Class**. World Economic Forum, May 2011. Disponível em: [http://www3.weforum.org/docs/WEF\\_ITTC\\_PersonalDataNewAsset\\_Report\\_2011.pdf](http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf)

## Página de assinaturas

# Maicon T

**Maicon Taichert**  
986.590.490-04  
Signatário

### HISTÓRICO

- 03 jul 2023**  
16:50:07  **Maicon Rodrigo Taichert** criou este documento. (E-mail: direito@fadesa.edu.br, CPF: 986.590.490-04)
- 03 jul 2023**  
16:50:08  **Maicon Rodrigo Taichert** (E-mail: direito@fadesa.edu.br, CPF: 986.590.490-04) visualizou este documento por meio do IP 170.239.203.253 localizado em Parauapebas - Para - Brazil
- 03 jul 2023**  
16:50:13  **Maicon Rodrigo Taichert** (E-mail: direito@fadesa.edu.br, CPF: 986.590.490-04) assinou este documento por meio do IP 170.239.203.253 localizado em Parauapebas - Para - Brazil

